HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 138 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, February 26, 2019

Chair

Mr. Bob Zimmer

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, February 26, 2019

● (1530)

[*English*]

The Chair (Mr. Bob Zimmer (Prince George—Peace River—Northern Rockies, CPC)): Good day. We'll call to order meeting number 138 of the Standing Committee on Access to Information, Privacy and Ethics. Pursuant to Standing Order 108(3)(h)(iv), we are here for a briefing on the security and intelligence threats to elections task force.

Today we have with us the Honourable Karina Gould, Minister of Democratic Institutions, for the first hour.

For the second hour, we have André Boucher, assistant deputy minister, operations, Canadian Centre for Cyber Security; and Dan Rogers, deputy chief, SIGINT. From the Privy Council Office, we have Allen Sutherland, assistant secretary to cabinet, machinery of government and democratic institutions; and Ayesha Malette, senior policy analyst, democratic institutions.

Minister Gould, we'll start with you. Go ahead for 10 minutes.

Hon. Karina Gould (Minister of Democratic Institutions): Thank you for the invitation to address the committee today. It is my pleasure to appear and to tell you more about the government's plan to safeguard the 2019 election.

I am pleased to be joined by officials today to speak to the technical aspects of Canada's plan. As the chair mentioned, this includes Allen Sutherland, assistant secretary to cabinet, machinery of government and democratic institutions; Daniel Rogers, deputy chief of SIGINT with the Communications Security Establishment; André Boucher, the assistant deputy minister of operations for the Canadian Centre for Cyber Security; and Ayesha Malette, senior adviser with the democratic institutions secretariat of PCO.

[*Translation*]

Before I start, I would like to express my gratitude to the members of the committee for their contribution over the past year to the study of disinformation. The information and views of the witnesses and members have provided valuable insight as we continue our efforts to safeguard the 2019 election.

Elections are an opportunity for Canadians to be heard, for them to express concerns and opinions through one of the most fundamental rights—the right to vote. However, this election will also experience an unprecedented amount of scrutiny.

[*English*]

As we have seen over the past few years, democracies around the world have entered a new era—an era of heightened threat and heightened vigilance—and 2019 will see a number of countries brace for volleys of attempted disruption: India, Australia, Ukraine, Switzerland, Belgium, the EU and, of course, Canada. Evidence has confirmed that the most recent Canadian general election, in 2015, was unencumbered by interference, although there were some relatively primitive attempts to disrupt, misinform and divide. These efforts were few in number and uncoordinated, and had no visible impact on the voter, either online or in line.

[*Translation*]

This election may be different. We've seen that the tools that were used to strengthen civic engagement are being used to undermine, disrupt and destabilize democracy.

We expect that some so-called "hacktivist" groups will use their cyber capabilities to try to influence our democratic process.

We could also face coordinated attempts at interference by foreign state actors, similar to what we have seen in other democracies over the last few years. This could include attempts to influence candidates or to manipulate social media to spread false or misleading information.

[*English*]

In recent years, we have witnessed foreign actors looking to undermine democratic societies and institutions, electoral processes, sovereignty and security. The malicious, multi-faceted and ever-evolving tactics constitute a serious strategic threat. We must be prepared for this. That is why in 2017 I asked Canada's Communications Security Establishment to analyze and make public an assessment of the current risk of cyber-threats and possible hacking of Canada's democratic processes. The report, "Cyber Threats to Canada's Democratic Process", was published as the world's first publicly shared threat assessment of its kind. It identified how key aspects of the democratic process, such as elections, political parties, politicians and media, are vulnerable to cyber-threat activity and influence operations.

● (1535)

[*Translation*]

This assessment, along with ongoing Canadian intelligence, and the experiences of allies and like-minded jurisdictions around the world have informed and guided our efforts over the past year, and led to the development of a plan of action based on four pillars.

We recognize that protecting Canada's democratic institutions requires a whole-of-society approach. Therefore, in addition to reinforcing and protecting government infrastructure, systems and practices, we are also focusing heavily on preparing Canadians and working with digital platforms that have an important role in fostering positive democratic debate and dialogue.

[*English*]

The four pillars of our plan are enhancing citizen preparedness, improving organizational readiness, combatting foreign interference and expecting social media platforms to act.

I'd like to take a few minutes to highlight some of the most significant initiatives of our plan.

Under the first pillar, enhancing citizen preparedness, we announced the digital citizen initiative. Our commitment includes an investment of $7 million towards improving the resilience of Canadians against online disinformation. We will leverage the expertise of civil society organizations that are directly working in communities on this issue.

We are increasing the reach and focus of the "get cyber safe" national public awareness campaign to educate Canadians about cybersecurity and the simple steps they can take to protect themselves online.

We have established the critical election incident public protocol. This is a simple, clear and impartial process for informing Canadians if serious incidents threaten the integrity of the 2019 general election.

The critical election incident public protocol panel is made up of five senior officials. It is expected to come to a decision jointly, based on consensus.

[*Translation*]

It is important to point out that this is the reason for a panel of five senior officials. It will not be one person deciding what Canadians should know.

The protocol will only be initiated to respond to incidents that occur within the writ period that do not fall within Elections Canada's area of responsibility.

The threshold for informing the public will be very high and limited to addressing exceptional circumstances that could impair our ability to have a free and fair election. As such, the threshold must extend beyond the normal negative rhetoric that is sometimes associated with political campaigns.

I am thankful that, in consulting with political parties on the development of this protocol, partisanship has been put aside in the interest of fairness. Incorporating input from all parties has allowed for a fair process that Canadians can trust.

[*English*]

Under the second pillar, improving organizational readiness, our national security and intelligence agencies are supporting Elections Canada by providing advice and guidance to improve its preparedness in the face of any potential interference in the administration of elections. The CSE is also offering ongoing cybersecurity technical advice and guidance to political parties.

The security agencies will offer threat briefings to key leadership and political parties, and security clearances are being arranged for senior members in each party to give them access to the right information to help them to strengthen internal security practices and behaviours.

[*Translation*]

Under the third pillar—combatting foreign influence—the government has established the Security and Intelligence Threats to Elections Task Force, or SITE, to improve awareness of foreign threats and support assessment and response. The team brings together the Communications Security Establishment, or CSE, the Canadian Security Intelligence Service, or CSIS, the Royal Canadian Mounted Police, or RCMP, as well as Global Affairs Canada, to ensure a comprehensive understanding of and response to any threats to Canada's democratic process.

Let me take a moment there to explain how the Critical Election Incident Public Protocol and the SITE Task Force are distinct yet related elements of our approach.

SITE ensures that the work of Canada's national security agencies is being done in a coordinated manner that aligns with the respective legal mandates of the agencies. Each of these agencies has 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.

● (1540)

[*English*]

The protocol will add a process for sharing relevant information with the panel of senior public service officials who will decide if incidents meet the threshold of interfering with Canada's ability to have a free and fair election.

When 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 national security and intelligence adviser to brief the panel accordingly, either through regular briefings or on an ad hoc basis, as is required.

We have activated the G7 rapid response mechanism, announced at the G7 leaders' summit in Charlevoix, to strengthen coordination among our G7 allies and to ensure that there is international collaboration and coordination in responding to foreign threats to democracy.

The fourth pillar is with respect to social media platforms.

I don't have to tell this committee that the face of mass media has turned from Gutenberg to Zuckerberg in a generation. It is a transformation for which the impact on society is impossible to overstate.

Social media and online platforms are the new arbiters of information and, therefore, have a responsibility to manage their communities. We know that they have also been manipulated to spread disinformation, create confusion and exploit societal tensions. The platforms have acknowledged the risk posed by misinformation and disinformation. I have been meeting with social media and digital platforms to secure action to increase transparency, improve authenticity and ensure greater transparency on their platforms.

Social media companies have reacted to the incidents of 2016 with some enhancements to their platforms. As a starting point, our government expects that those enhancements be made available to users in Canada as they have been made available to users in the U. S. and Europe.

[*Translation*]

This comprehensive plan is also bolstered by recent legislative efforts. Bill C-76, which received royal assent on December 13, 2018, takes important steps to counter foreign interference and the threats posed by emerging technologies.

[*English*]

Provisions in this bill include prohibiting foreign entities from spending any money to influence elections, where previously they were able to spend up to $500 unregulated, requiring organizations selling advertising space to not knowingly accept elections advertisements from foreign entities;

[*Translation*]

adding a prohibition regarding the “unauthorized use of computers” where there is intent to obstruct, interrupt or interfere with the lawful use of computer data during an election; and requiring online platforms to disclose the identity of advertisers by maintaining a publicly accessible registry of political ads published on the platform during the pre-election and the election.

[*English*]

It should be noted that Canada has a robust and highly respected elections administration body in Elections Canada. With the legislative, policy and programmatic efforts I have detailed for you today, Canada is in the best possible position to counter efforts to interfere in our democratic processes.

While it is impossible to fully predict what kinds of threats if any, we will see in the run-up to Canada's general election, I want to assure this committee that Canada has put in place a solid plan. We continue to test and probe our readiness and will continue to take whatever steps we can toward ensuring a secure, free and fair election in 2019.

[*Translation*]

Thank you.

[*English*]

and I now welcome your questions.

The Chair: Thank you, Minister.

We'll start off the first seven-minute round with Ms. Vandenbeld.

Ms. Anita Vandenbeld (Ottawa West—Nepean, Lib.): I want to thank you, Minister, for being here today and also for the incredible amount of work you've put into this, making Canada, I do believe, one of the first countries in the world to have these kinds of protocols.

Recently the all-party democracy caucus heard from Chris Walker, who has written on sharp power. This is power that some authoritarian regimes use. It's distinguished from soft power because it is subversive and it's intended to change public opinion or divide public opinion in other countries. When you mention the foreign threats, we're not unique. This is happening in countries around the world.

You mentioned the G7 rapid response mechanism. I wonder if you could elaborate a little bit on that and also the other ways in which Canada is collaborating with other democratic countries around the world to be able to combat this threat.

● (1545)

Hon. Karina Gould: It's interesting, this concept of sharp power. I hadn't heard that before, so I will look into that after this. If you have any information, please don't hesitate to send it.

With regard to our work in the G7, we are leading the Rapid Response Mechanism secretariat that will be hosted at Global Affairs Canada, which is looking at open source data to establish first of all, a baseline when it comes to how social media is being manipulated with regard to foreign interference in specific domestic activities, although it could also be with regard to, for example, elements of Canada's foreign policy that create spikes.

When we engaged with the White Helmets in Syria, for example, there was evidence of interference from foreign actors who were trying to polarize the debate or spread misinformation in that regard.

This is also in line with our work as a member of NATO. NATO has the Strategic Communications Centre, which is actively looking at these items. Canada hosted NATO StratCom in the fall and provided an opportunity for our media partners to engage with them and to learn about some of the foreign interference activities that have taken place. NATO does this in all of its member countries, and it's open to the media to participate, should they be interested.

We're also a member of the Five Eyes, and as such we share information with regard to foreign threats and interference into our democracies. This is something that we, as western democracies and like-minded countries, talk about quite a lot. I have personally had conversations with counterparts in France, the U.K., Germany, Ukraine, Latvia, Australia and the list goes on and on and on, because this is something that all of us are taking very seriously. We've seen, time and time again, different instances in which there has been evidence of foreign interference in the elections of like-minded countries and allies.

That being said, we're still assessing the impact of that interference.

Ms. Anita Vandenbeld: Our committee has heard a lot of testimony, as you know, about the ways in which data aggregators have influenced social media platforms, specifically in Brexit, but also in the U.S. election.

I notice that you have put in place the critical election incident public protocol. What would have been the impact in those countries or some of the others you mentioned, such as Ukraine or India, if something like that had been in place? I know it's hard to say, hypothetically, but in what ways could that have mitigated some of the things we saw happen?

Hon. Karina Gould: Well, actually, I think we can point to a very real situation that is not hypothetical, in that we looked at allied countries and like-minded countries around the world to see what mechanisms they had and have in place.

What stuck out for me was the French example of the Conseil d'État, which weighed in when there was a leak from the Macron campaign to basically say that it was a threat against their democracy, and they advised the media not to report on it.

That's a step further than what this is anticipating. We tried to come up with something that would fit within the Canadian context. The Conseil d'État in France has been around for a very long time. The idea was to avoid the kind of bureaucratic gridlock that we saw, for example, in the United States in the 2016 presidential election, and to avoid having one individual law enforcement agency going out and saying something, and to try to create a process, and to announce that well in advance so that Canadians could understand the process that would lead to such an announcement, should it occur. The hope, of course, is that it won't occur and we won't need to use it, but it's always better to prepare and plan for the worst.

● (1550)

Ms. Anita Vandenbeld: Obviously there would be a very high threshold set for when this might be implemented.

Can you give examples of the kinds of things that would trigger this mechanism?

Hon. Karina Gould: I am cautious about doing that, because I think everything is very context-dependent, and I wouldn't want to prejudge the outcome of the panel and their decision.

However, I think it's safe to assume that some of the major incidents that we've seen around the world—for example, the Macron leaks or what the U.S. was grappling with at the time—would be things of sufficient value to inform Canadians. But, again, it will be very context-dependent, and it will be within the context of the Canadian election, which is different.

Ms. Anita Vandenbeld: Good.

In that case, my other question would be about the fact that there's multi-party involvement. What kinds of safeguards are there to make sure that this is completely non-partisan and completely neutral, and that no one political party would be able to manipulate that system?

Hon. Karina Gould: Since the CSE put out the report in June 2017, we have been meeting with all of the major political parties represented in the House of Commons to facilitate a connection with CSE so that they can provide technical advice should parties choose to avail themselves of that. We're not informed of whether that relationship carries on or not. We simply facilitate the connection and have been meeting with political parties on an ongoing basis to build that trust.

As I mentioned in my remarks, I have been very encouraged by the fact that all of the major political parties represented in the House of Commons have really been at the table with regard to this. We will also be extending security clearance to all of the leaders represented in the House of Commons as well as three of their top campaign aides, and they will be briefed on an ongoing basis.

Ms. Anita Vandenbeld: Thank you.

The Chair: Next up, for seven minutes, is Mr. Kent.

Hon. Peter Kent (Thornhill, CPC): Thank you, Minister. Thank you to the officials who are here for the second hour.

I wonder if you have had time to read, first, the interim report that this committee filed last July, and then most recently, our final report in December entitled "Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly". It dealt very closely with the Cambridge Analytica-Facebook-Aggregate IQ scandal, and associated attempts to interfere in elections in North America and Great Britain.

I wonder what your comments are on the recommendations of this committee and on previous recommendations in our review of the Personal Information Protection and Electronic Documents Act, the PIPEDA review that was done by this committee, which recommended greater order-making powers for the Privacy Commissioner and more substantial, more significant penalties for violations of Canadians' privacy, including with regard to the democratic electoral process.

Hon. Karina Gould: Yes, absolutely. I have read both of the reports. As I mentioned in my opening remarks, I thank the committee both because it's really good work and also because I think it was being done even before this became a really sexy topic. I congratulate you on that.

I would note that with regard to both of the reports, there are several items that have been addressed and incorporated, both in Bill C-76 as well as in our announcement a couple of weeks ago with regard to protecting democracy. For example, in the first report, recommendation 5 is captured in Bill C-76 as well as recommendations 7 and 8.

Hon. Peter Kent: Bill C-76 doesn't cover foreign charitable funding through the CRA.

Hon. Karina Gould: Right, but to prevent foreign funding and influence in domestic elections....Well, it's with regard to any foreign funding toward third parties or political parties or candidates.

Hon. Peter Kent: Lead now is funded by foreign charitable funds channelled through organizations like Tides Canada.

Hon. Karina Gould: I'm not sure that there's evidence of that, but that would be something—

Hon. Peter Kent: We would refer you to the testimony in this committee of Ms. Vivian Krause.

Hon. Karina Gould: Again, we have the Commissioner of Canada Elections who would be responsible for investigating that. It is not something that has come up, and I would caution against those allegations, but I do think it is important to note that in Bill C-76, which was seen at the procedure and House affairs committee—and I see Ms. Kusie here who played a substantial role in that—we were able to have significant all-party consensus with regard to banning foreign funding with regard to third parties in our elections. That has been a very productive engagement.

● (1555)

Hon. Peter Kent: With regard to the critical election incident public protocol panel, I'm wondering why there are two significant omissions there in terms of the presence of the Chief Electoral Officer and the Privacy Commissioner, both of whom have much more relevance, I believe, with regard to the protection of privacy and the protection of the electoral process. Certainly these officials are well equipped with regard to foreign hacking and foreign electronic digital interference. In view of the recommendations that the Privacy Commissioner has been making for a couple of years, I'm surprised that he doesn't have a look-in on this panel.

Hon. Karina Gould: If I may, this panel is specifically put in place to deal with foreign threats to our democracy. We have Canadian legislation and mechanisms through the Commissioner of Canada Elections and the RCMP should there be a breach of Canadian law domestically. This is specifically with regard to foreign interference in the election. I would like to read the statement from the CEO of Elections Canada who, after the announcement, confirmed that he is an officer of Parliament and not a part of the Government of Canada:

> In its preparations for the next federal election, Elections Canada has been working closely with the national security agencies and the Commissioner of Canada Elections. We rely on their expertise so we can focus on our primary objective: administering the election and ensuring Canadians know where, when, and ways to register and vote.

With regard to a matter of national security, that's where the Government of Canada and the whole-of-government approach, through this critical election incident public protocol, will come into play. However, with regard to the administration of the election, of course, the CEO of Elections Canada will remain the primary interlocutor that Canadians can trust and count on.

Hon. Peter Kent: With regard to this panel's activities in a situation during the writ period, which would involve something like the deepening SNC-Lavalin scandal—the Prime Minister's original claim regarding the media report of allegations of attempted obstruction of justice, political interference pressure on the former Attorney General—this panel, given the clerk's testimony last week and if there was successive electronic retweeting of that story, would very possibly side with the government, as you said, and bring in to some doubt the ability of this panel.

Hon. Karina Gould: I should clarify, because at no point did I say that the clerk would side with the government on something that you said just now. What is important, and what I did say, was with regard to the fact that there would be a panel of five individuals who are senior public servants. They would be notified by the heads of the relevant national security agencies.

Should those heads of the national security agencies have sufficient reason to believe that there is an incident that merits their attention, that is of sufficient value, that it would impede the ability for free and fair elections, coming from a foreign threat, this panel of five would have to make a collective decision based on consensus as to whether or not they are going to inform the public

At the same time, all of the major political parties represented in the House of Commons, their leaders and up to three of their senior staff of their choosing will receive security clearances. They will all be briefed at the same time in terms of what is going on, so that we have transparency with regard to that and so that they have all of the same information coming to them. That is a very important element of this to ensure that everyone is getting information at the same time.

Hon. Peter Kent: If there are differences of opinion between the party representatives with the recommendations of the committee, how would that be resolved?

Hon. Karina Gould: It is up to the panel to make that decision, not up to the political parties, but they will receive the information at the same time.

The Chair: Thank you, Mr. Kent.

Mr. Angus, for seven minutes.

Mr. Charlie Angus (Timmins—James Bay, NDP): Thank you, Ms. Gould, for coming today.

Who at Facebook did you meet with?

Hon. Karina Gould: At Facebook I met with Kevin Chan. I would have to get you the names of the five other individuals, because I don't remember—

● (1600)

Mr. Charlie Angus: You met with Kevin Chan who is not registered as a lobbyist, who met with numerous people in the government's office, and who is a former member working for the Liberals. Was Kevin Chan your voice?

Hon. Karina Gould: I'm sorry, Mr. Angus, would you let me speak?

Mr. Charlie Angus: I'm asking my question here, if it was Kevin Chan? We spent over a year studying this and we could not get a straight answer out of Facebook. If Kevin Chan was your source, I want that on the record.

Hon. Karina Gould: Mr. Angus, I said there were five other individuals who we met with, as well, who came from Washington and Silicon Valley.

Mr. Charlie Angus: Above or below Mr. Chan? Would you give us their names?

Hon. Karina Gould: Happily, I just don't have them right now.

Mr. Charlie Angus: Thank you.

I guess I'm a little touchy. We did spend over a year studying this. We worked internationally and domestically. I see the report that you came out with. It's so "Cold War". We have the G7 rapid response, we have the critical assessment from Borm. Everything that we found is the very opposite of what you're coming forward with.

You ignored our key recommendations, one of which was the role of the Chief Electoral Officer, who will now be under Michael Wernick from the Privy Council. However, we had said all along that the Electoral Officer has an important role to play. In the middle of an election, things get very heated. If this critical G7 rapid response team that you bring in suddenly announces a threat, it could really destabilize an election. What we would need is real confidence.

Hon. Karina Gould: It's important to clarify the roles—

Mr. Charlie Angus: We would need real confidence, right?

Hon. Karina Gould: —and not conflate different issues.

Mr. Charlie Angus: So I am wondering why you have appointed Michael Wernick to that position and not the Chief Electoral Officer to make that decision for Canadians.

Hon. Karina Gould: If you'll let me answer your question, I would be happy to.

As I literally just responded to Mr. Kent not a minute or two ago, I will repeat what the Chief Electoral Officer said—

Mr. Charlie Angus: I heard that—

Hon. Karina Gould: —which is—

Mr. Charlie Angus: —but I'm asking why Mr. Wernick is not the Electoral—

Hon. Karina Gould: —he is an officer of Parliament, and not part of the Government of Canada. He is separate from that.

Mr. Charlie Angus: Okay.

Hon. Karina Gould: When we are talking about something that is of a national security issue, it is the Government of Canada that will do that.

Mr. Charlie Angus: Okay.

Hon. Karina Gould: During an election period, we have something called the caretaker convention—

Mr. Charlie Angus: Right.

Hon. Karina Gould: —that takes over to ensure continuity of government. It is important that—

Mr. Charlie Angus: Yes, I understand that. My concern is—

Hon. Karina Gould: —political actors are not compromised on that.

Mr. Charlie Angus: —that I share Mr. Wernick's concern about the rising tide of political extremism but I was very surprised that he suggested political assassination in the midst of a parliamentary hearing on whether the government had done wrong.

Do you not realize that would breach the rules for the Privy Council that they're not to wade into matters of conjecture and controversy? Yet he started out an answer to the panel about whether or not the government was involved in interfering with the rule of law, and he related it, not just to political assassination, but he said:

> I worry about the reputations of honourable people who have served their country being besmirched and dragged through the market square. I worry about the trolling from the vomitorium of social media entering the open media arena. Most of all, I worry about people losing faith....

Is that the position of the government, or is that his opinion?

Hon. Karina Gould: You would have to ask him that question.

Mr. Charlie Angus: Okay.

Hon. Karina Gould: That was his personal view, is my understanding.

Mr. Charlie Angus: Okay.

Because under the guidelines for the Privy Council officials—and I think your people beside you have read it—I quote, "Officials may give explanations in response to questions having to do with complex policy matters, but they do not defend policy or engage in debate... In other matters, principally those having to do with the administration of the department and its programs" must be strictly limited. "Matters of policy and political controversy have been reserved...exclusively for Ministers, principally because political answerability on the part of officials would inevitably draw them into controversy, destroy their" political "utility to the system and, indeed, undermine the authority and responsibility of their Ministers."

My concern is that Mr. Wernick, using a committee hearing to advance all manner of personal political conjectures—number one about how ethical the Prime Minister is; number two, how amazing Ms. Bennett was; number three, how terrible it was that people criticized her on Twitter—used his position to advance an agenda, which is destroying his utility as someone we can all look to and say, "You know what? In a matter of real political tension, we can trust him."

Do you not see that?

Hon. Karina Gould: Someone who has the oversight of the entire government and operations will clearly have a unique position in terms of how they are feeling and the threats that they can see arising on the horizon.

I think one thing that is very important is to recognize that in developing the critical election incident public protocol, we were deliberate in bringing together a panel of five senior public servants so that it would not fall on one civil servant to make that decision—

● (1605)

Mr. Charlie Angus: And I would not have had anything to say about Mr. Wernick before his testimony—

Hon. Karina Gould: —and to have a conversation and weigh those issues.

Mr. Charlie Angus: —but, given that he has very strict obligations as the chief of the Privy Council about what he can give opinions on, yet he said about Madame Bennett, "I am deeply hurt that...her reputation has been trolled.... There are vile things being said....there is no Canadian who has worked harder on indigenous reconciliation than the Honourable Carolyn Bennett..."

That may or may not be, but the people who have been challenging her on Twitter are indigenous grassroots who do not support her position. So if he thinks it's vile, my concern is that, when people say very controversial things in an election, and people will, and when people attack us and they attack government, at what point can we trust that Mr. Wernick will know the difference between what is fair and what is unfair criticism?

The fact that he has waded into matters of controversy in ignoring his obligations, to me, puts him in question, whereas I have no questions about the Chief Electoral Officer, but I certainly have questions about this incident team you have with Mr. Wernick.

Hon. Karina Gould: I will just reiterate, Mr. Angus, that the panel we've put together will not come together unless the national security agencies raise an issue of national security for them to consider, which they think—

Mr. Charlie Angus: Wouldn't it be better for the Chief Electoral Officer to say yes, this is serious, whereas Michael Wernick seems to think that people attacking government ministers is beyond the line —

Hon. Karina Gould: So the response again is that the role of the Chief Electoral Officer is as an officer of Parliament and to administer the elections.

Mr. Charlie Angus: Thank you.

Hon. Karina Gould: This is a separate issue and a separate role that they have.

With regard to the panel, it is extraordinarily important to reiterate that they will only come together should one of the heads of the national security agencies deem that they have seen foreign interference of a significant level to get them together to inform—

Mr. Charlie Angus: We need the public to have a confidence, and that's my question. If Mr. Wernick crossed the line in his Privy Council obligations, do we have that trust? I'm not sure that trust exists right now.

The Chair: Thank you, Mr. Angus.

Next up, for seven minutes, we have Mr. Saini.

Mr. Raj Saini (Kitchener Centre, Lib.): Good afternoon, Minister. Thank you very much for coming here this afternoon, especially with your colleagues.

I want to start off with a question on one of the pillars that you mentioned, expecting social media platforms to act. I know you have been in discussions with them regarding transparency and making sure that the people who advertise or pay for advertisements, and we know who they are...to combat the propagation of misinformation.

However, there is one point I want to ask you about, if there is something your department or some of the officials here could comment on. Sometimes, whether it be on Reddit or Facebook, there's a comments section. Sometimes there can be an infiltration by foreign actors or by others who want to disrupt the election mechanism we have here, where they can insert misinformation or disinformation within the comments section. Is there some protocol we are looking at to prevent that from happening?

Hon. Karina Gould: We are not looking, as a government, to intervene in the conversations that are happening on social and digital platforms. That is not the role of the government.

However, we expect that social media platforms will take an attitude and actions that are more responsible in terms of how their platforms are used to spread misinformation and disinformation.

Obviously, that is more complicated if you're looking at the comments section as opposed to a post. However, what we do expect is for them to take down inauthentic behaviour and inauthentic accounts. We have heard from both Twitter and Facebook about the number of accounts they have taken down. Both are in the realm of millions, and I could get you the specific numbers that we've heard if you're interested. I'm not entirely aware of the mechanism by which either of those platforms would go after the comment section, whereas if they go after the account that is a fake account or is known to be from a foreign source and posing as a legitimate domestic actor, that may get at this issue.

Mr. Raj Saini: You talked about the rapid response mechanism with the G7. I don't know the content of the sharing agreements, but obviously they are to make the system more robust for all of the G7 countries. I'm not necessarily worried about that because I think there are enough resources within the G7 to create a system that's robust.

My worry is more with nascent democracies or even going beyond the G7 to the G20. Recently there were elections in Nigeria and there has been some speculation that there has been foreign interference. There has been foreign interference prior to this election in Nigeria. You mentioned some other countries.

If you make the G7 strong, that's great, but it doesn't really do anything else for the democracies in the rest of the world. Has there been any thinking in the government, on your department's part, that whatever best practices or robust practices you have would be shared with other countries that may not have the same resources or the same capacity as we have in this country?

● (1610)

Hon. Karina Gould: My focus has really been on Canada's democracy. When I have had conversations with foreign counterparts they have really been about learning from their experiences to see what we could glean and apply here in the Canadian context.

I will say that apart from the European Union, Canada is leading the way in terms of protecting our democracy from foreign cyber-threats. The elements we announced on January 30 really set the stage for that.

That being said, I know there are efforts to ensure that whatever we learn is being shared with counterparts and allies. I've heard from many other countries that they're looking to us as well in terms of what we do and how they might apply that in their own jurisdictions.

Mr. Raj Saini: My final question is more of a personal question. As you know the election campaign is coming up and there may be things that are said on social media about certain candidates, true or untrue. What's the mechanism to resolve something that is untrue?

Hon. Karina Gould: In Bill C-76 there was a tightening based on the recommendations from the former CEO of Elections Canada to tighten the language surrounding false statements made against candidates. The previous clause in the Elections Act was too vague and unenforceable. We tightened it up, so it would be based on statements you could prove or disprove.

For example, if someone accused candidate X of having a criminal record, that's something you could prove or disprove. The mechanism, with regard to our elections legislation, is a complaint filed with the Commissioner of Canada Elections to which it would then respond.

The resources to the commissioner have been increased. Another very important element of this is that the commissioner has been both moved back into Elections Canada, but also empowered to initiate and lay charges as well as compel testimony. The powers have been strengthened, so the commissioner can be more effective in applying our legislation.

Mr. Raj Saini: One of your pillars is enhancing citizen preparedness, because the more education citizens have, the more robust the system will be. There will be less ambiguity. You mentioned something in your opening comments about creating a digital citizen initiative.

Can you give us a little background on what that is?

Hon. Karina Gould: One of the pieces of advice that is probably the best that I've heard, but also the most relevant, is that when we're talking about cyber-threats to our democracy, ultimately, the target is the citizen. Around the world, our counterparts have highlighted the fact that a resilient citizenry is the best tool with regard to fighting back against misinformation campaigns.

We announced $7 million for our digital citizenship initiative that will provide funding to civil society organizations in the realms of digital media and civic literacy. This is an extraordinarily important initiative. Over the past couple of years, particularly with the 2016 U.S. elections, it was a bit of a wake-up call to western democracies that we were taking our democracy a little bit for granted. It's important to ensure we continue to talk about democracy and democratic values in our own country, otherwise we could stand the chance of losing them.

The Chair: Thank you, Mr. Saini.

Ms. Kusie.

Mrs. Stephanie Kusie (Calgary Midnapore, CPC): Minister, it's always lovely to see you. I love that necklace by the way. It's just beautiful.

Hon. Karina Gould: Thank you.

Mrs. Stephanie Kusie: Also, I want to say that I really enjoyed your speech yesterday at the AI event. It was very informal. I think you should go with that format more, even when you come to committees. You do it so well. I wanted to compliment you on that.

You talked a lot about vulnerabilities. That was a major theme for you. Of course, as the opposition, we very much take seriously your responsibility to hold the government to account, in terms of safeguarding the election. I would say that at almost every step, we feel as though the government has failed, and not gone far enough in taking the steps required to safeguard the election.

I would use examples from Bill C-76.

The social platform registry, the most basic of information, in my opinion, didn't perhaps go far enough, in terms of protecting Canadians and providing information, as well as data management.

My colleague made mention of the foreign interference aspect. I've said this several times before. We, as the official opposition, put forward over 200 amendments. Many of them were rejected. As I have said previously, I feel very strongly that what we came out with in Bill C-76 was a slap on the hand for foreign interference. You know, "This is bad. You shouldn't do this," rather than legislating specific mechanisms, such as segregated bank accounts, which would make foreign interference impossible, from a monetary perspective.

More relevant to what my colleague, the Honourable Peter Kent, mentioned, is the funding outside of the writ and pre-writ periods, which is really still open season. It is, as we've come to see, severely affecting other parts of our democracy, including both immigration and—something very dear to my heart, as an Albertan—pipeline approval.

That's just the beginning. I certainly won't go into our positions, in terms of the vulnerabilities created by non-resident voting, voter identification cards and the changes to vouching in Bill C-76. This is something you've said is very important to you and the government. Yet we see that the steps to absolutely go to the furthest length possible to protect these electoral processes are not being taken. It was touched upon yesterday. My colleague, Mr. Saini, mentioned it briefly in his questioning earlier. It was mentioned by a former member of the Liberal government and the Liberal cabinet, someone I have much respect for and who is a former colleague of mine from foreign affairs, Allan Rock. It was in regard to, again, the management of social media platforms.

Of course, we are always looking for a balance in society. As I stated in my testimony at PROC last week, we have to rely on these corporations, with the objective to maximize shareholder value, to take it upon themselves to self-regulate. I understand that opens up questions such as free speech, etc. He did mention a concern that perhaps more than nudging needs to take place. My concern is also with your response, or what seemed to be your response. I'll give you the opportunity to address that. You seem to want to put it upon PROC to do a study, giving you coverage if you decide to take action with legislation, you can say, "Well, the committee did a study, and this is what they told me."

I'm asking you if you are ready and willing, in regard to the social media platform, to make the hard decisions and take the hard actions, not six months from now, but now, please.

● (1615)

Hon. Karina Gould: Thank you, Ms. Kusie. I do understand that you actually put a motion forward at PROC to study this issue.

Mrs. Stephanie Kusie: I did.

Hon. Karina Gould: Yes, so that committee would make that decision.

One thing I want to clarify, because this is the second time you've mentioned it, is in Bill C-76 third parties are now required to have separate bank accounts so they can account for all the money coming in. I think that was a really important issue to put forward, particularly to account for where money is coming from.

With regard to the vulnerabilities that I mentioned yesterday and often on this topic, you can pull those directly from the CSE report on cyber-threats to our democracy. They highlight very clearly that the principal threats with regard to cyber-interference are with regard to people mostly: politicians, political parties and the media, any time there is human interaction. As often is the case, those individuals and actors on the one hand may not be practising what is called good cyber-hygiene two-factor authentication and ensure they're protecting their accounts as well as possible, but also with regard to being susceptible to influence strategies and campaigns. When talking about those vulnerabilities, those are the ones I was referring to.

With regard to Bill C-76, on the whole I'm quite proud of the legislation because I think its primary objective is to ensure that all Canadians have the possibility to vote. I think that was really important in extending vouching for our most vulnerable Canadians, in ensuring that the voter information card can be used to establish residency, which we know, for example, for single senior women, is often a barrier to voting because they don't have those pieces of residence information.

● (1620)

The Chair: Thank you, we're past time.

Next up, for five minutes, is Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thank you for being here, Minister.

Our committee has recommended imposing a duty on social media platforms to remove manifestly illegal content in a timely fashion, including hate speech, harassment and disinformation, or risk monetary sanctions. I want to read a comment. This was in response to a media article about the hate and threats from the yellow vest movement. Interestingly, I think if they knew that the yellow vest movement in France was calling for a wealth tax, minimum wage, maybe they wouldn't associate with the yellow vest movement so much here in Canada, but they called Mr. Trudeau a "traitor to our country" who deserves to be "hung for treasonous crimes". That's posted on Facebook; that was left on Facebook; Facebook doesn't take it down, so should we expect social media companies to act or should we require them to act?

Hon. Karina Gould: I should clarify that my expectations have to fall within the electoral context at this point as I'm Minister of Democratic Institutions. However, that being said, I think we are moving in a direction where we need to require social media companies to act. That is outside the scope of my specific mandate right now, but I think that when we have very clear evidence that they are contravening laws here in Canada, they should be acting responsibly in that manner.

Mr. Nathaniel Erskine-Smith: I appreciate that. So within your mandate, we have Bill C-76, which rightfully creates a registry of ads, both in the writ and pre-writ periods. Is there any confidence in the conversations you've had with Facebook and others that they will ensure that database is as accessible as possible, with journalists in mind specifically?

Hon. Karina Gould: I have had that assurance from Facebook. I know all the social media companies are also looking to speak with Elections Canada to get clarification because Elections Canada ultimately will interpret the law and determine how that is, but my understanding is that they're trying to make that accessible and available to Canadians.

Mr. Nathaniel Erskine-Smith: With respect to Bill C-76, the focus is on transparency of advertising and that's really important, but there was an interesting comment when Mr. Zimmer and I were in Washington last July for a round table. Senator Warner said when they started looking into this issue, advertising was their main focus and that turned out to be the tip of the iceberg. The hijacking of the algorithms themselves was the real problem, whether it's the Internet Research Agency troll farms, or some other organizations. How do you see the steps that your office has taken as a solution to that problem?

Hon. Karina Gould: I've read Senator Warner's report as well. It's very interesting in this space, and probably one of the better reports I've read.

I tend to see the steps we've taken as steps to address the problems we've identified so far, understanding that this is an evolving field and that our understanding of the issue continues to grow.

In terms of full disclosure, as the minister responsible for this portfolio, I will say that when I came into it, I was thinking about hack and leak attempts. Over the course of the past two years, our understanding of the issue has changed dramatically. Right now, as an international community but also here in Canada, we are trying to understand the depth and breadth of the issue and come up with solutions that will attack the core of the problem. That's where I thank the committee for doing the work you've done, because it's really important in informing next steps.

● (1625)

Mr. NathanielErskine-Smith: You mentionedhacks. I readthe CSE'sthreatassessmentreport. I understandthere might be a new one forthcoming, but I read the last one. It said that the electoral systemhas great integrity, and that it was not so worried about ElectionsCanadaor the voting systembeinghacked,but thatit's the political actorswho are the greatweaknessin this. We've seenMPs and senatorsalreadyhacked,as far as it goes.

Therefore,when I look at $7 million for a digital citizenship initiative and I think of $7 million spentacrossthe country,how are we actuallygoing to educateCanadiansbetweennow and October? Wouldn'tthat$7 million for trainingandeducationpurposesactually be betterallocatedto educatingpoliticians,political staff, volunteers andriding associations,and to makingsureI get the training that I, my staff and my volunteersneed to make sure we prevent our accountsfrom being hacked?

Hon. Karina Gould: Thereis an issueof parliamentaryprivilege with that, in termsof the fact that Parliamentgetsto decidewhat informationyou chooseto useandnot use.In the announcementwe put out a seriesof infographicsandeducationaltoolsthat I invite any parliamentarianor Canadianto useandlook at in orderto seehow bestto protectthemselves.

The cyber centreof the CSE, which André can speakto a bit afterward,is stoodup but will be availablefor parliamentarians,as well as politiciansand their political entities,shouldthey chooseto useit, and we will be reinforcingthe "get cybersafe" campaignas well, so we all have a bit of ownershipand responsibilityto make surewe are demonstratingleadershipin this area.

That beingsaid, you can practisethe very bestcyber-hygieneout thereand still be a victim of a hack.

The Chair: Thankyou.

Just for the room, we have three more questionersto ask questions.We starteda bit late;hopefullythat'snot a problemfor the minister.

We'regoing to go to Mr. Gourdefor five minutes.

[*Translation*]

Mr. JacquesGourde (Lévis—Lotbinière,CPC): Thank you, Mr. Chair.

Thankyou for being here,Minister.

Canadianswill no doubt be very concernedby what we have heardaboutthe digital threatsFacebookgenerates.What we heard duringthe latestelectionin UnitesStatescould certainlyalsohappen in Canada.

It is difficult to deal with or reportthis infamousadvertisingand fakenewspublishedon Facebook,andit takesso muchtime. A new advertisementon Facebookcan make the headlinesfor 24 or 48 hours,evenif it is completelyfalse,regardlessof the partybeing attacked.Afterwards,it will be declaredas false, but the newshas alreadyspreadthroughoutthe public or has alreadysweptits way into Canadians'minds.If that happensrepeatedly,we may well have a task force saying that it is wrong to do that, but it will not be enough.

How will it be publicly announcedthat thoseare fake newsor falseallegationsin the media,suchas Facebook?

Hon. Karina Gould: As I said,I don'tthink it is the government's role to decidewhich newsis fake and which is real. That is a 21st centuryproblem.We are living in a mediaworld wherenews travelsvery quickly. I think that traditionalmediaalsoplay a role in ensuringnot to reportfake news.In addition,of course,politicians havea platformto saywhat they think. Ownersof digital platforms also have a responsibility to ensure the platforms are not manipulated.

I am an eternaloptimist,but I'm alsoa realist,andI wantto point out that, during the United Statespresidentialelection, those in chargeof digital platformsdid not to try to disclosethat type of manipulationand activities.At least,they are doing it now and are trying to avoid that kind of abuse.Of course,that is insufficient. They could do more,but at leastpeopleare moreawareof that type of misinformation.As I alreadysaid,this is not the solution,but one of the things that could be done would be to educateCanadians aboutthosethreats,so that they can makeinformeddecisionswhen they watchthe news,be it real or fake.

● (1630)

Mr. JacquesGourde: Is it the role of Elections Canadato undertakea public awarenesscampaignat the beginning of the election campaignto educateCanadiansabout that reality, to tell themto be especiallycarefulaboutit andto reportit if they hearfake newsor feel wrongedby what is happeningin socialmedia?

Hon. Karina Gould: That is an excellent question. Since ElectionsCanadais an independentgovernmentorganization,that may be a questionfor the chief electoralofficer. However,I can say that, in Bill C-76, we have given back the power to the chief electoral officer to inform Canadianson elections. If that is something that interestshim, he could talk to Canadiansaboutit.

Mr. JacquesGourde: It is clear that the next electionwill be crucial. In this new media environment,we will all follow things closely, at least as a legislator and political players. Should we prepareto take actionfollowing the 2019election?

Hon. Karina Gould: I think that,afterthis election,we will have to analyzewhat hashappened.The CSE'sreport,which I mentioned, should be updatedafter this election.An analysiswill be done of what has happened.I think it would be really appropriateand importantfor Parliamentto reviewthis.In addition,I assumethat the Chief ElectoralOfficer will producehis reportafterthe next election and, as he does after every general election, he will make suggestionson waysto improvethe country'selectorallegislation.

Thankyou.

[*English*]

The Chair: Thankyou.

Next up, for five minutes,is MadamFortier.

[*Translation*]

Mrs. Mona Fortier (Ottawa—Vanier,Lib.): Thank you very much.

[*English*]

Thank you, Minister, for being here today and for sharing the information that you did. I might repeat myself, but I know that you have probably more to share with regard to the question I have.

[*Translation*]

We are very serious about the work done to protect our election against outside threats and interference. As you know, we have looked at the violations committed, including by the Cambridge Analytica firm and Facebook. For several months, members of this committee have been studying the situation in depth in collaboration with parliamentary committees from around the world; this is an important step. Our committee has focused on doing this in a non-partisan way, knowing that the repercussions on our electoral system are a major source of concern for Canadians.

[*English*]

How sure can Canadians be that combatting interference from foreign actors, be they quasi-governmental or individuals working alone, is a priority for our government?

Hon. Karina Gould: They should be very assured that this is absolutely a priority. This is something on which I have been working in terms of a whole-of-government approach. The announcement it made on January 30 brought together the ministers of defence, public safety, heritage, ISED and justice. In many respects, this is something an ADM working group is looking at. The topic for which I was invited to come, the SITE task force, brings together CSIS, CSE, RCMP and Global Affairs Canada to really ensure that the whole-of-government is taking this matter seriously, because there is nothing more important than our wonderful democracy that we have here in Canada.

● (1635)

[*Translation*]

Mrs. Mona Fortier: The committee would like to better understand how, if interference was detected during the election, public servants could alert Canadians of the consequences of such interference. Can you explain to Canadians how that process would work?

Hon. Karina Gould: Of course.

As I mentioned, we have the Critical Election Incident Public Protocol. I think we have given the committee the infographic documents available on our website. According to that process, national security agencies that learn of an incident would inform the group made up of the following five senior officials: Deputy Minister of Justice and Deputy Attorney General of Canada, Deputy Minister of Global Affairs Canada, Deputy Minister of Public Safety, National Security and Intelligence Advisor, and Clerk of the Privy Council. Those senior officials would have to decide together whether it is worthwhile to inform Canadians of the incident. That group's intervention threshold would be very high and limited to incidents compromising our ability to have free and fair elections. If Canadians receive a message from that group, it would be because real foreign interference is impacting the election.

Mrs. Mona Fortier: I have one last question for you. Do you think penalties should be imposed on those who interfere in the electoral system?

Hon. Karina Gould: The Minister of Foreign Affairs will have to make that decision. Of course, the Canada Elections Act already stipulates that foreign interference in the election is illegal. Collusion between a Canadian player and a foreign player is also illegal. In such cases, the Commissioner of Canada Elections and the RCMP would have to intervene.

Mrs. Mona Fortier: Okay, thank you very much.

[*English*]

The Chair: Mr. Angus, for three minutes.

Mr. Charlie Angus: Exactly one year ago the Prime Minister issued a very stern statement to Facebook. He told them to clean up their act or we would regulate them. Then that never happened. Our committee then began our study, which really brought us down the rabbit hole of some really dark operators. I feel a real disconnect when I hear how we're talking about foreign actors, and foreign players and foreign countries; it seems jamming the phone lines on election day, when from what we've seen, it could be two guys above an optometrist's shop, with good data sets and the ability to switch and turn votes—100 here, 50 there—who could actually dismantle the democratic system.

When we met with 17 jurisdictions around the world, they all expressed their frustration about the unwillingness of Facebook to take any responsibility. In fact, our sister committee in the U.K. has called them "digital gangsters".

Yesterday the Toronto Star did an editorial that read, "Ottawa should stand up to Big Tech on privacy and democracy". It read, "Yet our government seems uncertain, even paralyzed in the face of the multiple challenges posed by the tech giants.... The United States...and...Europe...taking strong action to counter some of the worst effects of Facebook....yet Ottawa seems...content to sit on the sidelines." That's not me saying that; that's the Toronto Star, yesterday presumably after it got to see your report.

I have two quick questions. One, what assurances did you get from Facebook that nobody else internationally seems to have gotten? Number two, to reiterate, will you give us the names of whoever you spoke to at Facebook so we can invite them to see what kinds of reassurances the Canadian people will get?

● (1640)

Hon. Karina Gould: Mr. Angus, as I said in my last response to you, I will happily give you the names of the individuals. I just don't remember them off the top of my head, but we will get those to you.

Mr. Charlie Angus: I know. That's perfect.

Hon. Karina Gould: With regard to regulating social media, I actually do want to clarify that in fact I did regulate them through Bill C-76, through the online ad registry that they will have to comply with in the upcoming election. I think that is a really important step, and it's the first time, to my knowledge, that this has happened internationally.

With regard to assurances from Facebook, I don't have the assurances that give me full confidence that they are going to be completely seized with this and doing everything necessary, which is why I continue to have conversations with them, and have highlighted—

Mr. Charlie Angus: Why are we having conversations with them about our democratic system? That's my concern. If you're not completely satisfied, then I'm really not satisfied, because you're meeting with them.

Why are we tiptoeing around with a company that has shown such manifest disregard for undermining elections around the world? Why are we not talking about serious consequences, like the ones Germany is moving forward to, like the ones Europe is talking about? Do you not believe that our election system is still compromised by the ability of third party actors, domestically, to flip that Facebook platform because Facebook simply will not live up to its obligations?

Hon. Karina Gould: I think it's important to look at the strength of our electoral legislation and to recognize that in Bill C-76. That's why we put in the provision about the malicious use of a computer and how that is not allowed to happen. We do have a strong electoral system and strong legislation here in Canada. We have also strengthened the rules with regard to third parties, in terms of advertising, in terms of how they disclose their finances, which I think is really important.

I have confidence in our elections legislation domestically.

Mr. Charlie Angus: But that's still not Facebook.

Hon. Karina Gould: I still need to see more from the social media companies. That's why I am engaging with them and making demands of them, and I will be completely transparent with Canadians about how those go. I would be happy to have further conversations with you on this, because I think it is of the utmost importance.

Mr. Charlie Angus: Thank you.

The Chair: I have a couple of comments for the minister, just before we close. The phrase that came to me before, when I saw the legislation, Bill C-76, was that we are bringing a knife to a gunfight. In reality, we're not even bringing a knife; we're bringing a panel to a gunfight.

The concern is around how, especially with some very clear recommendations in our report, 26 very clear recommendations that were very specific, we see very few of those being taken up by the minister. What has been talked about here in committee as a whole is that if expecting that social media platforms will act is your final point, isn't that supposed to make them treat it more seriously?

I'll just refer you to a quote from the Information Commissioner from the U.K., which was later reiterated by our own Privacy Commissioner. "I think the time for self-regulation is over," Denham said. "That ship has sailed." I guess I just wonder—and this is for the minister—why we still let them self-regulate and expect them to do the right thing when they haven't, up to this point.

I guess what I'm concerned about, what I think all at this committee are concerned about, is that, as has been mentioned before, we're in a Cold War—the Cold War reference was brought up—but we're in a digital reality and we're still treating it like a Cold War problem.

With those comments, do you think you're doing enough?

Hon. Karina Gould: I would say that for many of the elements in both of your reports that have to do with elections, you can see those reflected, not entirely, but fairly closely, in both Bill C-76 and the announcement that we made with regard to protecting democracy.

On some of the other elements that are outside of my mandate, I will note that my colleague Minister Bains is conducting public consultations and will be coming out with a report specifically with regard to privacy and data and how companies use that. My understanding is that will be in the near term.

As I have said many times before, this is one of the great challenges we're facing right now. We have in many ways for a long time looked just at the tremendous benefits that social media and the digital world have brought us. I think 2016 was a real wake-up call for everyone around the world in terms of what was going on.

As in many moments in history, we now have to figure out exactly how to tackle this problem in a way that, on the one hand, continues to encourage the positive elements of social media—the ability for people to connect in ways they've never been able to connect before; the great democratizing abilities that it has in terms of sharing opinions and views, which I think is extraordinarily positive—and, on the other hand, mitigates the risks and the social harms that we see happening.

One of the things I have thought about over the past two years, the last year in particular, as a lot more of this stuff has come to light, is the fact that there have been very few times when we've had one industry that is so encompassing in so many aspects of our lives that it's difficult to attack it from just one position, whether it's democracy, privacy, public safety, law enforcement or whatever the case may be. We need to start thinking a bit more holistically about these digital giants and how we approach them.

That's where I think the work of your committee has been very helpful in terms of helping us think about some of these issues and how we manage them in a way that aligns with our values and our societal norms moving forward.

● (1645)

The Chair: Thank you, Minister.

We'll suspend for just a few minutes while you make your exit, Minister, and then we'll have the other presenters in the last hour.

Hon. Karina Gould: Thank you for having me.

The Chair: We'll suspend.

● (1645)

(Pause)

● (1645)

The Chair: I will call the meeting back to order.

First, we have a point of order from Mr. Angus.

Mr. Charlie Angus: Mr. Chair, I just want to put a concern of mine on the record. From our meeting last week with Waterfront Toronto, we received two forms of correspondence. One was an official letter from Jim Balsillie in which he said that the parliamentary secretary had lied about what he said and was misrepresenting facts, and he wants to set the record straight.

We also received correspondence—I don't believe we got the letter—from Julie Di Lorenzo, who said that false statements were made.

I am concerned. We've been approaching all our work in a very particular way. I'm worried about turning this into a battle between Mr. Vaughan and Mr. Balsillie, but I think Mr. Balsillie has a right to appear. I also think that Julie Di Lorenzo, if she said false statements were made during that hearing, should be allowed to speak as well.

We just need to find a format to make it work so that they can present, and we can get to this and then move on.

● (1650)

The Chair: Yes, I'll speak to this.

The letter was received by the chair, and I believe we're just waiting for it to be translated. Mike has just said it should be ready by tomorrow afternoon.

Further to that, we have invited Mr. Balsillie to come back to speak to the committee. He's not able to come Thursday, so we're looking for a date when he is able to come back. Based on conversations I have had with the vice-chairs, I can say that's already been done.

It's just the letter to the committee that's outstanding, and it will be coming tomorrow.

Mr. Charlie Angus: There's also Ms. Di Lorenzo, who I believe may have been on the real estate committee or had something to do with Waterfront Toronto. She said she was getting her lawyer to work with her on a letter, so I would like us to reach out to her in terms of whether we will be getting an official letter or if she will make a statement.

I want clarity in terms of what happened with testimony.

The Chair: Yes, the chair can do that. I'll just make sure the analysts have that request.

Mr. Maxime-Olivier Thibodeau (Committee Researcher): Sure.

The Chair: Perfect.

There is no presentation from the group, so we're right into questions.

I'll give the first seven minutes to Mr. Erskine-Smith.

Mr. Nathaniel Erskine-Smith: Thanks to new witnesses and to witnesses we've had before.

Specifically for CSE, as a starting point, I've read a previous threat assessment. Has anything changed since that threat assessment that we should know about?

Mr. André Boucher (Assistant Deputy Minister, Operations, Canadian Centre for Cyber Security, Communications Security Establishment): The publication of the update to the threat assessment is imminent. It's providing my team the time necessary to also build the advice and guidance that's focused and targeted to the elements of that report. I'd hate to pre-publish the report today, but I would assure you that we're not waiting for the report's publication to take action on the elements of it that we're already aware of.

By "imminent" publication, I mean probably days—weeks at the most.

Mr. Nathaniel Erskine-Smith: The minister said she was sitting down with social media platforms. From the security side of things, how much do you work directly with social media companies to ensure that their platforms are not being hijacked?

Mr. André Boucher: From a cyber centre perspective, the presence of the ecosystem...are all companies. My concern starts with the equipment we all use, the software that's on that equipment, and the way we interact with that equipment in those networks.

From my perspective, social media companies are one element of that complex ecosystem, and we treat them just the same. We engage with those companies and have the same expectations of their practices in cybersecurity measures and of their behaviour and responses in the ecosystem. This is similar to what other companies would have, from the device companies to the operating system or applications that ride on top.

Mr. Nathaniel Erskine-Smith: Would you share our committee's concerns with respect to hateful content, inflammatory content and content that incites violence, which stays on these platforms and is not appropriately dealt with in a timely fashion?

Mr. André Boucher: It is not the focus of the cyber centre to analyze or make comments on the information carried by computers, emails or social media content, but we expect all companies to behave as good Canadian citizens and be mindful of their presence and their responsibilities in that presence in Canada.

To get away from social media for a second, if a software company wasn't behaving as a good corporate citizen, we would have just as much of an objection with them.

Mr. Nathaniel Erskine-Smith: Sure. I always find it funny that Facebook is reliant upon free speech. I'm a great defender of it and I don't think people should necessarily be thrown in jail for saying absurd, ridiculous things. However, the idea that they can say these things on the Facebook platform and not have them taken down begs a question as to what community Facebook actually wants to build.

With respect to hijacking algorithms specifically, and let's use the Internet Research Agency as an example, they'll have a number of not just bots but people managing a number of accounts to amplify a particular message. Often, it's a message of disinformation or misinformation. Is that something your organization is seized with?

● (1655)

Mr. André Boucher: We certainly start a conversation with, "I expect all products in my ecosystem to be of the best quality possible," so if we were to observe or someone was reporting to us that there was something not right with the software or the hardware, would we investigate and try to get to the bottom of the story? Absolutely, and we would absolutely do something with the company, but there's also an opportunity in the foreign space, which I'll let Dan answer.

Mr. Dan Rogers (Deputy Chief, SIGINT, Communications Security Establishment): From the foreign intelligence perspective, we're looking at foreign actors outside of Canada and what their intentions might be toward Canada. One of the things we can do to help inform the cyber centre or help other elements of the Government of Canada to respond is to see those foreign actors. If we can identify what behaviours they're taking—if we can see their online infrastructure or the types of botnets or techniques they may be using—that will be an edge we can provide to the cyber centre and to other people in government who, within their mandates, can respond.

Mr. Nathaniel Erskine-Smith: Is there anything the platforms can do that they are not currently doing to combat this problem of hijacking algorithms?

Mr. André Boucher: The information would come to me from that team. We've never hesitated to engage with companies, domestic or foreign, regarding the quality and behaviour of their devices or software. We would do exactly the same in this instance.

Mr. Nathaniel Erskine-Smith: I mentioned the yellow vest movement, and I read a hateful comment that was an incitement to violence. There are many, obviously, that you can find across the Internet if you can bear to go to the comments sections.

We heard testimony from Michael Wernick that he was very concerned about violence in the upcoming election. Does it go beyond those sorts of online comments? Are there real, credible threat assessments, and should we be concerned that there is to be violence in the upcoming election?

Mr. Dan Rogers: What I can say, from the national security and foreign intelligence perspective, is that, although a lot of what we've talked about today is in the cyberspace of course we look for threats of all kinds that might be directed toward Canadians, whether that's terrorism, cyber-attacks or other types of malign foreign activity that we might see perpetrated against Canada or Canadians. In that space there are existing mechanisms. This isn't a new challenge for us. If we see those types of things, we'll report them. CSIS, the RCMP and others have the mandate to investigate those within Canada should they occur. The intelligence function that we and others will have will provide them with any information we see, so if it comes up we will be vigilant and we'll make sure they have that information.

Mr. Nathaniel Erskine-Smith: Mr. Sutherland, I don't know if you can speak to Mr. Wernick's comment and maybe give us a bit more detail. Is it based on just social media commentary and how nasty it tends to get or is there a real threat at issue here that the comments were in relation to?

Mr. Allen Sutherland (Assistant Secretary to the Cabinet, Machinery of Government and Democratic Institutions, Privy Council Office): I think Mr. Wernick was speaking from a personal view. He started his comments that way. I would say the worry that he expressed is one broadly shared by people who look at issues around social inclusion, not just in Canada but around the world.

Mr. Nathaniel Erskine-Smith: The last question I would have is with respect to digital education outreach initiatives. We know there's $7 million. An open question is how effective we can be in a short period of time to educate Canadians about misinformation or disinformation on the Internet. In the experience of the CSE, knowing that political actors like ourselves are a weak link, as it were, do you think the funds would be better spent to ensure that volunteers on our teams, our riding associations and those involved in campaigns, including ourselves, are doing everything we can to ensure we're not hacked and we're not vulnerable?

Mr. André Boucher: I will address a bit of that. The $7 million announced are incremental funds toward specific activities. I think we can't lose sight of the fact that we've actually started... even before the first "Cyber Threats To Canada's Democratic Process" report, we have engaged with all the participants who were mentioned in that report. The ongoing activity of making people aware and talking about prevention has been ongoing for years, and that's a significant investment.

The Chair: Thank you.

Next up, for seven minutes, is Mr. Kent.

● (1700)

Hon. Peter Kent: Thanks again to all of you for appearing again before us today.

Mr. Rogers and Mr. Boucher; you were last with us on October 18, I believe.

One of the questions I asked you had to do with how you would handle something like the Beyoncé play in the last federal election in the United States. A Russian entity or individual created a fake fan website for the well-known, popular star Beyoncé and attracted millions of followers with simple celebrity gossip, information, pictures and so forth. Then, a couple of days before the actual vote, this time bomb exploded with all sorts of statements and directions apparently from Beyoncé, which were intended, according to one of our previous witnesses, Dr. Ben Scott, to discourage black voters in the United States from participating in that election.

At the time, we talked theoretically. I don't want you to compromise or expose procedures and tactics, but I do want to talk about the capability of the intelligence community and this new panel to respond in the critical last few days or even final hours before an election to something like the Beyoncé play.

Mr. Dan Rogers: I can try to address the question.

There are a couple of elements that I might suggest highlighting. One of those is that it's much easier to respond to something when we have good information and intelligence closer to the time. As we are continuing our work with the security and intelligence threats to elections task force, CSIS, RCMP, CSE and Global Affairs will look to find out whether there are foreign actors trying to establish fake accounts and trying to pass this information on.

Hon. Peter Kent: Obviously, those who would attack the electoral system are updating their tactics as we go along. They could very easily plant a bad actor in Canada with a legitimate web address or identity and could carry out the same sort of thing within Canada.

How would you detect that?

Mr. Dan Rogers: It's a good question, and part of it is a hypothetical. One of the things I can say is, if we are to look at the foreign end of that, if we can find the intentions, plans or any sort of capability being created to create that sort of account within Canada and see the foreign perspective, that will give an edge to the cyber centre and other elements in Canada. That's what we are seeking to do, and we're refining our intelligence collection. As you can appreciate, I can't get into the specifics or the techniques and the tools that we'll be using, but exactly your task between now and 2019 will be to refine our abilities to try to detect things like that.

Hon. Peter Kent: With regards to the national cyber-threat assessment 2018, given the contents of that assessment report, does Canada in this election year actively consider Russia to be an adversary?

Mr. André Boucher: The basis for our analysis is a global trend upwards in threats to democratic institutions. We don't spend inordinate amounts of time trying to attribute where that behaviour comes from. The resources we have we turn towards detecting, finding solutions and turning to prevention as early as possible. I think it's important to realize, and it's in our report, that these threats have been mounting, and Canada being the key player in the world that it is, is likely to be a target of the same threats.

Hon. Peter Kent: The Minister reiterated the government's expectation that it expects social media companies to take concrete actions to help safeguard this fall's election. The members of this committee on both sides of the table lack confidence in any of the social media companies to do what they profess. As has been said here today, their focus is on growing their business plans and profitability, not on protecting privacy. We've heard that from the Canadian Privacy Commissioner, the British Columbia privacy commissioner, the U.K. privacy commissioner, and any number of other individuals. The bad faith some of the social media companies have demonstrated in appearing before us I think prompted the question: why does the Minister have to wait six months when we have very little confidence and expectation that they will behave better?

I'll give an example. Last year when Mr. Chan first appeared before us I asked a question. During the course of our meeting a viewer, a follower, emailed and asked about the Russian false posting in Latvia, which used old pictures of an infamous Canadian convicted military officer wearing a woman's bikini. The message on that email warned Latvians that Canadian soldiers leading the battle group task force in Latvia would attempt to encourage homosexuality among Latvians. Mr. Chan said he didn't know anything about that. More than a month later my office communicated with him again and said that the posting we talked about when he was at committee was still up. Although Mr. Chan, and certainly the Facebook employees who were watching the many monitors that he references, obviously did nothing until we prompted again a month later, three days later it was taken down. Again, do any of you at that table really have the confidence in the social media, that I believe members of this committee do not have, to prevent the sorts of things that we fear may well happen during the election process?

● (1705)

Mr. Allen Sutherland: I have a couple of comments on that. I think the Minister in her remarks stated very clearly that she has expectations of the social media companies and that the discussions are ongoing. What I hear loudly and clearly from this committee is that you have expectations of social media companies and that you've been disappointed by what you've seen so far and you expect more from them. That's a message that the Minister can certainly take away and use in her subsequent discussions with them.

The Chair: Thank you.

Just be really quick.

Hon. Peter Kent: The Minister mentioned elections in Europe this year as well as in Canada, but she didn't mention the recommendations of this committee in a number of reports now that the Canadian government consider implementing some of the very real and tangible measures that the EU brought in with the general data protection regulation in May of last year that goes far beyond. Canada is not anywhere close to having the sorts of protections of Canadian privacy that the Europeans have today.

Mr. Allen Sutherland: I can assure you the Minister is current on what's happening in the EU.

The Chair: Thank you.

Next up for seven minutes is Mr. Angus.

Mr. Charlie Angus: Thank you very much, Mr. Chair.

We have looked somewhat at foreign operators, but we have been very focused on the domestic threat and the ease of the manipulation of the platform. From an intelligence perspective, are you seeing any kind of rise in extremist language, extremist groups, extremist behaviour in political discussion in Canada?

Mr. Dan Rogers: I can say from CSE's point of view that we are mandated to look exclusively at foreign actors outside of Canada by law, so that's where we focus exclusively our foreign intelligence mandate, unless we're working at the request of CSIS under our assistance mandate. With that, I can say that the threats we're going to see are going to be published in the electoral context in the report that André mentioned earlier.

Mr. Charlie Angus: I guess that's my concern. You're looking at foreign threats, yet we have Sons of Odin and we have people who can't get dates who hate women and call themselves incels. We have white nationalists. We have all manner of people. We have people believing in giant lizard conspiracies and the flat earth. They're not foreign threats, but they are dominating domestic discussion.

Our focus has been the ability of this conversation domestically to be upended. If it's not coming from a foreign source, how are we going to know that the domestic threat is understood, is calculable and that we can actually come out with a credible response without it unfairly impinging on people's democratic rights to say whatever they want about politicians?

Mr. Dan Rogers: I can comment on that, too.

I should say that the SITE task force the minister mentioned brings together CSE, CSIS, RCMP and Global Affairs Canada and, of course, CSIS and the RCMP will have the domestic mandate to do threat investigations within their mandates. That's going to continue between now and 2019, and any threat-related activity that they see will be brought to the forefront for consideration.

Mr. Charlie Angus: I have spoken up publicly defending our present Prime Minister against some very vile attacks, because I think we need to have a standard of conversation, and when the Prime Minister does something we disagree with, he should not be hanged. He's not a traitor. He is democratically elected and he's our Prime Minister. I think we need to have that standard across the board.

I was I think very shocked when Michael Wernick, the Privy Council chair, suggested that there's going to be a political assassination. From an intelligence perspective, isn't that something that you don't say publicly?

● (1710)

Mr. Dan Rogers: From my perspective, I can't comment on the overall views of the clerk, but what I can say is that from a national security perspective we do cover those sorts of threats.

I would also just add for clarity that it's certainly not within our role to decide what is true and false or what type of discourse Canadians would find appropriate. We're really focused on the foreign intelligence and the national security elements of the issue.

Mr. Charlie Angus: Again, under "Guidance to Officials" who are giving testimony from the Privy Council, we have, "Officials must understand and respect their obligation...not to disclose classified information or other confidences of the Government to those not authorized to receive them." I am concerned about someone actually voicing a potential assassination. To me, that opens doors that should be closed. I would suggest, from the intelligence perspective, that you bring that back, because I think we have to be very careful about this conversation.

I guess my frustration here is that we've seen the ability of third party actors—not foreign threats, but third party actors—within Canada to upend elections by having really good datasets. We've talked about deep fakes by the use of false information. That ability to respond to those operators is going to need really nimble responses, but it seems to me that you're much more in terms of a militarized focus, whereas we're dealing with literally digital gangsters.

What is the reassurance, based on the work we've done in our committee, that the concerns we've raised are actually being heard and can be addressed in a nimble, quick manner, rather than have this election upended?

Mr. Allen Sutherland: Perhaps I could talk about it a bit from the critical election incident public protocol perspective, just to say that for what determines whether the threshold is reached and whether Canadians are informed of something, the expectation is that—and I think this is fair to say from the intelligence perspective—it's more likely to come from a foreign source. That has been the pattern.

When we look at France, when we look at the U.S. and when we look at the U.K., the pattern has been one of foreign actors intervening, but the protocol is not limited to just foreign interference. The key component is an impact that affects the conduct of a free and fair election. If you are correct and there is something happening on the domestic side of such a magnitude that it impacts the conduct of a free and fair election, then it gets captured by the threshold.

Mr. Charlie Angus: I guess I'm a little surprised that you think that the threat is foreign when what we've seen time and time again with the 17 countries we dealt with—the domestic threat of the genocide in Myanmar where Facebook was warned again and again about the extremist language against the Rohingya Muslims.

It did nothing about it; ignored it; has been condemned internationally; still it has not really taken steps.

In Sri Lanka, we heard the same thing. In Brazil; we had representatives from Brazil at the international committee warning us. In Nigeria, the ability to use those platforms to spread hate was not foreign; it was domestic. In each case, Facebook failed to respond.

For the 2019 election, we're gearing up to fight a Cold War when what we really need to know is how to deal with third party actors who want to influence elections—100 votes here, blaming people there, attacking immigrants over here and doing it very effectively through the manipulation of the algorithms to the Facebook platform. That's the question that we want to be reassured on, and I'm not hearing that.

Mr. Allen Sutherland: I appreciate that, and perhaps I wasn't very clear. It doesn't matter the source. If it impacts the conduct of a free and fair election, it's captured by the protocol.

Mr. Charlie Angus: But you'd have to be really on that. What I'm saying and what we've seen is that this is done by one vote here, one ad there, one black ad here, one comment on a site there, but patterns start to emerge and they're coming from the same few players. You'd need to have a real understanding of how those players operate.

● (1715)

Mr. Allen Sutherland: I just want to reassure you on one point: it can be a single incident, the culmination of many incidents or the accumulation. I think that's getting at what you're arguing.

Mr. Charlie Angus: Thank you.

The Chair: Next up for seven minutes is Monsieur Picard.

[*Translation*]

Mr. Michel Picard (Montarville, Lib.): Thank you, Mr. Chair.

One of the aspects that has not yet been discussed is the aftermath of the attack. I will explain.

Let's say that, one day, we are inundated with a huge amount of hateful messages, we react effectively and, the next day, we dismantle those hateful messages by making a correction or by posting a positive advertisement, regardless of the strategy. The damage is already done. We are in an environment of freedom of expression where some things are a bit less tangible. So the damage is social, in a way.

There is an issue when it comes to system attacks by hackers, where algorithms, codes and management systems can be attacked. Even if the attack has taken place and, in a best-case scenario, you have identified it and reacted to it on the same day, the system data is still compromised. Can the compromised nature of data be repaired?

If not, and if attack on data or algorithms compromised our system, the election underway would completely lose its legitimacy. As a result, the electoral process would lose its legitimacy with regard to this next election, in October.

Is the compromised nature of data and systems following an attack maintained, or can it be guaranteed that, after steps are taken to remedy the situation, data or systems can once again be trusted? Otherwise it would be impossible to accept the election as legal and legitimate.

Mr. André Boucher: I will provide some answers.

When an individual notices that their account has been hacked by someone and that wrong information has been disseminated, they can go on our website, where we say what should be done in hacking cases. One of the first things to do is take back control and remove the information. Depending on the type of attack, that information can be removed.

The quickness of intervention is important, as information spreads like a wave. I think that is what your comment was about. I don't think that wave can be stopped with the current tools.

[*English*]

Mr. Michel Picard: It's fair.

[*Translation*]

It's an attack on a reputation. If someone hacks my personal account and puts unfounded things in it, that is a matter of reputation, but we are talking about words.

If someone gets into the election data management system for an attack, we are no longer talking about reputation being at stake. That is real system hacking. Data, the program, the algorithm or the line of code is affected. A compromised line of code puts into question the election's legitimacy. Even if we managed to block the signal, our data that is at the foundation of our electoral system's management has just been compromised.

Is the compromised nature of data important enough for the election to be declared null?

Mr. André Boucher: The first answer I gave was in the context of social media hacking.

Your second question, if I understand correctly, is about the hacking of electoral systems, correct?

Mr. Michel Picard: Yes.

Mr. André Boucher: It is important to reassure us. We have been working with Elections Canada for a number of years to implement the necessary protection measures to avoid these types of incidents. If someone is getting into our systems, that activity must be detected as soon as possible to stop the hacking. In the unlikely but possible case of the system being accessed, we must be able to go back in order to identify the activity, close the door, make backups and re-establish the information's integrity.

I think the work that has been done, as well as the partnership and the collaboration, must be recognized. I am very confident in our systems when it comes to the upcoming election.

● (1720)

Mr. Michel Picard: So corrected data can be said to have integrity.

Mr. André Boucher: Absolutely.

Mr. Michel Picard: I now turn to Mr. Rogers.

This is a bit outside my area of expertise. Can a foreign signal be converted into a local signal to go unnoticed and fly under the radar? I assume that foreign signals do not arrive in Canada with an accent.

Mr. Dan Rogers: Thank you for the question.

I want to be clear, so I will answer in English, if that's okay with you.

[*English*]

If I understand correctly, your question is whether a foreign actor can come into Canada and masquerade as a Canadian. Technology—

Mr. Michel Picard: [*Inaudible—Editor*] signal. SIGINT.

Mr. Dan Rogers: Yes.

The answer is that yes, technology does allow foreign actors to masquerade as Canadian or otherwise. Our intention is to look at the foreign actor and try to find out whether they are attempting to do that, so that we can pass information on to, for example, the cyber centre. Then they can put in defensive measures or share that information with others who may the victim of the act.

Mr. Michel Picard: Your duty is to look at foreign signals. Is it possible for you to not only to stop the signal, but to return an attack to destroy the source?

Mr. Dan Rogers: Under the current mandate for CSE, our authorities are limited to intelligence collection. There are provisions in Bill C-59, which the Senate is currently considering. If that bill is passed, we may have more authorities in the future.

Mr. Michel Picard: That's what we are waiting for.

Mr. Dan Rogers: Yes.

Mr. Michel Picard: Thank you.

The Chair: We have about nine minutes left, so we'll be down to about three minutes each.

We'll go to Ms. Kusie first of all, for three minutes. Then we'll go to Mr. Erskine-Smith for three minutes. Then we'll be close to done.

Ms. Kusie.

Mrs. Stephanie Kusie: Given the concern you've heard from this side of the table today in regard to the non-partisanship or independence of the five individuals who comprise the panel that will decide the critical incident protocol trigger, I am asking for assurance from both Mr. Boucher and Mr. Sutherland that you will do everything possible in your power as public servants to support the absolute disclosure of equal and shared information to all political parties, please.

Mr. Allen Sutherland: I just want to be precise. If there was an event that passed the threshold, it is an obligation that the Prime Minister, the leaders of the opposition parties and Elections Canada be informed. I can give you full assurance that that's what will take place. It will be the same briefing to all actors. The decision would have been made that the threshold had been passed. The Prime Minister, the leader of the opposition party and Elections Canada are not the deciders. The decision will have been made, but they will be informed equally. I can give that assurance.

Mrs. Stephanie Kusie: Thank you, Mr. Sutherland.

[*Translation*]

Mr. Boucher, do you want to comment?

[*English*]

Mr. André Boucher: Yes, absolutely.

There will likely be many more events that do not pass the threshold. The practice of the cyber centre has always been—and will continue to be—to inform those who are affected or potentially affected when we detect incidents or events of significance. Unlike the threshold conversation, ours is always an unattributed conversation. It's about the manifestation and giving the tools to those who are or might be affected to defend themselves or remediate the problem.

In our conversation we would not be specific about "Entity X is having this issue." We would just say that there's an entity in the process having an issue and you can detect whether you are also having the issue with the following tips and indicators. We'll provide assistance to help resolve those issues. That's what would happen in all circumstances below threshold.

Mrs. Stephanie Kusie: Mr. Rogers, you might be tired of me talking about this, but I'm a member of the Trilateral Commission. We were fortunate to go to Silicon Valley in November to have an overview of a cybersecurity update with some of the most brilliant minds in the world. I felt that perhaps instead of being at Facebook and Google, we should have been at the main office of Fortnite.

I want to hear your comments, very briefly, in terms of how you find, engage and employ the absolute best to secure our electoral systems.

Mr. Dan Rogers: That's a great question, thank you.

We are recruiting, so anyone who's listening is welcome to send through a resumé.

● (1725)

Mr. Charlie Angus: For everybody around this table, ethics rules. I'll come after you.

Voices: Oh, oh!

Mr. Dan Rogers: It is an excellent point, because it is challenging to find the best and the brightest to come and work on our team. It is something we take pride in doing. We make extensive use of student and other outreach programs across the country to reach into universities and bring in what we would consider truly exceptional people to work on these problems.

The Chair: Thank you.

Last up is Mr. Erskine-Smith for three minutes.

Mr. Nathaniel Erskine-Smith: I have one question, then I'll pass it to Anita.

When a number of us were in Washington, we were speaking to members of Congress on this issue. One of the members indicated that in their world, they take a red team-blue team approach where their accounts are hacked, whether by their political staffers or by Congress people themselves. There are attempted hacks and then they are told how they were hacked and how to prevent them in future.

Are there any plans to hack us for the betterment of our democracy?

Voices: Oh, oh!

Mr. André Boucher: I welcome the invitation.

No. We do provide advice to political parties. As you may have heard, one of the measures we use with campaign managers and others is a simulation. Phishing emails are a good example. To this day, phishing emails remain the most prevalent threat coming to each and every one of our inboxes. A campaign to give people an awareness of what that looks like and how to react, and then the post —

Mr. Nathaniel Erskine-Smith: I say it less seriously, but I would encourage you to communicate with your American counterparts. I think it would be a worthwhile exercise here in Canada to implement a simulation like that on a regular basis.

Anita.

Ms. Anita Vandenbeld: Thank you.

I want to go back to the critical election incident public protocol. Without that, what is the default? What is it right now? My understanding is that there would be absolutely no informing of political parties. Any one of the members of that panel could go to the press on their own, without that process. Worse yet, there could be an incident and none of them make the public or the political parties aware.

Can you tell me, without this, what exists right now? What would be the default right now if we didn't have this in place?

Mr. Allen Sutherland: That's a very interesting question. Thankfully, it's hypothetical.

In the absence of a protocol during the writ period, I think government officials, indeed, ministers and the Prime Minister would be put in an untenable position: They would have to weigh in and decide whether something had passed the threshold. Obviously, you would be stuck in a partisan dilemma there.

The Chair: Thank you, all.

I just have one question. It refers to the trip some of us made to Washington about a year and a half ago, to talk about Equifax. It was still alarming to me to find out that we're not regulating our credit bureaus in our country. That said, the reason the Equifax breach was even discovered was that there was an overarching group called Homeland Security that actually warned Equifax of a potential breach. They warned them several times, but they did not respond and did not fix it. That's what caused the breach of 150 million Americans and about 19,000 Canadians give or take, I guess.

Do we have a similar system in Canada? I would rather you not answer if we don't. You can tell me later. Do you have a similar process?

What concerns me about this is a statement that Mr. Rogers made. We have a mandate to investigate if they occur. My concern is whether the fire has to be lit for you to extinguish it, or whether you actually take steps to prevent the fire from occurring in the first place.

Mr. Dan Rogers: Let me just correct one thing before I hand it on to André for a great answer. We investigate foreign actors and their intentions to discover them, not simply if they are brought to our attention. I apologize if I misspoke there.

I'll hand it over to André. One of the benefits of our system is that the intelligence capacity we bring to bear on the foreign signals intelligence side can find the activities of cyber-actors. These can be passed on to the cyber centre so that it can provide that sort of insight and detection early on.

The Chair: We have about 30 seconds or so.

Mr. André Boucher: That's a good warning, if you know me and the microphone.

The really good news that Mr. Rogers just talked about—the fact that we have one joint team—is a strength in Canada, an absolute strength.

The equivalent of the Homeland Security, or DHS, in the U.S. definitely exists in Canada. In fact, the cyber centre is what you will find is the equivalent at DHS: CISA. They have a cyber-equivalent cyber centre. Our practice is very similar to that.

Hypothetically, Mr. Rogers and his team detect something from foreign space happening to one of our constituents and inform my centre. We would actually go out, reach over to them, and of course, for reputation and other reasons, we'd start with a very discreet, "We think you have this and you should do something about it". However, if need be and we need to escalate, we would take more public measures.

● (1730)

The Chair: I'll finish with a last plug for what our committee is going to be doing on May 28 here in this very room—the international grand committee, meeting number two.

We met with eight other countries plus Canada in London to talk about these very issues, about foreign threats to our democracy, etc. We're going to be meeting in Canada this time for the second meeting. There will be a similar invitation list, inviting the platforms to appear.

Any advice that you have for the committee, witnesses to pursue, etc., would be appreciated.

Thank you for coming today to committee.

Have a good afternoon, everybody. The meeting is adjourned.