HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

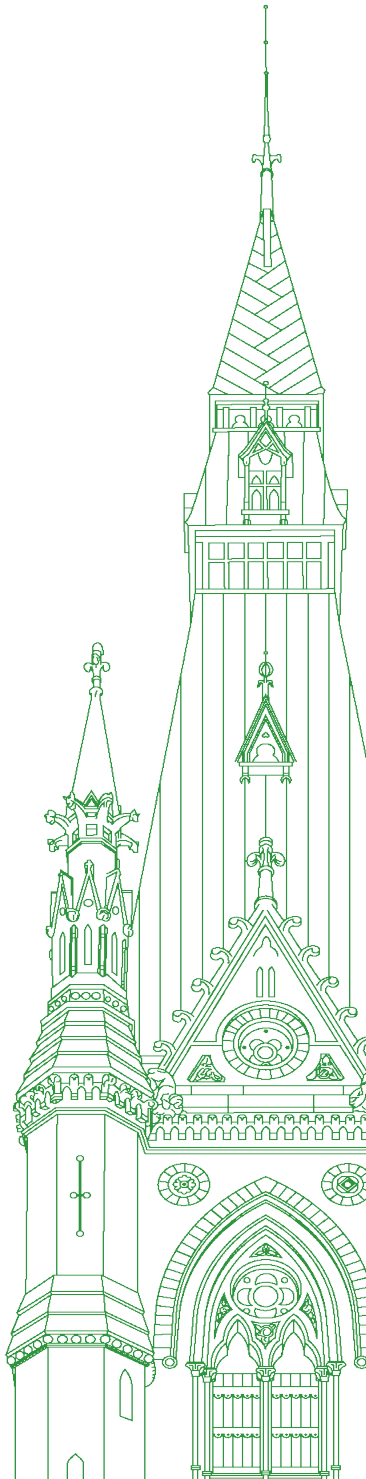
44th PARLIAMENT, 1st SESSION

Standing Committee on Procedure and House Affairs

EVIDENCE

NUMBER 124

Thursday, September 26, 2024



Chair: Mr. Ben Carr

Standing Committee on Procedure and House Affairs

Thursday, September 26, 2024

● (1100)

[*Translation*]

The Chair (Mr. Ben Carr (Winnipeg South Centre, Lib.)): Good morning, everyone.

[*English*]

I just happened to walk into the room past President Macron, and I see we have mac and cheese for lunch today. That was a very appropriate choice made by the chef of Parliament. *Merci*.

Voices: Oh, oh!

[*Translation*]

Ms. Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): We get it.

[*English*]

The Chair: Oh, come on, Luc. Give me that one, man.

Whether it was a good joke or not, we started the morning with a laugh, and that's what's important.

[*Translation*]

I'd like to welcome you all.

[*English*]

As you know, we have a couple of witnesses with us here this morning.

[*Translation*]

We welcome Stéphane Perrault, chief electoral officer.

Welcome, Mr. Perrault.

Also with us is Karine Morin, senior director, integrity, regulatory policy and Parliamentary affairs.

[*English*]

I noticed that we have Ms. Idlout with us this morning. Welcome. It's nice to see you. We sit together on the indigenous and northern affairs committee, but it's nice to see you in this context.

Ms. O'Connell, welcome to PROC, as well, this morning.

Colleagues, we will follow the usual format: six minutes in the first round, followed by five minutes, with a couple of two-and-a-half-minute slots.

Mr. Chief Electoral Officer, between you and Madame Morin, there will be 10 minutes for opening remarks. You don't need to use those 10 minutes, but they're yours should you feel you need them.

I'm sorry. I forgot to mention this: Before we begin, colleagues and witnesses who may not be in front of committee often, I have a reminder about the headsets. In order to avoid damaging audio feedback and other challenges that can pose a health issue for our interpreters—who work very hard on our behalf—please make sure that when they're not in use, they are placed on the sticker in front of you. Try to keep your phones away from the microphone when you are speaking. Of course, if it's in your ear, witnesses, that's fine.

With that, Monsieur Perrault, I will give you the floor.

[*Translation*]

Mr. Stéphane Perrault (Chief Electoral Officer, Office of the Chief Electoral Officer): Thank you, Mr. Chair, for the opportunity to speak with the committee this morning about Elections Canada's pilot project to include the Inuit language on federal election ballots in the electoral district of Nunavut.

I am accompanied by Karine Morin, who is responsible for the project at Elections Canada.

As it involves variations to several rules prescribed by the Canada Elections Act, this pilot requires approval under section 18.1 of the act, which provides for the Chief Electoral Officer to devise and test alternative voting processes with the prior approval of the committees of the House and Senate that normally consider electoral matters. I am therefore seeking approval from the committee today.

There are a few unique realities in Nunavut that support this pilot project. First, Inuktut is recognized as one of the official languages across the territory, which also constitutes one electoral district. Most of its population are Inuit, at 84% or a little more, and speak Inuktut as their mother tongue.

If approved by the committee, this project would help identify improvements to make the electoral process more inclusive and accessible to Inuktut speakers, while also identifying operational and legislative issues that would need to be addressed in order to implement this as a permanent service offering.

In addition, this pilot would complement Elections Canada's efforts to gradually offer more communication products in Inuktut in the electoral district of Nunavut. Committee members will recall that during the 2021 general election, new communication products included a ballot facsimile and a poster-sized version of the ballot that were provided in Inuktut at polling places.

When I appeared before this committee in March 2022 during its study of the inclusion of indigenous languages on federal election ballots, I provided different options for the committee's consideration for the inclusion of indigenous languages on federal ballots and explained some of the challenges for each.

In its report, the committee recommended that Elections Canada undertake a pilot project to include Inuktut on federal election ballots in the electoral district of Nunavut. Following your report, my office began developing a proposal for this pilot, informed by discussions with several Inuit representatives and organizations and aligned with the experience of Elections Nunavut. I would like to underline today that all those consulted have welcomed the initiative.

● (1105)

[*English*]

I would like to remind members that this is a pilot initiative that is unique to the electoral district of Nunavut. It is a new and exploratory initiative that forms part of Elections Canada's efforts to pursue gradual approaches to better reflect the linguistic reality of electors in Nunavut.

In brief, the pilot would allow candidates and political parties running in Nunavut to submit their names in Inuktut, whether in Inuktitut using syllabic symbols or in Inuinnaqtun using the Latin alphabet, as well as in English and in French, and to have those names appear on the regular ballot. This would also allow electors in Nunavut to write the name of a candidate in Inuktut on a special ballot when voting by mail or at the local Elections Canada office when using write-in ballots.

Candidates and political parties would be invited to provide their names in Inuktut. Elections Canada would not translate or transliterate candidate or party names and would not require identification documents to verify candidate names in Inuktut. This is the same approach currently used by Elections Nunavut.

As we plan for the implementation of this pilot, there are a number of challenges and limitations that we are aware of. One of those challenges is ensuring quality control of the regular ballot in Inuktut, within the very short time frame between the close of nominations and the printing and shipping of the ballots so that they arrive in time for advance voting in the different communities in Nunavut. We have retained the services of readers of Inuktut to assist us with this task.

Another challenge arises from the fact that we are not planning any IT system changes as part of the pilot. This means that while Inuktut names will be reflected on the ballots, it will not be possible to fully incorporate Inuktut into all electoral information products, such as election results on our website on election night.

To ensure the integrity of the counting process for special or write-in ballots, the pilot will also rely on hiring readers of Inuktut at the local Elections Canada office in Iqaluit and at the counting facility here in Ottawa. Election workers who read Inuktut would assist in recording the intentions of voters who used Inuktut when filling out special ballots. It's important to be aware that Inuktitut is not a fixed language and that different symbols can be used to express a similar sound, so the name may vary. We need people who read the language, to be able to make sure that they are not unduly rejected if they're written in a different manner. Political parties would also be invited to send observers who can read Inuktut to maintain the integrity of the counting process during the pilot.

With respect to next steps, I have also written to the Senate committee and hope to meet with them later this fall. If we receive approval for the pilot project from both committees, we will invite the political parties to submit their proposed party names in Inuktut as part of our first implementation phase.

I plan to write to both committees after the pilot to report on operational and legislative issues that would need to be considered should Parliament wish to make this a permanent service offering, as I think is certainly the objective.

[*Translation*]

Before I conclude, I will point out to members that I have provided a table of the variations to the Canada Elections Act. There are not many, but they are required to carry out the pilot project. If it's approved, I hope they will be included in the committee's report.

I appreciate the committee's invitation and interest in this project. I would be pleased to answer your questions.

The Chair: Thank you very much, Mr. Perrault.

[*English*]

Thank you for that.

Thank you for the very clear and instructive materials that you've provided. I am looking forward to the conversation today.

With that, we will turn to our first line of questioning, which goes to the Conservatives.

Mr. Cooper, the floor is yours for six minutes.

● (1110)

Mr. Michael Cooper (St. Albert—Edmonton, CPC): Thank you very much, Mr. Chair.

Let me say, at the outset, that this is a worthwhile pilot project, and I want to congratulate you, Mr. Perrault, for putting it forward.

You stated that the pilot project would allow candidates and political parties to submit their names in Inuktut, whether using syllabic symbols or using the Latin alphabet, as well as in English and in French. From the standpoint of what a ballot would look like, hypothetically, there could be four different versions of a candidate's name and political affiliation. Is that correct?

Mr. Stéphane Perrault: There are more likely three versions of the candidates' names—usually French and English are identical—and possibly two variations of the party name.

Mr. Michael Cooper: When you appeared at this committee in March 2022, you stated:

> The use of printed ballots with more than two languages raises important questions regarding accessibility and design. Putting the names of parties and candidates in multiple languages on a ballot risks making a crowded, busy text that may be difficult for some voters to comprehend, especially voters with low literacy levels or an intellectual disability, as well as voters with a visual impairment.

Do you still share those concerns? If so, what measures is Elections Canada planning to undertake, pursuant to the pilot project, to mitigate these concerns?

Mr. Stéphane Perrault: I will put my comments in context. At the time, the committee was discussing the possibility of a broader use of indigenous languages on the ballot, including in electoral districts where there could be, with the 1% threshold, up to five indigenous languages in addition to French and English.

That was a very serious concern, in my opinion. I am much less concerned with that here, because we are talking about two or possibly three languages. I don't see that as a major issue. I think it's something that we will have to measure and appreciate as part of this pilot project.

Mr. Michael Cooper: Thank you for that.

In the briefing material prepared by Elections Canada with respect to the pilot project, last updated on July 29 of this year, the following was noted: "Special ballots are being considered but further analysis is required at this time to ensure the integrity of the process is maintained and the operational requirements are met."

You mentioned that special ballots will be included in the pilot project. I think we have a sample of a special ballot. Has that analysis been completed?

Mr. Stéphane Perrault: We have made the decision that we need to absolutely have readers of the language in order to be sure that the ballots are not unduly rejected. Based on consultations and discussions that we've had, it's very clear that we should have people who speak the language in order to ensure that they're not unduly rejected.

Mr. Michael Cooper: Maybe you could elaborate a little bit on what specific concerns there were with respect to the integrity of the process as it concerns special ballots.

Mr. Stéphane Perrault: The concern that we had in mind was the fact that, as I indicated, the written form of Inuktitut is not fixed. A person's name can be expressed using different symbols to indicate the same intent. Someone who is not familiar with the language may not be able to properly understand the voters' intentions. We do need people who are capable of reading the language fluently to make sure that ballots are not unduly rejected.

Mr. Michael Cooper: Are there any other issues of quality control that you see? Certainly you've cited one example of that, but are there other concerns?

Mr. Stéphane Perrault: I would say that, theoretically, when somebody submits a name, we need to make sure that the name is not fanciful or is not "vote for me". Not being a reader of the language, I could not make that determination. That's why I indicated that we have retained the services of people who speak the language to make sure that there is no significant abuse or error in the construct of the ballot itself.

Now, we've had discussions with our colleagues at Elections Nunavut, and that is not something they have experienced, but we do need to make sure, because we do not have that linguistic capability.

Mr. Michael Cooper: On that point, when you referenced Elections Nunavut, the process that is being proposed in the pilot with respect to candidates making a submission as to how their name would appear on the ballot is the same process that has been practised by Elections Nunavut. Is that correct? How long has that practice been in place in Nunavut?

● (1115)

Mr. Stéphane Perrault: It is the process that they have in place. I cannot answer your second question as to how long. It's certainly been several electoral cycles. They have not encountered any issues with that, but they do not translate or transliterate the names. I understand that typically candidates do submit both in the Latin alphabet and in Inuktitut. There are linguistic variations. They have 25 communities with linguistic variations, but they have one writing for each of those communities. The candidates for those communities use the language as it is used in those communities, and that does not present a challenge.

At the federal level, with a single candidate for the district, they will use one variation of that language, and that will be it. There won't be 25 variations of that writing.

The Chair: Thanks very much, Mr. Cooper.

It's over to Mrs. Romanado for six minutes.

Mrs. Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.): Thank you very much, Mr. Chair.

Monsieur Perrault, it's a pleasure to see you again, and we're happy to have you back to present this study to us. I remember working with the PROC committee on this study, so I'm happy to have you back here today to give us an update.

I have three questions.

You mentioned that you're going to also be presenting to the Senate committee. Because we are in a minority Parliament and an election can happen at any time, are you prepared to launch this pilot project for the next election, should it be called before October 20, 2025?

Mr. Stéphane Perrault: I can only launch the project with the approval of both committees.

That cannot happen because there are deviations from the act, which are recorded in the document that I've shared. There's a need for that. Once we have that.... We've translated all of the material; you have copies with you. There are other materials, as well. However, we have not produced them. We have to print them and put them in packages, so that they can be ready to be delivered. We do need to engage with parties to make sure they provide their names, should they wish to do that. Then, of course, we have to train the workers.

It would not be an instant implementation. The sooner I can get the approval, the sooner I can get working on making that happen.

Mrs. Sherry Romanado: You mentioned that it wouldn't be possible to fully incorporate Inuktut in all electoral information products. You mentioned the website. If a candidate wants to learn more about how to put forward their candidacy to run in the next federal election, will that information be provided on the web to potential candidates?

Mr. Stéphane Perrault: I'd have to validate that, but certainly the local returning officer would be there to assist all the candidates who want to put in their nominations.

This is a process that, as I said, is very similar—apart from the party names—to the one used in territorial elections, so the candidates would not be unfamiliar with that process. We're following the same approach.

Mrs. Sherry Romanado: This may sound like a bizarre question, but with respect to the size of the ballot.... We've just gone through two by-elections where one had the longest ballot. I believe that in the last election, there were 91 candidates on the ballot.

You mentioned the difficulty with the time between when someone submits their nomination package and becomes an official candidate and the time when you have to print the ballots or the special ballots and terms. Should this happen again when we have the election in Nunavut—if we had a similar situation with 91 candidates submitting their names—what challenge does that pose for you? I can't even imagine the size of the ballot, let alone your ability to quickly have that documentation printed.

Mr. Stéphane Perrault: That's correct. We also have to validate the names.

Obviously, we haven't seen that in Nunavut. There are typically fewer candidates there, and we are not planning for a 91-candidate ballot in multiple Inuktut languages. If that were to happen, this could possibly be a roadblock to the implementation of this project.

I'm optimistic that this would not happen in Nunavut.

Mrs. Sherry Romanado: You've provided us with the temporary variations for the Canada Elections Act. You mentioned that once you've met with PROC and with the Senate committee, it wouldn't be an instant implementation. Are there additional requirements for you to come back to committee before you can proceed with it, or would you just be able to go along, continue the process and hopefully be ready for the next election?

● (1120)

Mr. Stéphane Perrault: The only circumstance where I would need to come back is if the Senate were to require something different as a condition that would vary from your approval. I would then have to come back to this committee.

Mrs. Sherry Romanado: My colleague, MP Fortier, has a question, so I'll cede my time to her.

[*Translation*]

Hon. Mona Fortier (Ottawa—Vanier, Lib.): Thank you, esteemed colleague.

Mr. Perrault, thank you very much for this initiative. Obviously, I was not part of the studies or discussions on this. My riding of Ottawa—Vanier has a huge Inuit community, and they still have an address in Iqaluit. I can imagine that they will want to vote on election day or vote on a special ballot that will be sent to their electoral district.

In other ridings, are we ready to welcome those who will want to exercise their right to vote as part of this pilot project?

Mr. Stéphane Perrault: Some people's usual place of residence is Nunavut, but they are in Ottawa for all kinds of reasons. There's a pretty good Inuit community in Ottawa. These individuals have the right to vote in Nunavut. They will be able to obtain the form and related instructions online. There are paper copies of those instructions for those who wish to receive the package that will enable them to vote in the language of their choice at that time.

Hon. Mona Fortier: I find that interesting, because I will be able to take part in the pilot project myself when the time comes. In the next election, I will make sure that the local offices in Ottawa are ready for this practice. I hope to be able to take part on the ground and inform those who want to vote about the process.

Mr. Stéphane Perrault: I just want to qualify that. People who are not in Nunavut, that is to say outside the electoral district, will have to apply online. We're not going to equip all districts.

Hon. Mona Fortier: Okay.

I imagine a phone number will be made available to these individuals in case they have questions about this. It would be good to share that information with them.

Mr. Stéphane Perrault: Yes, a phone number will be provided.

Hon. Mona Fortier: Perfect.

Thank you very much.

The Chair: Thank you, Ms. Romanado and Ms. Fortier.

[*English*]

Thank you, Mr. Perrault.

I will note that until the recent by-elections, my by-election of last year held the record for the longest ballot, with 48 names. They've since doubled that, so I'm no longer a record holder, I suppose, in that regard.

[*Translation*]

Ms. Gaudreau, you have the floor for six minutes.

Ms. Marie-Hélène Gaudreau: Thank you very much, Mr. Chair.

It's always a great pleasure to have you here, Mr. Perrault. It is important to have a good grasp of the situation. I, for one, am constantly learning about these things.

To be honest, I have to say that I had a few questions, but my colleagues have already asked them all. However, I have taken note of the request that the decision be made quickly, given the circumstances. Our concern, at least mine, is that you have everything you need to carry out this initiative given what might happen anytime.

Are there any challenges that have not been raised and that could give us the opportunity to help you if that situation were to materialize soon, and should we support the project?

Mr. Stéphane Perrault: The challenges are those specific to a new initiative. We'll take a look at them. I think we've done everything we can to understand the situation. We've consulted with people, including Elections Nunavut, but there are always situations that we don't anticipate. That's why it's a good thing it's a pilot project. It's also why I intend to conduct an evaluation of the pilot project with the communities afterwards. There will be focus groups, and they will share with us their impressions of their experience.

As I said earlier, the situation is not exactly the same as it is in the territories, since we don't have a candidate in each community. There are also language variations. So we will learn from this exercise and make the necessary adjustments.

One of the challenges is that it's very hard to withdraw a service offering once it has been provided. This is not a permanent service. The act would have to be amended to make it permanent. I hope that happens and that it'll be done fairly quickly after the next election so that we don't end up in a situation where this service is offered, and then we stop providing it after the next election.

● (1125)

Ms. Marie-Hélène Gaudreau: I understand what you have just told us, and I think that all my colleagues have taken note of those comments.

There's a lot of time left, and I don't want to monopolize if I don't have to. However, I would like to know how things work in a large territory.

Could you explain the process to me a little and tell me if there are any differences?

Mr. Stéphane Perrault: It's quite a unique reality. I think most Canadians don't have the opportunity to appreciate just how many differences there are between electoral districts. In terms of geography alone, we're talking about approximately two million square kilometres.

To put things in perspective, I would point out that, in the territories—and I'm not including water here—the area is about the same as western Europe. There are 25 communities. I'm unsure of the exact number, but I believe that Elections Nunavut has 25 or 23 returning officers in the communities. We have only one. Obviously, that requires it to maintain ties with the community.

The fact remains that these are quite extraordinary challenges in terms of logistics and fast deployment, especially when it comes to printing ballots on time for advance polls. Printing is not done in Nunavut because of the specific requirements for ballots under federal legislation. So they have to be dealt with on the night nominations close. Nunavut is the priority. We need to finish the review that evening to make sure that printing and distribution can be done in time for the advance polls.

Ms. Marie-Hélène Gaudreau: That's very interesting.

That's it for me, Mr. Chair.

The Chair: Okay, thank you.

[*English*]

Next is Ms. Idlout.

Lori, it's really nice to have you here. You can certainly offer a unique perspective on this.

The floor is yours for six minutes.

Ms. Lori Idlout (Nunavut, NDP): *Qujannamiik, Iksivautaq*.

Thank you, Stéphane and Karine. It's nice to see you both again. I caught one of your focus groups in Iqaluit, so it's nice to see some of the results of what you've been trying to do in helping to make sure Inuktitut-speaking and -reading people can be more engaged in the federal election process. I appreciate all of the efforts you've made.

I want to ask some questions that would help give some context to what my experience has been, so more parliamentarians can understand some of the challenges you're talking about—and opportunities, even. Having been a territory since 1999, Nunavut has been holding elections for some years now. Having been from NWT before Nunavut became a territory, with the NWT electoral system as well, I understand that providing ballots in more than four languages is also a possibility.

I wonder if you could explain to the committee whether you've consulted with NWT on what they're doing. They have 11 official languages.

Mr. Stéphane Perrault: Yes, we have. My colleague here has been in regular contact with our friends at Elections NWT.

One of the things we have been doing, with their assistance, is translating more of the products into various languages. There are, as you said, 11 official languages there. Those will be found on site at polling locations in order to make the voting experience more inclusive and reflective of the linguistic reality.

We have a very good working relationship with our colleagues there.

Ms. Lori Idlout: Thank you for that.

You mentioned during your speech that it will not be possible to fully incorporate Inuktitut into all electoral information products, such as election results.

I wonder if you could describe for us what the challenges are in making sure that Inuktitut and Inuinnaqtun can appear in other electoral information products.

Mr. Stéphane Perrault: The choice we made is because of timing. We don't know when the election will take place, and we do not want to invest in changing all of our IT systems until we have a satisfactory experience and the agreement of Parliament to make this a permanent service offering. It's a compromise.

However, from a voter experience point of view, voters will see the ballot and products at the polling station in their language.

● (1130)

Ms. Lori Idlout: I'm wondering if there are barriers in the current legislation.

As you mentioned, the printing of the ballots happens outside of Nunavut. Are there barriers in the legislation that prevent the ballots from being printed in Nunavut communities?

Mr. Stéphane Perrault: The ballot, as designed in the Elections Act, requires a counterfoil and a stub that can be turned. There are a limited number of printers that can offer that type of printing. This is not unique, in fact, to Nunavut. We have a limited number of printers that serve all of Canada.

Ms. Lori Idlout: You seem to understand that Nunavut is vast. As you mentioned, it's two million square miles. There are three time zones in Nunavut. All 25 communities are fly-in communities.

Would you agree that ensuring that printing can happen in Nunavut could help lessen that barrier?

Mr. Stéphane Perrault: I would answer in two ways.

I have the power, under the act, to make certain adaptations. For a stopgap measure, we always typically allow for the possibility of printing copies of the ballot locally, without the stub and counterfoil, irrespective of what we're talking about here today in terms of languages. That's simply because there's a risk—weather or other circumstances—that we cannot get the ballot into some fly-in communities in time. There's always a stopgap measure. In that case, with adaptation of the legislation, the vote can proceed with, essentially, copied ballots, which are hand-numbered. We haven't had to use it, but it's always very close.

For a more fulsome solution, the alternative is to remove the counterfoil requirement. This is something unique at the federal level, to my knowledge. Provinces and territories do not have that element in their ballot format. That's something that brings a broader series of considerations to the table.

Ms. Lori Idlout: I'm sorry, but is that legislated in the Elections Act?

Mr. Stéphane Perrault: It is legislated, yes.

Ms. Lori Idlout: That could be another amendment to help ensure that indigenous languages could be—

Mr. Stéphane Perrault: There would be other benefits to removing the stub and counterfoil. Again, this is a security control, but it is not one that is commonly used; in fact, as I said, at the provincial level, it is not used.

Ms. Lori Idlout: As Nunavut is only one riding with 25 different locations, have you seen what barriers Nunavut has? I especially remember medical patients who were not in their home communities who tried to go vote in Iqaluit. What opportunities would you recommend to make sure that, in that one riding, for example, people can still vote even if they're not in their home community?

Mr. Stéphane Perrault: Right now, they can vote by special ballot but only until day six, and that's a limitation.

In order to remove that limitation, we have to introduce electronic lists of electors, which is a project we have for the next election, but not necessarily in Nunavut. It will not be wide-scale for the next election, but down the road, because it is a single riding, it would be possible with electronic lists to have a strike-out to make sure there's no double voting and therefore allow more opportunities of that nature.

The Chair: Thanks very much, Ms. Idlout.

Colleagues, we are going to head into the second round of questioning, which means there is a little less time.

Mr. Cooper, the floor is yours for five minutes.

Mr. Michael Cooper: Thank you, Mr. Chair.

Mr. Perrault, the date of the next territorial election in Nunavut is October 27, 2025. Is that correct?

Mr. Stéphane Perrault: That is correct.

Mr. Michael Cooper: Thank you for that. I find that very interesting, because October 27, 2025, happens to be the same day that the Liberal government's Bill C-65 proposes to push the date of the next federal election back to.

The fact that Bill C-65 would set the date of the next federal election to the very same day as the Nunavut territorial election demonstrates that the story the Liberals have told Canadians about the need to move back the fixed election date by one week, namely to avoid a conflict with a holiday and with the Alberta municipal election, is completely disingenuous. It is about as dishonest as it gets.

They have moved it back for one reason and one reason only, and that is so that soon-to-be-defeated Liberal MPs who would not qualify for their pensions if the election was held on the current fixed election date would suddenly qualify for their pensions. It is a pension bill disguised as an election bill, and if the Liberals were honest, they would name the bill what it is, and that is “the loser Liberal pension protection act.”

With that, I will cede the balance of my time to Mr. Calkins.

● (1135)

Mr. Blaine Calkins (Red Deer—Lacombe, CPC): Thank you for being here.

I have a couple of questions.

First of all, can you elaborate a little more on the importance of the stub and counterfoil in ballot security and control? How important is that?

Mr. Stéphane Perrault: The stub and counterfoil take us back probably to 19th century concerns around what is commonly referred to as “daisy chain fraud”, whereby a voter walks in, obtains a ballot, does not return it to the poll worker, walks out with a blank ballot and then hands it over to a candidate or party operative. In exchange, they start a chain whereby they can give ballots to future electors, and these ballots would be pre-marked. In that chain, fraud could occur whereby the marking of the ballot actually takes place outside of the poll in successive waves to influence the vote.

This is not something that has been seen in modern times. I don't know, in fact, that it has been seen in Canada. Risks of fraud in this day and age are more of a digital nature than they are of this nature, and that's why I don't believe—and I may be mistaken—the counterfoil and stub procedure exists anymore at the provincial and territorial levels.

Mr. Blaine Calkins: Okay. Still, fraud prevention and the integrity of the election is paramount. This does sound like something that could potentially happen. I don't know why we would expose ourselves to that if we ever decided to move away from that.

I have some other questions. I'm not a linguist—that's my daughter, who's good at this kind of stuff—so I'll be asking some questions. I don't know who best can answer them.

Just for clarity, from your description, it sounds to me like Inuktut is more of a phonetic language, using the syllables, than it is a grammatical issue. You can have several candidates with similar names. These things happen. You have now 343 or so ridings that will be in play in the next election. Are you confident that you'll have enough people who are fluent in the various dialects, for lack of a better word? What do you do at that point in time? If the variance between the names is so little, even on the English and French sides of the equation, then one could only assume that they would be very similar in the various regions where the languages are used in Nunavut. Will this be a problem?

Mr. Stéphane Perrault: This proposal, this pilot, would not add to this problem, because the candidate's name would also continue to be required in the current language, which is the French or English language, as the case may be.

Mr. Blaine Calkins: But the purpose of this exercise is that people don't speak English or French. If what we're trying to do is engage more people who might not be able to engage in one of the official languages of English and French, and we don't have consistency in the Inuktut language, is this potentially problematic? Would the political parties' names be changed? Will the ballot be consistent across all of the territory in an election?

Mr. Stéphane Perrault: The ballot will be consistent. The party names will be decided by the parties. Elections Canada is not going to translate or transliterate. Some parties' names currently, the Bloc Québécois being one example, do not exist in English. There are English party names that do not exist in French. Parties don't have to have a translated name, even in French and English, as we speak.

Similarities in names currently exist. There are mechanisms to add a mark or add a middle name to make that difference in the current framework, without the additional concern of Inuktut. I do not believe it adds to the confusion. In fact, it may reduce it because of the additional language.

That said, there are two things to keep in mind. The vast majority in Nunavut do speak English or French, and we always try to have poll workers who speak Inuktut. We don't always succeed, but we certainly try to do that. They can help the voters understand the ballot if there are questions.

● (1140)

The Chair: Thanks very much, Mr. Calkins.

Mr. Turnbull, the floor is yours for five minutes.

Mr. Ryan Turnbull (Whitby, Lib.): Thanks very much, Chair.

Thank you, Mr. Perrault and Ms. Morin, for being here today. It's great to see you.

I'm really happy to hear about the work we did on PROC. I'm looking at Lori Idlout for her advocacy in this area and for the incredible contributions she has made. Lori, it's really great to see you back here.

I'm glad to be back on PROC. I'm glad to see this pilot moving forward. I think we can all agree that it's a real step in the right direction. Thank you for your commitment and your work on this. I do have a few questions, but I wanted to show my solidarity for your hard work to make this happen.

I read your opening remarks. I think there might be some differences, perhaps, in what you said and what you wrote ahead of time. I note that at some point towards the end of your remarks, you said that you envisioned coming back to the committee, or coming back to Parliament, with “operational and legislative issues” that might need to be remedied in order to make this pilot “a permanent service offering”. I think this is the way you said it, which is great.

What do you anticipate those might be? It sounds like you already have an idea that there will be some challenges that need to be overcome, or some legislative changes that may be necessary, in order to do this more permanently. What do you anticipate some of those to be?

Mr. Stéphane Perrault: We are simply cognizant of the fact that it is not as simple as it may appear at first glance. We've tried to do consultations and work with territorial partners who've done this, and consult locally. We think we have everything covered.

You will notice that in the document I shared, in the legal variations there is a final clause that would allow me to make any additional change necessary for the implementation if something arises. It's not a policy direction change. It's if there's a technical issue. This is why it's a pilot. When we come back, we will take stock of what took place and how well it went. I'm confident that it will go well, but the nature of the pilot is to draw lessons and enable Parliament to make a permanent decision on whether to go forward with this or not, or to go in a different way.

Mr. Ryan Turnbull: Thank you for that.

Are there other precedents in areas where you have the power to make slight changes to your operations where necessary? Do you then justify those in writing? How does that work?

Mr. Stéphane Perrault: There are two powers in the act.

One is for the implementation of the special ballots in various forms. There are adaptations I can make that are similar in formulation to this, where it's necessary for the carrying out of the provisions. There are regularly some adaptations that are made for that. They're always published on our website, and they're shared with the parties and candidates as we go.

Then there's a provision in section 17 of the act that is more for unusual and unforeseen circumstances. You can think about electors who are displaced by a flood or a fire. We have to allow them to vote out of riding. This is a fairly common occurrence, and it's expected to be more common in such a big country. There is a power there and, again, these adaptations are made publicly and transparently. They're published on the website and shared with parties and candidates.

Mr. Ryan Turnbull: I led you to that because I had a feeling that you were going to say that. It's not unheard of that you have some flexibility within your operations and that you justify that and document it so that people are aware. There's a level of transparency there that we all agree is paramount to upholding our institution here, which is very important. Thank you for that.

I think that sets the stage, perhaps, for you coming back later at some point in the next Parliament to report back on how things went, which leads me to my next question. You've talked about how this could perhaps be a permanent service offering. I think that in our previous work and deliberations as a committee there was quite a lot of support for this pilot. I think the underlying objective is to remove barriers and increase voter engagement.

My question is, how are you going to measure the success of this pilot? You've mentioned doing focus groups and getting feedback, which I think means you're open to continuous improvement—which is fantastic—but how will you determine whether or not this is successful?

● (1145)

Mr. Stéphane Perrault: Essentially, there are two aspects. One is, from an operational point of view, are there hurdles that we had to confront? What were those hurdles? There's a technical aspect to success in this way.

The other one is the voter experience. That's where it's important to get out into the communities and speak to the users, and not simply do a survey that may or may not have much uptake.

The Chair: I'm sorry, Mr. Turnbull. That is all the time we have for your line of questioning. Thank you.

[*Translation*]

Ms. Gaudreau, you have the floor for two and a half minutes.

Ms. Marie-Hélène Gaudreau: Thank you very much, Mr. Chair.

Once again, I found it very interesting how the relevance of the pilot project will be measured and the results it will produce.

I like pilot projects, in that they are tests that also allow us to have long discussions afterwards. Maybe that's why I don't have a lot of questions for you, but I do have one.

In Quebec, we put candidates' faces on ballots.

Is that also the case currently in Nunavut, or is the situation somewhat the same as in the rest of Canada?

Have you thought about that situation?

Mr. Stéphane Perrault: I think that's a great question, and I thank you for asking it.

Yes, I have. I have to say that it raises challenges.

The Canada Elections Act, as it currently stands, doesn't allow for faces to be added to ballots. However, I think that option should be explored in the longer term.

In that case, I would also try the pilot project formula, but that project would not necessarily result in amendments to the act. We would suggest adding faces to the signs at the polling stations to see how that works.

Operational considerations should also be taken into account, including the production of candidates' images within a fairly strict time frame. We also have to think about the quality of those images. Some candidates may have reservations.

So that would be something we would want to experiment with. It won't be for the next election, but I would certainly do a pilot first, again, using faces on signs rather than on the ballot. We could see if there are lessons to be learned and go from there.

Ms. Marie-Hélène Gaudreau: That's really fascinating.

Thank you.

Thank you, Mr. Chair.

The Chair: Thank you, Ms. Gaudreau.

In the end, you didn't use three minutes today.

[*English*]

Ms. Idlout, the floor is yours.

Ms. Lori Idlout: Thank you so much. *Qujannamiik*.

I'm going to build on my line of questioning with regard to electors who happen to not be home in their communities on election day, because a lot of the time they have been away for weeks or months at a time, especially if it's medical travel.

As well, Nunavut, being such a huge territory, has three urban hubs—or four, maybe. In the west, we have Yellowknife and Edmonton. For the central part, we have Winnipeg, and then for the eastern part, we have Ottawa. As Mona pointed out, we have an increasing population of Inuit as well.

I wonder if Elections Canada has considered maybe doing special one-day polls in these urban centres to make sure that, for example, the medical patients' votes are counted.

Mr. Stéphane Perrault: It is a significant challenge for us to do that. I think we're taking an important step forward with this pilot to see what challenges we face and whether we can expand further.

At this point in time, people who are voting by special ballot in Nunavut will have the ability to use.... If, for example, they're in a hospital in Nunavut, out of their home, they will be served with a special ballot that includes Inuktut on it. If they are detained in Nunavut, they will be served with that offering. However, if they are detained outside of Nunavut, for example, we will not have different kits for different prisons across the country. Those electors would not have access to the special ballot. There are limitations to what we are doing now. I think we have to recognize that.

All electors from Nunavut can apply by mail, especially those who are outside of the district. If they are outside of the district for a significant amount of time, we would like to communicate as much information as we can so they can plan their vote and obtain a special ballot in Inuktut to cast their vote, but that would require an application online. We will not be distributing those kits directly across the country or even in the three hubs that you mentioned.

● (1150)

The Chair: Ms. Idlout, I'm going to turn the floor to Mr. Duguid, as your time is up, but I understand there may be some time coming back to you.

Mr. Duguid, the floor is yours.

Mr. Terry Duguid (Winnipeg South, Lib.): Thank you, Mr. Chair.

Ms. Idlout already mentioned that Winnipeg is a service centre for many Inuit who come south for medical treatment and other services, and I'd like to cede my time to her.

The Chair: Ms. Idlout, I give you the floor.

Ms. Lori Idlout: *Qujannamiik* so much, Terry. I appreciate that very much.

Just to continue the discussion about ensuring that electors can make their votes count, given the barriers, I wonder, as well, if there has been consideration of the important roles that the election officers have in the communities. I'm not too sure about how many of your staff will be bilingual in Inuktitut. I think that a lot of the time, unfortunately, we might find that the staff you end up hiring are bilingual in only English and French, whereas candidates might have scrutineers who are bilingual in English and Inuktitut.

I wonder what kind of resolution might happen if the bilingual Inuktitut scrutineer has a difference of opinion with what's going on when the votes are being counted for the different candidates.

Mr. Stéphane Perrault: That's a very good question.

The role of the scrutineer, as always, is to observe the count and make note of any disagreement that they have, and there are opportunities for either a recount or a contested election before a court. There are legal remedies for that, but that is not unique to that.

It is a challenge to recruit. It's a challenge across the country, but it's even more of a challenge in Nunavut. We always seek, as much as possible, to have people who speak Inuktut, but we are not always capable of recruiting every poll worker who can speak it. That is the case. As much as possible, we will have at least one person at each poll to assist anybody who has linguistic challenges.

Ms. Lori Idlout: Thank you.

I think I just have a little bit more time.

Just to keep broaching the idea of the opportunity that elections can have with having special polls outside of Nunavut.... I just lost my train of thought. Damn it, I had such a good idea.

Having special polls is such a good opportunity to really make sure that some of the barriers that are experienced in the different communities within one riding, with having to fly out from different communities and with the challenges of weather.... By the way, I am excited to have the same election day as the Nunavut election day. I think that's a great opportunity to make sure that there's increased voter turnout. I think electors would prefer to vote on the same day rather than one week apart. I do hope that with the approval of this pilot project, we do consider how elections.... I don't know the terminology they use about how people would be less likely to go to vote if they are one week apart.

I'm glad to hear that you would make special provisions so that people in hospitals, at least in Nunavut, are visited by election officials to make sure they can vote as well. Hopefully that also goes for elders who might not be mobile.

● (1155)

Mr. Stéphane Perrault: Mr. Chair, with your permission, I would seize the opportunity to talk about the challenge.

I understand the enthusiasm for having a single day of voting in terms of having people drawn on the same day. However, there's the availability of locations and, more importantly, poll workers. We cannot have poll workers administering two sets of rules with different identification requirements at the same time.

Recruiting poll workers for a federal election is a huge challenge. We spoke about the challenges of having enough who speak the language. Having to compete for recruitment with any provincial or territorial management body would have an extreme impact on the availability of services.

I would caution the committee. Hopefully, if it does come to study Bill C-65, I can speak to it, but I do not recommend overlapping provincial and territorial elections with a federal election.

The Chair: Thank you very much, Mr. Perrault.

I'm sorry, Ms. Idlout. We do have to keep going here.

My apologies to Mr. Duncan, as I accidentally skipped him when going to Mr. Duguid. Nonetheless, he'll still have the same amount of time.

Mr. Duncan, we'll go to you for five minutes, and that will conclude this round.

Mr. Eric Duncan (Stormont—Dundas—South Glengarry, CPC): Thank you, Mr. Chair. It's no problem. I have a thick skin, so I've gotten over it quite quickly.

Mr. Perrault, thank you for being here today.

I want to build on exactly that topic of the overlapping election date as proposed in Bill C-65. It would present some massive logistical challenges in terms of polling locations and the human resources side of things for poll workers in a federal election and a territorial election. You've alluded to that.

I also want to get your comments on this. When we talked about this pilot project and the supports, you mentioned in your comments and throughout this morning about Elections Nunavut helping with those language requirements and verifications. Are you confident, or less confident, that on election day—if the counts are on the same evening and the same night—you're going to have the human resources in Nunavut, and you mentioned in Ottawa as well, to be able to prepare the ballots?

Will you, under the special voting rules and special ballots, for example, be able to interpret those that need to be deciphered?

Mr. Stéphane Perrault: Yes. Our consultations with Elections Nunavut, based on their experience, show that it is quite possible to do the count using multilingual ballots in Nunavut. It may not be the same elsewhere in the country with other indigenous languages, but it is possible.

There is, as we've discussed, a significant community of people who speak the language here in Ottawa. We are confident that we are going to be able to recruit people to it.

Mr. Eric Duncan: Specifically, right now, it is proposed in Bill C-65 that the election days would be overlapping. It's one thing to partner with a territory—Elections Nunavut in this case—but to have the HR necessary on election night for special ballot counting.... I'm just thinking. I just looked up the numbers quickly. There are 22 districts and ridings in the territory for that. There are dozens of candidates and multiple languages additionally that are used in the territory. With the overlap, are you still going to be able to have the HR that's required?

You do mention that there is, but when they're running their own election, I'm sure they have the same recruitment challenges for poll workers and for those who speak the language. Is that not going to be an increased challenge in this case?

Mr. Stéphane Perrault: We are relying on their experience but not their resources to conduct this pilot. If there was an overlapping election on the same day, on polling day, that would present important challenges, whether or not we do this pilot. Simply the ability to have locations and staff, poll workers, to conduct the election would be a very significant challenge.

Mr. Eric Duncan: My last question is on the report that you will do back to our committee on this pilot, and our support to do so.

In reviewing all of this, when we look at the poll-by-poll results or how individuals voted, it shows them by poll, and then group one or group two of special voting rules. Just looking at the last election in Nunavut, in 2021, there were 614 votes under the special voting rules, with only 12 rejected ballots as part of that, but it was about 8.4% of the votes cast. Are you able to break down further, just for numbers' purposes, whenever somebody would complete a special ballot, what percentage of individuals chose to write their special ballot in Inuktitut?

Then, if there were challenges—you mentioned that the spelling and the symbols could be a bit different—would you be able, in this circumstance, to break that down further, just to understand the scope, and if there is a challenge with that, the volume or magnitude of that, or lack thereof, if that would be the case?

● (1200)

Mr. Stéphane Perrault: Yes. I do not expect to do that examination on polling night, because the priority there is to get the results out, but certainly once that task is completed, we would examine unusual rejection rates. We could open the poll bags and look at how many ballots were cast using which language and so forth. There is an opportunity to take the time to study this carefully.

The Chair: Thank you, Mr. Duncan.

Colleagues, that concludes our discussion with Monsieur Perrault and Madame Morin.

I want to thank you both very much for being here.

Just briefly, for the benefit of both committee members and the public who may be watching, in terms of the next steps here, I have asked our analysts to draft a report on this subject. That will come to the committee for consideration. At that point, we will determine whether or not we want to send that report, as is or amended, back to the House. That will be our contribution to this part of the procedure. Then, as has been mentioned, our colleagues over at the Senate, in the legal committee, will also have to render their own judgment.

In terms of the next steps for this, we will await the report from our analysts, and we will have an internal discussion. Mr. Perrault, we hope to be able to get back to you in the not-too-distant future with our findings and our analysis on that.

In the meantime, colleagues, that was a great meeting and very interesting discussion.

Thank you, Ms. Idlout, for joining us and providing your contributions here as a guest member.

We're going to suspend briefly, colleagues.

[*Translation*]

When we come back, we will continue the meeting with a completely different matter. We'll see you in a few minutes.

● (1200)

_____(Pause)_____

● (1205)

[*English*]

The Chair: Okay, colleagues.

[*Translation*]

We will now begin the second part of the meeting.

[*English*]

We are transitioning into a different conversation now, colleagues.

Welcome to Mr. Genuis.

Ms. Mathyssen, welcome back.

Colleagues, we are here to discuss the question of privilege related to cyber-attacks targeting members of Parliament. We had several meetings in relation to this discussion in the last session, and we have some meetings dedicated to continuing the discussion as we move forward in this session.

We have a number of witnesses with us today. We do have some technical audio difficulties with the witness who's appearing online, but I would like to get us moving, and I hope we will be able to troubleshoot that in the very near future.

Appearing today we have with us Michel Juneau-Katsuya, former chief of the Asia-Pacific desk at the Canadian Security Intelligence Service. From the Centre for International Governance Innovation, we have Aaron Shull, managing director and general counsel; as well as Wesley Wark, senior fellow. From the Inter-Parliamentary Alliance on China, joining us online is Luke de Pulford, who is the executive director.

Colleagues, we are going to get under way.

Witnesses, you will have five minutes each. Mr. Shull and Mr. Wark, I understand you may be splitting your time, but it will be five minutes in total for your testimony in the introductory component here.

With that, I'm going to go to Mr. Juneau-Katsuya to begin.

The floor is yours, sir.

● (1210)

[*Translation*]

Mr. Michel Juneau-Katsuya (Former Chief of the Asia-Pacific Desk, Canadian Security Intelligence Service, As an Individual): Thank you, Mr. Chair.

Members of the committee, thank you for giving me another opportunity to share my observations and concerns about the future of our nation.

[*English*]

I was asked to comment on the question of privilege related to the cyber-attack targeting members of Parliament. In short, expect a sharp increase of cyber-attacks in the next years targeting not only members of Parliament but many elected officials of all government levels: federal, provincial and municipal.

Cyber-attacks have been and will remain the weapon of choice for many threat agents. This implies direct and substantive attacks against elected officials, institutions and our democratic systems. The intelligence community identifies basically five threat agents: state-sponsored attacks, radicalized citizens, organized crime/hackers, political activists and insider threats.

In terms of state-sponsored threats, in the last two years, very dark revelations have come to be known publicly about how the current and previous governments have neglected or avoided—sometimes intentionally—acting against foreign interference threats. Since the cat is now out of the bag, foreign agents will be forced, for a while, to work a little bit more covertly, so cyber-attacks will be chosen. Today, we hope the public's and elected officials' awareness has been raised, but it's not enough, sadly. When it comes to cybersecurity, Canada is last in investment compared to others in the G7 and the Five Eyes.

As the work of the committee demonstrates, you are still working on the issue, and many of you must feel like you are pounding your head against a wall. Unfortunately, petty political gains prevent Canadians from receiving the necessary protection. Not enough has been done on the legal side, like bringing modifications to the Criminal Code. A bad course of action has been selected, I must say, despite the fact that many experts advised going in different ways. From the public's perspective, this has only increased the bitterness and the loss of confidence in our institutions.

[*Translation*]

I repeat: We inevitably expect a sharp increase in cyber-attacks against elected officials in the coming years.

Offensive powers such as China, India, Russia, Iran, Israel, Pakistan, Saudi Arabia and many others will have to change and adapt their strategies. They will also have to reduce their presence on the ground, at least for a while, and be more subtle and sneaky.

[*English*]

Thus, when launching more cyber-attacks against officials, various forms will be deployed: continuous negative and supportive campaigns against people opposed to them or in favour of them, hacking various systems to gain sensitive information, and neutralizing communications and compromising data by targeting specific individuals.

The nature of the work of elected officials is to travel to meet their constituents and to sometimes work at home—everything needed to weaken our cybersecurity. Therefore, more discipline, more awareness, more verification, more ongoing education and more vigilance are needed.

You must have noticed that I've used the words “elected officials”. I stress that we need to work with the federal, provincial and municipal levels. Currently, cities like Toronto, Vancouver and Ottawa, and even smaller cities like Brossard, Markham and many others, are under the influence of agents of China, as we speak, at the highest level. This is not fiction; this is fact. Do you want names? I have names. National security without the participation of the provinces is just wishful thinking.

● (1215)

[*Translation*]

The House of Commons Sergeant-at-Arms reports that there have been 800% more cyber-attacks against elected officials since 2018. The Royal Canadian Mounted Police, or RCMP, has noted that since 2023, it has received 65 times more requests for protection and doesn't have enough staff to protect all members of the House of Commons. In Quebec, since the last municipal election, more than 10% of municipal elected officials, more than 800 people, have resigned because threats were made against them or their families. In the last provincial election in Quebec, they had to give candidates bulletproof vests and bodyguards.

[*English*]

I will stop at this point, and I will be glad to take questions to develop a bit further the points that I have presented.

The Chair: Thank you.

Mr. Shull and Mr. Wark, I'm not sure who would like to go first.

Mr. Wark, it looks like it's you. The five minutes between the two of you will begin now. The floor is yours.

Dr. Wesley Wark (Senior Fellow, Centre for International Governance Innovation): Thank you, Mr. Chair.

Aaron and I can be a dog-and-pony show, but I'm not sure how much value I can give you in 2.5 minutes. I'll do my best, but we are really appearing here as individuals.

The story of the APT31 cyber-attack—CSE calls it a cyber-incident—is a complex one, and I hope it might be of some assistance to the committee to provide my perspective on it.

The Canadian public and the members of Parliament first became aware of a cyber-attack, or cyber-incident, by a PRC entity known as APT31 in March 2024 when the United States Department of Justice unsealed an indictment against seven APT operatives. The indictment revealed that the efforts of this PRC group spanned some 14 years and targeted U.S. and foreign critics, businesses and political officials. One of its many targets was the Inter-Parliamentary Alliance on China, IPAC, which experienced an attack in January 2021 that was technical in nature and that was designed to elicit details of a target's IP addresses, browser types and operating systems through spearphishing. Caught up in this reconnaissance attack were a number of Canadian parliamentarians. The attack was understood as being unsuccessful.

CSE and its cyber centre were at the forefront of efforts to identify this cyber-incident—in fact, CSE was first tipped off by a trusted foreign partner—and to work with the House of Commons administration. Collaboration between CSE and the House of Commons administration is regulated, as I think you know, by an MOU first signed in 2016. Testimony at PIFI on September 24 indicated that a new version of the MOU has recently been signed, stimulated by lessons learned from the APT31 case.

Documentation provided to PIFI, including a chronology of events, indicated that information sharing among CSE, the cyber centre and the House of Commons IT security team about the APT31 reconnaissance was neither seamless nor sufficient in 2021.

CSE's mandate and capabilities need to be understood. It has a sophisticated sensor intrusion warning capacity that it deploys on networks and in the cloud to protect federal institutions and other levels of government. Here, I must disagree with my colleague, Mr. Juneau-Katsuya, in terms of understanding Canada's cybersecurity capabilities. The sensor capacity that CSE has developed has won praise from Canada's Five Eyes partners as best in class. It was first deployed to protect Parliament, starting in 2018, and has since been expanded.

According to the most recent annual CSE report, the organization blocks on average 6.6 billion intrusions a day. When CSE becomes aware of a cyber-operation targeting Parliament, it passes technical information about that attack to the IT security staff of the parliamentary administration for further action. CSE does not engage directly with parliamentarians in terms of providing threat warnings, in contrast to the process set in place for CSIS according to a ministerial directive issued in May 2023. CSE is not a domestic security service. However, it does have an assistance mandate under the CSE Act, and it can provide supportive intelligence and technical means to CSIS.

A directive issued by the chief of CSE in September 2023, and provided in an institutional report to PIFI, emphasizes the significance of its assistance mandate, as well as the need to—and I'll quote from that directive—“Ensure the timely dissemination of its products to the appropriate consumers of intelligence", including the House of Commons administration. That important principle must be upheld and continually tested in practice.

Going forward, and I will end on this point, I believe it will be particularly important—

● (1220)

The Chair: Just one moment, Mr. Wark. I'm sorry.

Was there a point of order?

Mr. Blaine Calkins: I'm hearing French translation on the English channel right now.

The Chair: Okay. It's working now.

I pressed pause. You're at about a minute, but I'll offer you a couple of seconds more to buffer for that.

Go ahead.

Dr. Wesley Wark: A couple of seconds more.... I remember when it used to be 10 minutes, Mr. Chair.

Going forward, I believe—and I'll just end on this point—that it will be particularly important for parliamentarians to be informed when appropriate and to inform themselves about threats posed by cyber-attacks. Parliamentarians cannot be mere passive consumers of warnings. While cyber-attacks come in multiple nefarious forms, online information operations deploying disinformation and malinformation may ultimately prove to be the greatest threat to the activities of parliamentarians and to the trust Canadians place in Parliament.

Thank you, Mr. Chair.

The Chair: Mr. Shull, were you going to add commentary here? There are a few seconds remaining.

Mr. Aaron Shull (Managing Director and General Counsel, Centre for International Governance Innovation): No, that's fine. We'll pick it up in the questions, Mr. Chair.

The Chair: Okay. Thank you very much.

We are going to try to turn now to Mr. de Pulford.

I'll just ask that you begin speaking. We'll know within a couple of seconds whether our technical difficulties have been worked through or not.

The floor is yours.

Mr. Luke de Pulford (Executive Director, Inter-Parliamentary Alliance on China): [*Technical difficulty—Editor*]

[*Translation*]

The Chair: Unfortunately, Mr.—

[*English*]

Mr. Luke de Pulford: Thank you very much, Mr. Chair.

I hope.... Is it okay?

The Chair: Okay. It sounds like we can hear you.

I'm just looking for a thumbs-up from our audio folks.

Okay. We're good. The floor is yours for five minutes.

Mr. Luke de Pulford: Thank you, Mr. Chair and members of the committee, and thank you to the staff of your committee for facilitating my participation.

As has been described, I'm the executive director of the Inter-Parliamentary Alliance on China, or IPAC. Around March 23, 2024, I learned that the U.K. government was preparing to make an announcement regarding a PRC state-sponsored cyber-attack against certain U.K. politicians. I was involved in some of the journalism leading up to it.

On the morning of the 25th of that month, the announcement was given from the dispatch box by then deputy prime minister Oliver Dowden, who did not mention the Inter-Parliamentary Alliance on China, IPAC.

Later that day, the United States Department of Justice unsealed an indictment that said the following: “the Conspirators registered and used ten Conspirator-created accounts on an identified mass email and mail merge system to send more than 1,000 emails to more than 400 unique accounts of individuals associated with IPAC.” According to the U.S. government, then, this was clearly an attack. It was targeting IPAC.

For this and other reasons, on April 4, 2024, 42 IPAC members from around the world wrote to Secretary Blinken, saying, “We were very concerned to learn that the APT31 pixel-reconnaissance effort had focused principally on the IPAC membership.... We were further alarmed that no IPAC legislators appear to have been warned by their own security or intelligence services.” The letter precipitated some correspondence with the U.S. State Department.

During this time, the FBI, through the State Department, kindly offered to take our distribution list and cross-reference it with their list of 400 emails associated with IPAC. They agreed to inform us of emails appearing on both lists.

On April 19, we got back a list of hits—121 hits, to be exact. On April 22, I sent a second list to see whether more emails were attacked than we had sent from our list, as 121 is nowhere near the 400 that were claimed to have been targeted by the FBI. Later, I got four more hits on May 3.

As a result, I was able to confirm via the FBI that members of IPAC from 18 Parliaments had been attacked: 120 parliamentarian members, 116 of these using parliamentary emails, and four using non-parliamentary emails. One of those four, by the way, was Canadian, and I believe he is in the committee today. In total, there were 18 Canadian politicians. That number included five staff around the world.

I sought then to brief every person targeted on what had happened, as I did not consider it ethical to refuse to disclose such information to those targeted. As a very gentle corrective to Mr. Wark, who has just spoken, Canadian MPs did not learn from the United States Department of Justice that they had been targeted. They learned principally from me and from IPAC.

I have very little time, so here are a few issues to highlight that may provoke discussion.

First, we have high confidence that the attackers had obtained IPAC's distribution list, which included personal email addresses of politicians, including one Canadian.

Two, we have confirmed that two targeted countries were informed in 2021, before the FBI had contacted governments in 2022.

Three, in 2022, the FBI communicated to host governments that this was intended to be part of a progressive attack.

Four, two IPAC members, a French senator and one other whom I can't name as an investigation is ongoing, were successfully compromised in or around March 2021, two months subsequent to being attacked by APT31.

Five, there will be many more email addresses targeted than those I've confirmed. All I have is the correspondence between my list and the FBI's list.

Six, the response of various parliamentary security services was highly variable around the world.

For the committee's consideration, my arguments would be as follows, and I'm very happy to discuss these.

First, we believe that failing to inform parliamentarians meant that they could not protect themselves or the sensitive information to which they had access from a progressive cyber-attack, including high-risk transnational repression cases, which many of our parliamentarians handle.

Second, telling parliamentarians that this attack was not successful or not serious is questionable at best and misleading at worst. There is a marked disparity between briefings given on this by the FBI and other government agencies, especially regarding the severity of these attacks.

● (1225)

Regarding other recommendations, hopefully I'll have time to cover those in questions.

Thank you very much, Chair.

The Chair: Thank you very much, sir, for your opening remarks.

With that, colleagues, we are going to head into the first round of questioning.

Mr. Genuis, the floor will be yours for six minutes.

Mr. Garnett Genuis (Sherwood Park—Fort Saskatchewan, CPC): Thank you, Chair.

My questions will be for Mr. de Pulford.

I'm going to try to cover a lot of ground. I know you could probably talk for six minutes on each of these, but just maybe in 45 seconds or less, why does IPAC matter? Why is IPAC important? Why is it a target for the PRC?

Mr. Luke de Pulford: The PRC doesn't like dissent abroad. It doesn't like people challenging its consensus. I tend to believe that where governments find themselves—because of economic dependency or because so many are rather diplomatically cowed by the assertiveness of the People's Republic of China—governments are less willing to speak out than parliamentarians can.

IPAC creates a space for parliamentarians to speak out and try to defend the rules-based order, which is under pressure from China. That's why it matters, and that's why China doesn't like it.

Mr. Garnett Genuis: Do you have reason to believe, beyond this particular attack, that IPAC is particularly in the sights of the CCP? Are there other data points that lead you to see this particular targeting?

Mr. Luke de Pulford: Yes, this is at least the second breach that we have suffered. Before we went to Taipei recently for our annual summit, somehow the People's Republic of China obtained our delegates list and targeted members in at least nine countries to try to prevent them from coming. This involved phoning up, in a very undiplomatic way, legislators in Colombia, in north Macedonia, in Slovenia, in various countries, to try to tempt them to go to China instead of Taiwan or to tell them that they might face consequences if they did come.

Unfortunately, IPAC has been in the sights of the PRC for some years, but it seems to be getting more severe, not less.

Mr. Garnett Genuis: It's unfortunate, but it's also a compliment to your important work.

How could APT31 have accessed IPAC's email list, in particular my personal email, and your delegates list, as you just referred to?

Mr. Luke de Pulford: Thank you. I think that's a very important question.

The reason we have high confidence that they obtained our distribution list is that the list of hits that came back from the FBI included exactly the same personal email addresses that we used to contact various MPs. Most of the other email addresses on that list were just parliamentary email addresses, which are public domain. But the very ones that we used to contact people on personal addresses, sometimes Gmail addresses or Proton Mail addresses—which, as you know, Mr. Genuis, included yours—were exactly the ones that the attackers had also used.

I do not know how they obtained that, but I do have one possible theory.

Unfortunately, somebody who used to volunteer for us, a man named Andy Li, was arrested in China under the national security law. He is in prison in Hong Kong, and he awaits sentencing for national security law crimes, some of which are associated with IPAC. We know that they breached his system, and they may have gotten our distribution list from him. Very disturbingly, when he was apprehended, he was taken to Shenzhen prison in China and reportedly tortured. This is something the UN rapporteur on torture has actually raised formally, so this isn't just idle speculation. Very unfortunately, in fact very tragically, we believe that that might have been the way they obtained our list.

● (1230)

Mr. Garnett Genuis: Thank you.

I think all committee members would join me in deploring the torture and the treatment of Mr. Andy Li. I know that this is very personal for members of IPAC who have worked with him. I think it's important that this is on the record.

Mr. de Pulford, some of the counter we've heard from the government is that it's really complicated to inform members of Parliament and that there are lots of different kinds of cyber-attacks. They've tried to bury this in apparent complexity when, to me, it's very simple. If a person is targeted and the FBI tells you they're being targeted, you would just pass along that information. There are a number of countries that did inform their members of Parliament.

To break through the false claims of complexity here, what happened in those countries? What went well in terms of the process of informing members of Parliament, and what can we learn from that?

Mr. Luke de Pulford: In my opinion, unless there is a very good intelligence reason not to inform parliamentarians, I can't see a good reason why elected representatives wouldn't be told they've been targeted in a progressive cyber-attack. They don't have the ability to defend themselves in such circumstances or to raise their security game. That would be my fundamental answer.

To your point about the other countries, I know that in Switzerland and Lithuania parliamentarians were warned. In fact, they were possibly even warned before the FBI had done its foreign dissemination requests, which is the mechanism through which it tells other countries stuff that they might want to tell their own parliamentarians because, obviously, the FBI can't contact you directly. That would be a violation of diplomatic norms.

In those countries, in Switzerland and in Lithuania, they briefed their MPs because they knew they'd been attacked. Clearly, they didn't see a big intelligence problem with telling them. They wanted them to be able to protect themselves and to know that they were a target.

Mr. Garnett Genuis: I'm almost done, but I have two quick final questions.

In those cases, do you know who told them? Was it their Parliaments? Was it their security agencies? That would be worth knowing.

Answer that one first, and then I'll ask my last question if there's time.

Mr. Luke de Pulford: My understanding is that they were briefed by both. Very often in different countries parliamentary security and various intelligence services operate in lockstep anyway, so I—

Mr. Garnett Genuis: Okay.

For my last question, I want to ask about the sovereignty concerns around the FBI that you mentioned.

[*Translation*]

Ms. Marie-Hélène Gaudreau: I have a point of order, Mr. Chair.

What we're talking about is so important. I know you've stopped the clock, but can we please speak more slowly, even if it means taking more time. I missed a couple of sentences. Those may have been key points for my speaking time.

[*English*]

The Chair: Okay. Thank you.

Mr. Genuis, you probably heard that in the translation. There has been a request for you to slow down the pace a little bit so the translators can keep up.

My clock shows 10 seconds, but I'm going to call it 30, and please do your best to slow down.

Thank you.

Mr. Garnett Genuis: I understand that the FBI has this protocol around not wanting to inform us directly. They want to go through our national governments and respect sovereignty, but we live in a democracy where Parliament is supreme. If Parliament were to ask an allied intelligence agency like the FBI to inform members of Parliament directly of threats they identified, do you think that would be a reasonable safety valve so that members of Parliament, including members of the opposition, aren't beholden to decisions of the executive to constrain our ability to access information that's important to our safety?

Mr. Luke de Pulford: Honestly, Mr. Genuis, I think that's a bit above my pay grade in the realms of diplomacy.

Certainly the information that the FBI gave us was exceptionally useful, and we're very grateful to them for it.

● (1235)

The Chair: Thanks very much, Mr. Genuis.

Mr. Duguid, the floor is yours for six minutes.

Mr. Terry Duguid: Thank you, Mr. Chair.

I want to thank all of our witnesses for painting a stark and concerning picture of the cybersecurity threats that our nation and other nations face, and that threat is increasing.

One thing that concerned me most was that our private devices were being targeted. We do have protections for our parliamentary systems, our parliamentary emails and some of the resources we have access to as parliamentarians. I'm a politician and I'm a parliamentarian, and there's lots of interplay. Sometimes the area is grey between the political and the parliamentary, as you know.

I'm wondering how you learn about attacks on private devices and how we can better protect ourselves as parliamentarians. Is there a gold standard out there somewhere? Is there a nation we could emulate? Mr. Juneau-Katsuya mentioned that we may be in the latter half of the pile with respect to G7 countries. Is there a nation on earth with the best training and the best cybersecurity hygiene that we could emulate?

I'll open that up to any one of our speakers.

Mr. Michel Juneau-Katsuya: Yes, there is definitely more effort performed by our Five Eyes allies when it comes to warning, training and raising awareness. In security, the human factor is always the weakest link. Contrary to maybe the academic comfort that Mr. Wark has put into the technology, it's not enough. Just take an example, a very benign example. Just this week, it was reported in the newspaper that a city councillor in Gatineau went to Russia with his equipment without even thinking that he could be compromised or something like that. This is naive to borderline stupid. In that perspective, it is the human being that is the weak element, not the technology.

We have phenomenal technology. CSE does a fantastic job. It's also supported by the private sector like Bell Canada and other groups that co-operate to try to protect us, but at the end of the day, common sense needs to be injected as well. From that perspective, from an operational point of view, we need to be capable of warning more and training more—with continuous training, not only the training you get when you get sworn in and when you arrive as a new member of Parliament, and then we forget about you for the next five years. No, we need to constantly repeat this, particularly with staff. It was mentioned during the Hogue commission that 11 candidates and 13 staff members were on the payroll of the Chinese consulate in Toronto. You can see that not only members of Parliament will be targeted, but their staff as well.

Mr. Terry Duguid: Mr. Shull, you weren't able to speak earlier. I'll give you the chance now.

Mr. Aaron Shull: Thank you very much.

I'd just like to say that the fact that Mr. Genuis's personal email was compromised is horrible. It was because of his job as a parliamentarian, so I thought I'd offer some concrete advice to this committee that I hope will be helpful.

First, allocate a parliamentary budget for personal cybersecurity protection. I'll tell you how I protect myself. I'll bet you that I'm probably better positioned than everyone in this room, and I'm just some guy. I'm not in the public eye and I'm not being targeted the same way you are. I use an encrypted multi-hop VPN for my data. I use biometric and cryptographically locked password managers. Each of my passwords is over 20 characters long and reads like gobbledygook. If you tried to brute-force my passwords, you'd have to really, really want to. I use the most sophisticated malware protection on the commercial market. I use a hardware multi-factor authentication for my most sensitive accounts. If you wanted to hack me, it would require a state-level actor who really wanted to get in. Then, for my most sensitive stuff, you'd have to get the keys out of my pocket.

For all of that we're talking hundreds of dollars, not thousands of dollars. Let's allocate some budget for that. Let's make sure that members of Parliament can be part of their own defence. If they're going after your personal accounts, it's not because of your personality; it's because of your day job.

● (1240)

Mr. Terry Duguid: Does anyone else want to comment?

I mean, to my mind, we should all have a cybersecurity audit to point out the weak points and how we can shore them up.

Mr. Michel Juneau-Katsuya: I'll give a quick statistic. A few years ago, I participated in research that was done by Telus. They interviewed 600 Canadian companies to try to find out where the weak link was within companies. They found that the greatest number of security breaches was done by the executive.

The Chair: Thank you, Mr. Duguid.

Mr. Shull, you can have my phone for an hour at the end of the meeting.

Voices: Oh, oh!

[*Translation*]

The Chair: Ms. Gaudreau, you have the floor.

Ms. Marie-Hélène Gaudreau: Mr. Chair, will I get three more minutes? I'm just kidding.

I've tried to sum up this very important topic.

Mr. Juneau-Katsuya, I'd like you to tell us about the consequences of our lax approach. What will happen to us in Quebec and Canada?

I'd also like you to tell us about existing role models. We talked about the presidential election in Taiwan. Who are our role models?

What do you recommend, other than password management?

Mr. Michel Juneau-Katsuya: There are several models, but they're not all infallible. I repeat that, at present, there is certainly a lack of collaboration between parliamentarians and intelligence agencies.

For a very long time, the Canadian Security Intelligence Service, or CSIS, and the Communications Security Establishment, or CSE, weren't even allowed to inform anyone except the prime minister or the Minister of Public Safety. Bill C-70 looks set to change all that. It remains to be seen how this will play out in practice.

One thing is certain: prevention is needed. Equipment can't do everything, and it can't stop everything. We need to develop a new business culture. I'm not talking about spyware or James Bond, but a business culture. We need to acquire new reflexes, because we're still very vulnerable. If we create a breach, we're literally letting everyone into the house.

The TikTok app has been cited as an example. Why is TikTok problematic? If someone blindly signs the terms and conditions and gives access to his or her phone, contact list, camera and microphone, which can be activated remotely, it becomes nothing less than clandestine wiretapping equipment.

Let's say I'm a teenager going to CEGEP or school. I'm not necessarily the target of cyber-attacks, but my contact list may contain information about my uncle, who works for the Department of National Defence, my mother, who works for the government, or my sister, who works for a very important strategic company. So we've just given a foreign power, like China, access to all this information.

Ms. Marie-Hélène Gaudreau: People listening to us may be thinking that it's no big deal that we have access to their contact list.

If the government doesn't act, what will the consequences be for citizens, for individuals? I want to know, so that we can react.

Mr. Michel Juneau-Katsuya: The consequences are that we are losing our strategic position on the international stage. We're losing the confidence of our allies, who are now looking at us and saying that Canada isn't serious. From this perspective, there's a whole section of our population that is poorly protected, that is vulnerable and that will be used.

According to experts, Canada has literally millions of zombie computers. These are computers that hackers have managed to get into, which are used to bounce from one computer to another. We lose track of them.

We're very ill-informed at the moment. In my statement, I said that Canada was lagging behind the G7 countries. We're not investing enough in the fight against cyber-attacks, and we're not doing enough to raise awareness among the population, particularly parliamentarians, who are the primary target.

As the effectiveness of foreign interference has been reduced on the ground, in the years to come, many more covert means will be used. Computer attacks are a case in point.

● (1245)

Ms. Marie-Hélène Gaudreau: Mr. Wark, earlier, Mr. Juneau-Katsuya said that cyber-attack was a weapon of choice. I have young adults at home. They tell me it's okay for people to know about their lives.

Do you agree that cyber-attack is now a weapon of choice? Why do we need to guard against it?

[*English*]

Dr. Wesley Wark: Thank you for the question. I will say this cyber-weapon is a very formidable one, and it has downed various vectors, as the professionals often refer to it. How did it become so formidable? I think there are really two answers to that.

One is a general answer. It's the nature of the digital lives that we all lead, which creates great openings and vulnerabilities, particularly for sophisticated foreign state actors to try to gain access to our data for all kinds of manipulative purposes.

The other answer is that it's a very significant threat. The other way in which cyber has become so significant is that it has created an entirely new kind of tool for foreign states to conduct espionage operations against adversaries or countries of interest. The foreign espionage aspect of cyber capabilities is one that I think we perhaps do not pay enough attention to in the context of all the discussions we've had about foreign interference.

Thank you.

[*Translation*]

Ms. Marie-Hélène Gaudreau: What you're saying is that when you use something that's free, you're a product. I think people need to be made aware of this.

I'll have two and a half minutes of speaking time later, because I haven't finished with the other two witnesses.

Thank you.

The Chair: Thank you, Ms. Gaudreau.

You're right on time, as always.

[*English*]

Ms. Mathyssen, the floor is yours for six minutes.

Ms. Lindsay Mathyssen (London—Fanshawe, NDP): Thank you so much.

Thank you to the witnesses for appearing today.

I certainly want to say how seriously we absolutely need to take this. You've made this very clear. I know we all take it seriously.

What I took from past conversations with our own security personnel and people in charge of this is that they were saying they didn't inform at the same rate. Eventually, they did, but they didn't inform because this was something that was stopped. It didn't get through the net. The idea was that there are so many attacks that if they were to let us know about all of them, that's all they would do.

What are your comments on that, per se? Do we have to change that mentality? Do we just say, let us know about all of them?

Could you comment on that a bit?

Mr. Michel Juneau-Katsuya: What will be targeted are the people of strategic importance. Parliamentarians are definitely people of strategic importance. Critical infrastructure is definitely of strategic importance.

There is a very easy technical term that everybody knows, called a “ping”. Every day they try. They ping. They knock at the door and see if the door is open. They try the handle. We don't necessarily need to know that because, yes, indeed, there are hundreds of thousands, if not millions, of attacks every day. From that perspective, we cannot....

When somebody is particularly targeted repeatedly because of what they do in their work, what they promote, what they challenge or what they denounce—like transnational oppression and things like that—they should be warned. They should receive better attention. They should also be receiving training to a certain extent, like I said, to develop a new business culture and a new way of being aware, because awareness is the only true defence that we have. The technical can only do so much.

Mr. Aaron Shull: Did you want me to come in on this?

● (1250)

Ms. Lindsay Mathyssen: Sure.

Mr. Aaron Shull: In preparation for this, I went through all of the other witnesses' testimony. If I were to offer advice to remedy what I saw in the previous evidence, I'd offer you three pieces of advice.

The first is, get your information-sharing house in order. It was one of those kinds of things where everyone didn't really know who was sharing what with whom, when, and why. There was a recognition that this was a problem. As my colleague Mr. Wark has indicated, the MOU has been updated. If you haven't seen that, I would encourage you to take a hard look at that and just make sure that it's tight. Also, treat this like a dress rehearsal. This is going to happen again and again. Just make sure you know who's on first with respect to the sharing of information, what happens and what that threshold is.

The second, as I had already indicated, is to have some personal money to protect yourselves. While the evidence indicated that the threat was stopped, we don't know—I'm sorry, Mr. Genuis—about your personal account, because that wouldn't have fallen within the IT department of Parliament.

The third is training, but not just cyber training. It's general awareness so that you can be your own best partner in your defence.

Ms. Lindsay Mathyssen: Both of you, Mr. Shull and Mr. Wark, have come before the defence committee before, where where we've had conversations. It's good to see you in another committee.

We had important conversations about how social media giants are being weaponized against Canadians as well. We're seeing social media bots taking over. Of course, algorithms that are written specifically to make as much money as possible, and advertisements that are surrounding those algorithms, are driving Canadians potentially down a specific path, and there is an ignorance or a denial of that by social media giants.

What do you think government needs to do in order to manage that in a different way than we have before?

Dr. Wesley Wark: Ms. Mathyssen, that's a very difficult question. I guess my first response is that I'm not sure governments have the primary responsibility in this regard. I think it's up to all Canadians to be educated about the nature of these kinds of threats and to exercise good judgment to the extent possible.

Regulating social media companies, particularly foreign giants, is a complex task. There are things that can be asked of social media platforms in terms of their own self-monitoring of malicious information and making more transparent the nature of their business enterprise so that we all understand what we're being subjected to. That would be helpful.

It's not consistent around the world, but generally the approach has been, so far, to try to work in partnership with social media companies. Perhaps we'll find that it's not going to work entirely satisfactorily, but it's going to be a difficult business, because they are giants.

Mr. Michel Juneau-Katsuya: There's a counter-discourse that needs to be developed from the government—

The Chair: I'm sorry, Mr. Juneau-Katsuya. Be very quick.

Ms. Lindsay Mathyssen: I'm sorry. Can he finish his sentence, just because of that disruption?

The Chair: Yes, he can.

Go ahead.

Mr. Michel Juneau-Katsuya: I totally agree that social media is currently weaponized, and with the arrival of artificial intelligence, this is going to be even worse. We definitely need to pay attention.

When it comes to cybersecurity and the element of Parliament, what is currently happening is that there's a lot of radicalization taking place, because some foreign countries are using social media to influence certain groups. The polarization that is taking place turns onto our streets, where we have MPs being assaulted by people, and that is happening in cyberspace as well.

That's the reason why we need to pay attention and to develop a stronger discourse—a counter-discourse to what's currently happening.

The Chair: Okay, thank you very much.

Mr. de Pulford, I just wanted to note that I know you've raised your hand a few times. The rules stipulate that, unfortunately, unless you are recognized by a member, I can't cede the floor to you. I just wanted to provide that clarification. Perhaps in the line of questioning to come, you'll be called upon, but I just wanted to offer that.

Mr. Cooper, the floor is yours for five minutes.

Mr. Michael Cooper: Thank you very much, Mr. Chair.

Mr. de Pulford, you noted that two politicians were successfully compromised. For clarification, was this part of the same APT31 progressive reconnaissance attack?

● (1255)

Mr. Luke de Pulford: Thank you for your question, Mr. Cooper.

We do not know, because we don't have evidence of that. I put that question directly to the FBI, and this is what they said: “We have no data showing whether the APT group took any additional targeting actions after sending the initial tracking link emails, but based on our cumulative knowledge, it would be assumed there would have been follow-on efforts by the cyber-actors to target those accounts.”

We don't have evidence of it, but I'll give you the timeline. They were successfully compromised two months after the progressive attack had begun—the pixel reconnaissance attack in January 2021.

Mr. Michael Cooper: Thank you for that.

You also indicated in your testimony.... The position the Government of Canada has taken was to say, “Well, these 18 parliamentarians weren't informed, but to some degree, it's not really that big of a deal because the attack was successfully thwarted.” You stated that this position is, if I heard you correctly, “questionable at best and misleading at worst”. Can you perhaps expand upon that?

Mr. Luke de Pulford: Yes, absolutely. I would like to say, very quickly, that people from all parties in Canada were attacked in this attack. The attackers didn't care which parties they were from.

However, I do not believe it is correct to say that the attack was unsuccessful. In fact, we've already heard from one of the other witnesses today that because they do not know what happened with Mr. Genuis's personal account, they cannot assure us that the attack was unsuccessful. It is simply not possible to say that.

Not only that, but, technically speaking, it's very difficult to ensure that anyway, for the following reasons: Many parliamentarians around the world were told these were low-level, unsuccessful attacks, like marketing emails. That in itself is not incorrect. Pixel embedding or pixel tracking is very common. However, in the hands of a state-sponsored hacking group like APT31, it's very different.

Very briefly—I know I don't have much time—what they can do is triangulate where that person is from. They can find a vulnerable router, and then easily hack that on the basis of the information they gathered from pixel reconnaissance emails, or much worse. We have a member whose emails were compromised and given to a political opponent for kompromat, so this is rather serious. It ought not to be described as a low-level, unsuccessful attack.

Mr. Michael Cooper: Thank you for that.

Mr. Juneau-Katsuya, the government put in place a ministerial directive in May 2023. However, the 18 parliamentarians were kept in the dark about this attack all the way through. It was only thanks to IPAC that they became aware of it. I would note that, following the issuance of the ministerial directive in May 2023, 24 government agencies and departments received a briefing in August 2023 about this attack, including the Prime Minister's department at the PCO.

What good is a ministerial directive if there is no follow-through? I would welcome any comments you have about the ministerial directive issued in May 2023 and about what, if anything, could be improved upon with respect to that directive.

Mr. Michel Juneau-Katsuya: It does very little good. If you do not share information about what's going on or learn from the experience of others, you're not going to get ahead of the bad guys. The bad guys will always win. We need to be capable of a bit more transparency. We also need to have accountability. That's one of the things that are lacking. A lot of people, including those in the private sector, will try to hide as much as possible.

Back in 2010, there was a successful attack on the Treasury Board of Canada that went through a law firm in Toronto. They went through the private sector to enter the Canadian.... To this day, we're not able to assess whether we have cleaned the entire Treasury Board system. The Treasury Board was shut down to outside communication for three weeks in that period of time.

It is very important to work in co-operation and share information and experiences in order to defend ourselves.

Mr. Michael Cooper: You would agree that it's a failure, and that the 24 government agencies, including the Prime Minister's—

The Chair: Mr. Cooper, be very brief, please.

Mr. Michael Cooper: —were briefed, but these members of Parliament were left in the dark following the issuance of that directive.

Mr. Michel Juneau-Katsuya: Mr. Chair, I didn't hear what he said.

● (1300)

The Chair: Mr. Cooper, we are over time. I will give you the opportunity to repeat the question very quickly, please, and get a brief response from Mr. Juneau-Katsuya.

Mr. Michael Cooper: I think—

Mr. Michel Juneau-Katsuya: We are learning. Everybody is learning. There's definitely.... In my 40 years of experience in the intelligence world, what I've seen in the government is a constant attempt to hide as much as possible those “failures”. But that's not the right way to do it. We need to be capable of sharing and learning from one another so we can get stronger and better at our job.

The Chair: Thank you very much, sir.

Next we have Mrs. Romanado, for five minutes.

Mrs. Sherry Romanado: Thank you very much, Mr. Chair, and I'd like to thank the witnesses for being here today.

I want to pick up on something that Mr. Juneau-Katsuya mentioned in a previous example of an incident that happened with the Treasury Board in 2010, and it was through a law firm.

Mr. Shull, you also mentioned how there are the physical tools that we can use, and there's also the training in personal responsibility and being careful about how we do the business that we do and get the training that's required. But in this case of APT31, we heard from the previous witness that it was through their organization that the email distribution list or email addresses were accessed. In the case in 2010, it was through a law firm.

There's educating parliamentarians in terms of us making sure that we're careful about what we're doing and that we're using every tool in the tool kit, as Mr. Shull said—and I would love to show him my phone as well after, to secure. There's the behaviour, and then there are the tools as well. But what would you advise organizations that we're involved with? For instance, many of us give our email addresses out when we're talking with people who want to meet with us, organizations and so on. They're creating distribution lists as well that we have no control over. We are public officials. We share our information so that people can get in touch with us.

How can we make sure that if a third party has these distribution lists, they're also being mindful of the fact that they are susceptible, especially if they're working with a lot of parliamentarians, to keep our information safe? What would you recommend to them as well?

Mr. Michel Juneau-Katsuya: To control and to be capable of raising awareness with a third party is a very difficult task, because you don't necessarily have control over what they do, how they do it, whom they train and stuff like that.

Again, it returns to general public awareness and being informed, but there's another element as well that should be taken. Sometimes you don't have control. As you pointed out, your email address is publicly known. People might take it and simply use it for their own purpose, and only at the end are you going to see that they used your address. However, when you do business with people, you should be able to ask them for certain standards. The Canadian government should be capable of imposing those standards as well, just like Public Works imposes certain standards when people contract with the government.

Somewhere, somehow, there's this kind of new business culture that I'm talking about. It still needs to be defined in its details, but somewhere, somehow, there's a general awareness and education that needs to start to percolate more to the general public.

Mrs. Sherry Romanado: Okay.

Mr. Shull, I'll give you a few seconds to answer, but I also want to get back to Mr. de Pulford, because he wanted to provide us some additional recommendations, and I don't think he had a chance to do so.

Mr. Shull, do you have anything to add to that?

Mr. Aaron Shull: I'll just respond to your question, which, if I understood it correctly, was about email addresses. You don't need to hack a database to get your email address. You can get it off the Internet.

There are really three questions that are germane to this committee's work. One, when does CSE notify your IT department, and what do they do as a consequence of that notification? Two, when do notifications go to members themselves, under what circumstances and who is indeed the lead? Is it CSIS? Is it CSE? Is it your IT department? That's what landed us in this discussion today. Three, what do you do as an individual member of Parliament when you leave here and pick up your personal device, because while your day job might stop for the day, threat actors are still looking at you as a person?

Mrs. Sherry Romanado: Thank you.

Mr. de Pulford, you wanted to add some additional recommendations. I think you only had two of them for us, but if you'd like to add to that, please do.

● (1305)

The Chair: You have about 45 seconds, sir. We're running over time. Thank you.

Mr. Luke de Pulford: Thank you for the opportunity.

There need to be more resources for parliamentary security. This is a David versus Goliath fight, unfortunately. That's the case not just in Canada but really across the world. There needs to be threat modelling for every MP and staff. It's very important. Staff are exposed too, because of who they work for, and are very often an easy way in to a member of Parliament. Staff need to be included in training processes. In some places, mystery shopper phishing has been done by parliamentary security in order to work out whether or not parliamentarians are up to standard. That could also be recommended.

Finally, those responsible should be sanctioned. In the United Kingdom and the United States, APT31, confirmed to have imposed this attack, was sanctioned. Well, 18 Canadians were attacked as well. Surely a similar remedy ought to be appropriate for them.

Thank you.

The Chair: Thank you very much.

[*Translation*]

Ms. Gaudreau, you have two and a half minutes.

Ms. Marie-Hélène Gaudreau: It will be difficult, Mr. Chair, but I've found a solution.

Gentlemen, you no doubt have pages and pages of information to answer my initial questions. In particular, they deal with the consequences of being lax. We haven't discussed the consequences for the economy, but we have talked about the strategic position of countries in the world, and about countries that could serve as models. Obviously, there are still many recommendations I'd like to hear about.

Mr. Shull, before I talk to you about my solution, I have a question for you about my password.

You said your password was 20 characters long. Mine is 16. Is that enough?

[*English*]

Mr. Aaron Shull: That's pretty good.

[*Translation*]

Ms. Marie-Hélène Gaudreau: That reassures me. I was told that it could take 100 years to find a good password.

What I wanted to talk to you about today is the CSE, which appeared before the committee.

I'll spare you the details, since you're well acquainted with the matter. However, as someone who isn't at all in the field, I found information on the APT28 attack campaigns since 2021 on the website of France's national cybersecurity agency.

In the end, I didn't need to ask you any questions because I found the entire procedure in a summary. That information is public on that site. In any case, you aren't answering questions, and you don't want to inform us.

My understanding is that we have a lot of work to do.

Mr. Juneau-Katsuya, why hide?

Mr. Michel Juneau-Katsuya: That's the killer question.

Why hide from foreign interference and national security breaches? Why hide when we have weaknesses and can reveal them? Why hide the successes we've also had? There have been successes, not just failures.

This culture of silence in national security has been killing us for years.

Is it a bad British legacy? I don't know. I couldn't say exactly, but we've had this kind of culture for too long. We have to abandon it, we have to change, we have to be much more transparent now.

Ms. Marie-Hélène Gaudreau: Mr. Chair, this has to change.

Thank you.

The Chair: Thank you, Ms. Gaudreau.

[*English*]

Ms. Mathyssen, you have the final questions. You have the floor for two and a half minutes.

Ms. Lindsay Mathyssen: I love it when I get the end bit.

Mr. Juneau-Katsuya, I'd love clarification from you on what you said in your opening remarks about cyber-offensive powers. You listed several countries. Can you just repeat them for us here?

Mr. Michel Juneau-Katsuya: Yes. They're China, Russia, Iran, Saudi Arabia and Israel, and we could go on. In 2015, the CSIS director, Mr. Michel Coulombe, testified in front of a Senate committee and referenced that 115 countries were practising cyber-offences or cyber-attacks. That was 115 countries back in 2015, according to the estimation of CSIS. That's more than half the countries.

It's very easy to be very offensive. Take a nerd who is good with computers, give him two Red Bulls and a computer, and he's good. That's it. That's all. He's gone. He's capable of doing a lot of damage.

What we need to understand—and Madame Gaudreau's question is so important—is the consequences, because we don't talk enough about the consequences, only to raise awareness and the level of urgency to start working on it. We're not necessarily able to curb the consequences right away, but we need to be capable of raising awareness, to pay more attention to what's going on and to realize that it will be worse before it gets better.

● (1310)

Ms. Lindsay Mathyssen: On this list, there are 115. Obviously, there are the countries we're not on good terms with, and there are the countries we are on good terms with. Is Canada doing enough with the countries we're supposed to be allies with on those fronts to make a dent?

Mr. Michel Juneau-Katsuya: These allies disappeared with the end of the Cold War. We moved from a military confrontation to an economic confrontation when the Soviet bloc disappeared. Now it's everybody for themselves.

What we're talking about now is national security going through solid economic viability for your countries. Everybody competes for the same market share, for the same contracts and for the same sort of competition economically, and that economic war has transferred itself into cyber.

The Chair: Thank you very much, Ms. Mathyssen.

Colleagues, that brings us to the end of the meeting.

Thank you very much, witnesses, for being with us.

Colleagues, this is a friendly reminder that we will be extending our next two meetings. We'll be beginning at 10:30 and ending at 1:30.

The meeting is adjourned.