HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

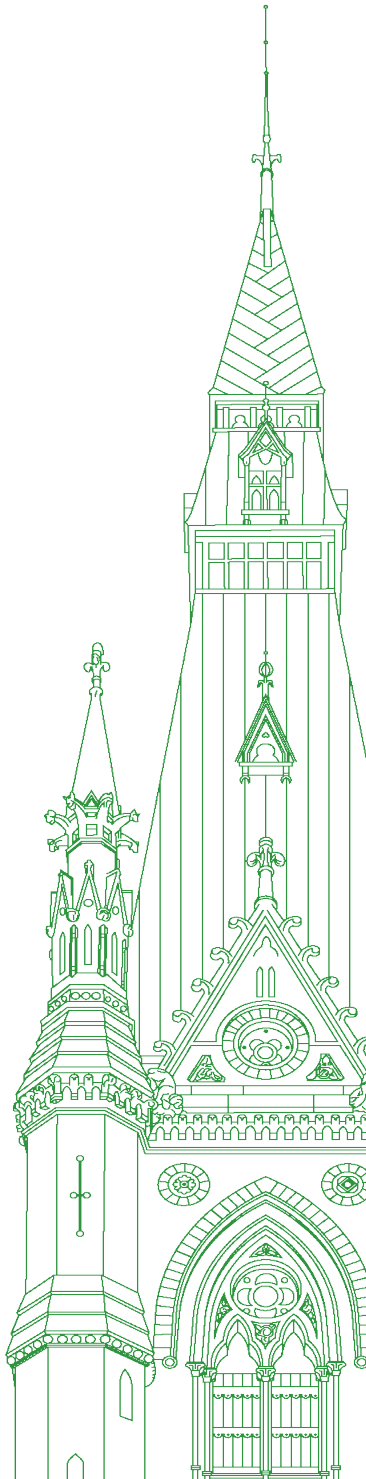
Standing Committee on Procedure and House Affairs

EVIDENCE

NUMBER 120

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Tuesday, June 11, 2024



Chair: Mr. Ben Carr

Standing Committee on Procedure and House Affairs

Tuesday, June 11, 2024

● (1105)

[*English*]

The Chair (Mr. Ben Carr (Winnipeg South Centre, Lib.)): Good morning, colleagues. It's good to see everybody.

[*Translation*]

I trust you had a pleasant Monday.

[*English*]

We are gathered for meeting number 120 of the Standing Committee on Procedure and House Affairs.

We are continuing, colleagues, as you know, our study on the question of privilege related to cyber-attacks targeting members of Parliament.

We will follow the same format today as we did last week, which is that the first hour will be in public and the second hour will be in camera. We'll have to take a couple of minutes to turn over once we hit the end of that hour.

Joining us today as our witnesses from the Canadian Security Intelligence Service are David Vigneault, director; Peter Madou, assistant director, requirements; and Bo Basler, director general and coordinator, foreign interference.

Mr. Vigneault, you and your colleagues will have up to 10 minutes for opening statements, and following that we will go into our line of questioning.

Welcome to our committee.

Thank you for being here, Mr. Vigneault. The floor is yours.

[*Translation*]

Mr. David Vigneault (Director, Canadian Security Intelligence Service): Thank you very much, Mr. Chair.

Good morning, members of the committee.

Thank you for the opportunity to be here today

The Chair: Mr. Vigneault, please wait a moment.

[*English*]

We're having a translation issue.

Okay. It looks like we're good.

[*Translation*]

Go ahead, Mr. Vigneault.

Mr. David Vigneault: Thank you, Mr. Chair.

The issues of cybersecurity, their nexus to national security, and attempts by adversaries to interfere in Canada, are becoming ever more complex. These issues require the full attention of the Government of Canada and all Canadians.

Increasingly, threats to the security of Canada take the form of cyber-threats. Malicious cyber-activity targeting Canada is growing in scale, complexity and sophistication, with cyber-threat actors seeking to advance their economic, political, security and ideological interests to the detriment of Canada and its allies. In short, the digital ecosystem has transformed the nature and conduct of warfare, espionage, diplomacy and trade.

[*English*]

Cyber-threat actors include those affiliated with foreign states, including military and intelligence services, as well as non-state actors.

CSIS actively investigates a variety of cyber-actors, including those from or associated with China, Russia, Iran and India. Regardless of who is directing their activities, cyber-threat actors employ a range of technologies and techniques to exploit weaknesses in information systems, target individuals to gain unauthorized access to systems and networks, or leverage infrastructure in Canada to achieve their broader strategic and geopolitical goals to the detriment of Canada.

CSIS is mandated to collect intelligence on threats to the security of Canada, to advise the government on those threats and, when appropriate, take measures to reduce them. This includes threats that emanate from the cyber-domain.

More specifically, when CSIS identifies national cybersecurity threats, it uses a variety of investigative techniques, including human sources, warranted collection and other methods to determine the scope, motivation, target and source of the threat.

[*Translation*]

The Canadian Security Intelligence Service, CSIS, engages broadly with industry, academia, governments, and indigenous groups to help strengthen Canadians' alertness and resilience to a growing cyber-threat environment. For example, since 2021 alone, over 70 briefings have been provided to parliamentarians on foreign interference and espionage, in which security awareness, including cyber-hygiene, was a key discussion point.

Additionally, CSIS routinely provides intelligence assessments to our government partners, allowing them to make informed policy and operational decisions. CSIS also shares these assessments and investigative leads with our trusted foreign partners in order to assist them in ensuring the integrity of the global information infrastructure upon which Canadian security relies.

[*English*]

However, I would like you to know that CSIS is part of a community of agencies and departments seeking to protect Canada from cyber-threats. While CSIS plays a vital role in the team, it works closely with other key players such as the cybersecurity experts at the Communications Security Establishment, the cyber centre, Public Safety Canada and the RCMP, just to name a few. Together we work to safeguard Canada and its assets, information and national security from an array of cyber-threats.

Regarding the committee's specific study, our colleagues and cybersecurity experts at the CSE and CCCS, with CSIS, produced a chronology of events detailing the interactions between our organizations and the House of Commons.

I will note that CSIS learned of any issues with the House of Commons IT system from CSE in January 2021. Following this, our agency directly briefed the House of Commons IT staff with CSE. From there, we worked with CSE and the House of Commons from January through April 2021 to investigate this activity.

This work outlined that IPAC members were targeted, but importantly, it found no instance of compromise on the system, nor any follow-on activity.

CSIS broadly disseminated intelligence products to clients across the Government of Canada detailing APT31's email tracking attempts on IPAC members in Canada. CSIS's work with the House of Commons predates the FBI reporting that was shared with both CSIS and CSE on any information that was released to the public by the U.S. in 2024.

● (1110)

When this incident was uncovered in early 2021, CSIS followed the protocols that were in place at the time. CSIS worked directly with CSE and the House of Commons to better understand the incident and its impact. Our investigation, alongside CSE's work, helped to inform the House of Commons on the specific technical measures that could be taken to mitigate the incident.

[*Translation*]

In 2023, the Prime Minister issued a ministerial directive to CSIS, which outlined and clarified CSIS’s role and responsibilities in relation to the investigation, notification and reduction of threats to parliamentarians. The directive outlines that, wherever possible within the law, CSIS must ensure that parliamentarians are informed of threats to the security of Canada directed at them.

This is uncharted territory for CSIS, and is providing an opportunity for reflection, learning and improvement. What is different today under this directive is that it compels us to have the conversation with our partners on how best to ensure that parliamentarians are informed on the potential threats they face. It may not be CSIS, for example, when we are not the lead department responsible for the issue at hand, but because the ministerial directive was issued to CSIS, we will lead the discussion on the process.

[*English*]

Mr. Chair, I think I will skip the recap of the chronology because of time. I will speak quickly to some legislative authorities.

Members of the committee, I think you all understand that the CSIS mandate is guided by legislation that is nearly 40 years old. In the face of rapid technological change and an increasingly complex cyber-ecosystem, gaps in CSIS authorities that limit its ability to detect, investigate and respond to foreign interference, including by sharing information, have become more pronounced.

Bill C-70, which currently sits before the House, proposes a set of focused amendments that will improve CSIS's operational response to foreign interference.

Among these amendments is a proposal to enable information sharing outside the federal government to build resiliency to national security threats, including foreign interference. This will help to build resilience before the threats materialize and will directly enable parliamentarians to make decisions that are more informed.

More broadly, Bill C-70 will ensure CSIS investigations are nimble and responsive, resulting in better collection of intelligence and advice, including for parliamentarians.

The last thing I would say, Mr. Chair, is that in reflecting on this situation in preparation for this appearance, I think my analysis with my colleagues is that everybody did the work they were supposed to do. However, the outcome for parliamentarians is not, I think everybody will agree now, in hindsight, what was desired.

I welcome the work of this committee. I welcome the work that CSIS can do to make sure that in the future we learn from this, and that the outcome for parliamentarians and for Canadians is a different one.

[*Translation*]

Thank you.

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

[*English*]

Witnesses, we will now go into rounds of questioning. Just for your awareness, there'll be six minutes allotted to representatives from each political party here today. Then we will go into a slightly reduced line of questioning following that.

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

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

Mr. Vigneault, on November 19, 2021, CSIS issued a classified analytical brief to 35 Government of Canada clients on the topic of the Beijing-directed APT31 cyber-attack campaign. Of the 35 Government of Canada clients who received the briefing, did that include the Prime Minister's national security and intelligence adviser?

● (1115)

Mr. David Vigneault: Mr. Chair, I do not have the specific distribution list. I can say that, generally speaking, such a product would indeed be distributed to the Privy Council Office, and that would include the national security and intelligence adviser. That's the general practice, but I will have to double-check on this specific item.

Mr. Michael Cooper: Did that likely include certain ministers, departments and deputy ministers?

Mr. David Vigneault: Mr. Chair, the way that the distribution of intelligence works is that the departments are responsible to the intelligence unit within departments to make this information available to their ministers. It would be hard for me to know.

Mr. Michael Cooper: Perhaps the easiest way to go about this is, would you, Mr. Vigneault, undertake to provide a list of the 35 Government of Canada clients who were briefed to this committee?

Mr. David Vigneault: I will do that, Mr. Chair.

Mr. Michael Cooper: Thank you.

Is there anything you can elaborate on with respect to that briefing?

Mr. David Vigneault: Mr. Chair, I do not have specifics of that briefing. What I can say is that, as an intelligence service working with our partners in Canada, as I mentioned in my remarks, but also working with our international partners, we have seen an increase in the sophistication and the aggressive nature of cyber-targeting by China, including by APT31.

Mr. Michael Cooper: Thank you very much.

On August 25, 2023, CSIS issued a second briefing, a classified intelligence assessment to what in the timeline are described as relevant Government of Canada clients, which referenced the ATP31 cyber-attack. Would that have included the Prime Minister's national security and intelligence adviser or PCO? Do you know who those relevant clients are?

Mr. David Vigneault: Mr. Chair, my answer to this question will be the same as my initial one. I can look into the specific distribution. My assumption is that it would be, but I will confirm with the committee.

Mr. Michael Cooper: You will undertake to provide a list of who those relevant Government of Canada clients are. Thank you very much for that.

I would note that August 25, 2023 was after the ministerial directive that you alluded to was issued on May 16, 2023.

That directive provides that: CSIS will seek “to ensure that parliamentarians are informed of threats to the security of Canada directed at them”. Why were the parliamentarians not informed pursuant to the ministerial direction?

Mr. David Vigneault: Mr. Chair, I think this goes to the core of the issue.

As I mentioned, in the cyber-ecosystem, you have different actors with different responsibilities and mandates. We each did our work in collaboration but also, to a certain extent, in parallel.

The initial information did not emanate from CSIS. It emanated from our colleagues at CSE. We work with them to work with the House of Commons.

On the question that the member is asking, if and when the ministerial directive would apply to CSIS is an interesting one. We are learning how, and we are adapting this ministerial directive.

Mr. Michael Cooper: I don't mean to interrupt, but—

Mr. David Vigneault: Mr. Chair, if I could just finish this, I would say that the key point here is that the assessment at the time was that the information had been shared with the House of Commons in order to mitigate that threat.

Mr. Michael Cooper: It hadn't been shared with the members of Parliament, which was the basis upon which the directive had been issued. Nonetheless, CSIS was briefing Government of Canada clients who were deemed relevant, presumably the Prime Minister's department, the PCO. You had said that, although there might be other agencies or departments who may be better suited to brief members of Parliament, CSIS would have the role of facilitating or leading discussions around arranging such briefings.

Did that happen?

Mr. David Vigneault: Mr. Chair, I'm not sure I would say that I would see that the role of CSIS would have been to organize such a briefing, but I think what is clear in hindsight is that the outcome for parliamentarians is not what anyone wanted, so my commitment to this committee is to learn from this, work with the committee and learn from the results of your work.

With our partners—I can tell you that I was talking to my partners at CSE—we all have the same objective, which is to make sure that in the future we're going to achieve a different outcome for parliamentarians.

I think this is one of the roles.... I would say, being very candid with you, that working with parliamentarians through the House of Commons is something we all need to get better at. We normally go through the House of Commons. I don't want members to think that this is a cop-out by saying that we shared the information with the House of Commons and we washed our hands. That was not at all the intent and the approach.

However, clearly, for people who were targeted by APT31, the outcome was not the one that people would have expected. My undertaking to this committee is that, with my colleagues, we will learn from this and make sure with our partners that we are achieving different outcomes in the future.

● (1120)

The Chair: Thank you very much.

Thank you, Mr. Cooper.

[*Translation*]

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

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

I too would like to understand how it happened. Then we'd be able to know what we should do if something like that were to occur again.

First of all, the chronology provided by the Communications Security Establishment to committee members reported that on February 18, 2021, it was decided that CSIS would inform the House of Commons.

The Communications Security Establishment gave CSIS a list of technical questions to help analyze the suspicious activity.

Why was it decided that CSIS would act as an intermediary between the CSE and the House of Commons?

Mr. David Vigneault: Mr. Chair, I don't have a precise answer about the intermediary role, except for the fact that each organization maintains relations with the House of Commons.

Both headquarters and the regions work closely with the House. I'm assuming there was some kind of connection. I'll ask Mr. Madou to answer that.

Mr. Peter Madou (Assistant Director, Requirements, Canadian Security Intelligence Service): Yes, it's no doubt owing to the fact that for quite a few years, we've had a lot of dealings with the House of Commons. It was no doubt a more straightforward way of proceeding. When a more strategic analysis of a problem is needed, it's usually CSIS that does it. Our colleagues at the CSE work more on the technical analysis side.

Hon. Mona Fortier: Who, according to you, is responsible for informing parliamentarians of attempted cyber-attacks like the one that occurred?

Mr. David Vigneault: CSIS, in partnership with its colleagues, assumed that as soon as work began with the House of Commons, the House authorities would inform the MPs. This didn't happen for various reasons.

I know that the conditions under which it happened were complex; it was during the COVID-19 pandemic. There were all kinds of restrictions on who would be present at the office, which complicated meetings. It was before the vaccine was available. Canadian Security Intelligence Service employees were in the office throughout the pandemic, which contributed to some of the confusion in the allocation of tasks.

Having said that, I believe we should all just ask ourselves how we could handle things better in the future.

Hon. Mona Fortier: It seems to me that there are sometimes a lot of cooks in the kitchen. We should try to find a recipe to follow and establish who does what. I think that's what we're trying to understand about the threat that occurred.

Mr. David Vigneault: Mr. Chair, that is indeed true.

When there are national security issues, CSIS usually takes the lead. In the case we are talking about, the national security threat was detected by our partners at the Canadian Centre for Cyber Security. So at the outset, the analysis was more technical.

Once again, we assumed that when the House of Commons authorities were informed, they would be the ones to pass the information on to the parliamentarians. That didn't happen.

We'll rely on the outcome of the committee's work, and take steps as an agency to arrange for the various spheres of activity to work together and analyze how to work closely with our partners to achieve good results, regardless of who does the actual work.

● (1125)

Hon. Mona Fortier: Do you think that only one of these three organizations can speak to parliamentarians? Are there situations in which these three organizations, or perhaps two of them, should share their information with them to keep them properly informed?

Mr. David Vigneault: Mr. Chair, from 2021 to 2024, the discussion surrounding national security and foreign interference changed dramatically in Canada.

I shouldn't speculate here, but in future there could well be an entity responsible for communicating information of this kind to parliamentarians. It could be the House of Commons, given its special relationship with parliamentarians, working together with CSIS and the CSE, both of which could also be involved. This would ensure that the best possible information is communicated to parliamentarians as quickly as possible to enable them not only to protect themselves, but also make the right decisions.

Hon. Mona Fortier: In closing, for the parliamentarians themselves, when someone has not been contacted in the proper manner, for example, are you informed? Were you so informed in the situation under discussion? Do you follow up with parliamentarians following an incident, no matter what happened? Do you think that's important?

Mr. David Vigneault: As I mentioned, in the case under discussion, when parliamentarians have been targeted by an APT31 cyber-attack, it wasn't done that way. As I mentioned in my opening address, we are accordingly going to work with our partners to ensure that we have all learned from this situation.

The Chair: Thank you, Ms. Fortier.

Hon. Mona Fortier: Thank you very much.

The Chair: Ms. Gaudreau, the floor is yours for six minutes.

Ms. Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): I think we've just pinpointed something as a result of the previous questions. There is no entity that takes control to prevent what we experienced. We may have been only speculating, but I think doing so is essential.

On several occasions, Mr. Chair, Mr. Vigneault said, “we assumed”. One should never assume. I'm always saying that.

Mr. Vigneault, can you reassure me by telling me that since this incident, memoranda have been systematically sent to the minister responsible?

Mr. David Vigneault: Yes.

Ms. Marie-Hélène Gaudreau: So if someone is on vacation, let's say, it won't end up in the wastebasket. If there's an important memo, it will be read and not treated as a minor alert. I'd like assurance on that.

Mr. David Vigneault: Mr. Chair, I can assure the member that CSIS is working in partnership with Public Safety Canada to make sure that won't happen. The minister was very clear about that.

Ms. Marie-Hélène Gaudreau: As for us, our role is to legislate, and I see that the act contains several items that place limits on what you can do. For us to be able to do our work, we have to know what you need.

Take a few moments to talk to us about that. I'm sure it's something you've thought about.

Mr. David Vigneault: Mr. Chair, as I mentioned in my opening remarks, the House is indeed currently studying a bill to modernize certain aspects of the Canadian Security Intelligence Service Act, Bill C-70.

It's interesting to look at things with a bit of hindsight. The act came into force in 1984, in the middle of the Cold War, following a commission of inquiry whose role was to review certain activities of the organization that had been responsible for national security at the time. To me, it looked like a rather defensive bill. Its purpose was to prevent certain lapses from recurring.

In my humble opinion, the circumstances that existed in 1984 no longer apply in 2024. The world has changed. Canada's image has changed and the threats we are facing have changed, not only in terms of complexity and the number of stakeholders responsible, but also the impact they have on the everyday lives of Canadians and Quebeckers.

The sharing of information amendments proposed in Bill C-70, which is currently being studied by Parliament, are absolutely essential. Their purpose is to simplify part of our data system, and the way we obtain orders from the Federal Court, while maintaining judicial authorizations. I'm sure that these changes will have a very direct impact on Canadians.

As Minister LeBlanc said, it was a first step, and other efforts would be required in future to modernize the Canadian Security Intelligence Service Act. Once again, when the time comes to protect Canadians against threats, it's important to know that the methods used by those who contrive them can change very quickly. We therefore have to make sure that we're not lagging behind these changes.

● (1130)

Ms. Marie-Hélène Gaudreau: I'm somewhat worried about how long the legislative process takes. We are now working on Bill C-70. By the time the amendments come into force, will the act still be effective and will it still address our needs?

It's urgent to do something right now. I believe we all agree on that. Can we succeed in providing measures as quickly as possible so that you have the tools you need?

At our most recent meetings, witnesses told us that they were all restricted to their respective sandboxes, in isolation, without being able to speak to the others. I even told a few of them last week that I'd like to be their client, because then I'd be able to get some information. I'm certainly not getting it now from House Administration, and I don't know if they're ever going to give us any information.

We need recommendations because I feel that Bill C-70 will be outdated by the time it's adopted.

What do you think?

Mr. David Vigneault: I think Ms. Gaudreau has put her finger on something rather important.

As a public servant, I'll allow myself to make the following comment.

When discussing matters of national security, it's important, to the greatest extent possible, not to politicize them. We need to be flexible in order to find a way to modernize the various statutes as soon as possible.

Technological changes are accelerating and we depend to an enormous extent on communication systems. Some companies have been changing their procedures and methods. A lot of work is also being done on access to telecommunications data.

What I'd like to see is a parliamentary committee which, instead of studying complex omnibus bills, regularly invites witnesses to appear and asks them about databases, progress in combatting threats, and how to address needs as quickly as possible. That's my message to the committee.

Ms. Marie-Hélène Gaudreau: Thank you very much, Mr. Chair. I'll stop now.

The Chair: Thank you, Ms. Gaudreau.

[*English*]

Ms. Mathyssen, it's over to you for six minutes.

Ms. Lindsay Mathyssen (London—Fanshawe, NDP): Thank you to the witnesses for appearing today.

It's been made clear—you yourself said it, Mr. Vigneault—that the assessment at that time was made; the information was shared and peak communication happened. However, we're constantly learning in a very quickly changing environment that.... Clearly, this is an important matter to raise to show that processes need to change. I appreciate the work that is continuing to be done.

It's important moving forward to think about those bigger issues. I know I'm focused on them. I'm clear in terms of where we need to go as a committee, but the questions I have are within a bigger scope.

I want to talk about the NSICOP report.

There was a shocking confirmation that proxies of Modi's government interfered in two recent Conservative leadership.... This isn't new information. The bureau reported two years ago on a 2022 intelligence assessment by CSIS.

The report stated:

> Government of India agents appear to have interfered in the Conservative's 2022 leadership race by purchasing memberships for one candidate while undermining another, and also boasted of funding "a number of politicians at all levels of government,"

The same week, Baaz reported that a Conservative member of Parliament was approached by a Government of India proxy to rescind their support for one of the candidates.

Can you tell this committee, or confirm, that the intelligence taken by CSIS was shared with that NSICOP report?

● (1135)

Mr. David Vigneault: Mr. Chair, with all due respect to the member's question, I will not be able to comment on leaked information to the media. That said, I can assure the member that we have shared and testified to all of the information that was relevant to the committee's review.

I will ask Mr. Basler, who is our counter-foreign interference coordinator, to speak about the volume and depth of our information sharing.

Mr. Bo Basler (Director General and Coordinator, Foreign Interference, Canadian Security Intelligence Service): Thank you, Director.

Yes, NSICOP certainly had access to any and all service information outside of some that was redacted for cabinet confidences, but any of our classified intelligence was made available to the committee. As well, a number of officials appeared before the committee to be interviewed and answer direct questions throughout their review. They also had all the information that was given to the independent special rapporteur when he was doing his review. The same information has gone to the National Security and Intelligence Review Agency as well as the public inquiry.

There are four separate reviews that have had access to, I think, at last count, at least from the service, over 8,000 documents that have been shared with the review committees.

Ms. Lindsay Mathyssen: At the beginning of this year, PressProgress reported that CSIS was investigating foreign interference in the nomination race for a candidate from Oxford. They cited that local Conservative Party officials had been interviewed by CSIS and local Conservative activists were visited by CSIS officials.

I ask the same questions in terms of whether it was shared with NSICOP. I understand not wanting to comment on leakages, but the fact that these leaks continue to happen must be concerning. I don't want to ask about the specifics of that, but overall, we're talking about these processes and we're talking about leaks and we're talking about improvements. Can you talk about the first bit of the question and the second?

Mr. David Vigneault: Mr. Chair, I would say that in this case our assessment was that it was investigative journalism as opposed to a leak in this specific story.

I will obviously not be speaking to the specifics of our investigative techniques or investigative interests, but I think what is very clear is that we have said publicly in our annual reports, in speeches, in appearances in front of this committee and other committees of the House and the Senate that CSIS has been concerned with foreign interference for very many years. It's part of our act. We have been investigating this, but what we have seen over the last number of years is an increased aggressiveness by a number of countries.

The speed and complexity at which the threat of foreign interference is coming at Canadians, yes, at the democratic processes, elections, but also at Canadians from different diaspora groups who are being interfered with in their democratic rights by foreign nations, this is something that is of grave concern to CSIS. This is why we have been speaking about this both publicly and privately to government. I think Canadians, through the work of this committee and other committees and the NSICOP and NSIRA and the commission of inquiry, are now getting a better sense of what is required.

Maybe the last thing I would say is that one of the best tools to address foreign interference is what we're doing right now. We're talking about it in public. Of course, I will not be able to share classified information, but by having more public discussion about these issues in different places with different people, we will increase resilience against these actors. It's not going to be CSIS or the RCMP or someone else catching people doing it all the time. We hope that we're good at what we do, but it's going to be Canadians in their day-to-day activities who will raise the flag and say, "There's something happening here. Maybe I should be talking about it."

● (1140)

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

Colleagues, we now go to the second round.

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

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

Turning to the NSICOP report, footnote 63 at page 17 of the report indicates that CSIS briefed the Prime Minister on February 9, 2021, about foreign interference activities by the Beijing regime, more specifically involving efforts to manipulate Canadian media, including "paying to publish media articles without attribution, sponsoring media travel to the PRC, pressuring journalists to withdraw articles and creating false accounts on social media to spread disinformation."

Did you brief the Prime Minister on February 9, 2021? Was it you?

Mr. David Vigneault: Mr. Chair, I do not have the report in front of me, but I will take the member's word that it's indeed accurate, the reference.

I do not remember that specific briefing. I will have to double-check if it was myself, someone from my staff or somebody else who briefed the Prime Minister.

Mr. Michael Cooper: Thank you. Could you undertake to find out as well if the Prime Minister had been briefed prior to February 9, 2021, on the same subject matter?

Mr. David Vigneault: Mr. Chair, we'll take that under advisement. We'll try to see what we can do. In different committees—

Mr. Michael Cooper: I would appreciate that. Thank you.

Mr. David Vigneault: —we have provided a number different chronologies. We'll try to see what we can do.

Mr. Michael Cooper: Thank you.

Page 17 of the NSICOP report goes on to state that the SITE task force observed during the 2021 election a coordinated campaign "aimed at discouraging Canadians, particularly of Chinese heritage, from supporting the Conservative Party". It states, "Specifically, different Chinese-language media outlets in Canada adopted the language of a PRC state media article, without specifically attributing it. Most of these media outlets were linked to the PRC via partnership agreements with the China News Service, the Chinese Communist Party's primary media entity".

Had a foreign influence registry been in place at the time, those media outlets would have had to publicly register in light of their partnership agreements with the PRC. Is that correct?

Mr. David Vigneault: Mr. Chair, I'm looking to my colleague here on whether he wants to opine on this.

I would have to defer the question to my colleagues at Public Safety Canada, who are devising the current regime. I would not have a definitive answer to provide to this committee.

Mr. Michael Cooper: Well, I would submit that the answer would be yes, insofar as it is an arrangement. A partnership agreement would be an arrangement with a foreign entity, correct?

Mr. David Vigneault: Mr. Chair, it appears to be the case, but again, I would not want to speculate. I'm not the expert on the foreign registry. Our colleagues at Public Safety are.

Mr. Bo Basler: I don't think we could expand further on the nature and scope of when a partnership agreement would come into force under the current proposed legislation right now. I think it would be a stretch for me to go that far.

Mr. Michael Cooper: Okay. Well, I realize that you might not be the authority on the subject matter, but if one looks at the legislation, it's quite clear that it falls within the definition of an arrangement. I would just observe that, based upon the NSICOP report and other information, including through Global Affairs Canada and the reports of a rapid response mechanism, it is well documented that during the 2021 election, the Beijing regime ran a disinformation campaign aimed at discouraging Chinese diaspora communities from voting for the Conservatives. You would agree with that.

Mr. David Vigneault: Mr. Chair, through the commission of inquiry presided over by Justice Hogue, CSIS, in partnership with colleagues, has made public some summaries of information, including specifically on this information. I think to be as precise as I can with respect to the member's question, I would refer the committee to that summary, which uses all of the classified information and the open information in coming up with the best possible story.

I think that would be the definitive story on this matter, Mr. Chair.

● (1145)

Mr. Michael Cooper: Do I have 15 seconds?

The Chair: No. You're over.

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

The Chair: Thanks very much, Mr. Cooper.

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

Mr. Mark Gerretsen (Kingston and the Islands, Lib.): Thank you, Mr. Chair.

There's a lot of talk going on lately about foreign interference, and I think you think that's a good thing. As you said earlier, Canadians need to be aware. Whether it's your work, the Hogue commission or NSICOP, this issue is out front in public. Is it safe to say that part of the reason for it is the work that's ongoing and the elevated importance of that work over the last number of years, Mr. Vigneault?

Mr. David Vigneault: Mr. Chair, that's a very interesting question. We've been reflecting on this issue.

In my view, I think we, CSIS and partners, are putting more resources and emphasis on this, because we have seen the threat increasing in the last number of years. We have seen a number of actors coming at it much more aggressively and doing things we had not seen before.

Mr. Mark Gerretsen: Knowledge is power, then. Knowledge is power. Having this information gives us and you and those responsible the power to be able to do something about it.

Mr. David Vigneault: Indeed it's the case. That's why, while respecting, in our case, the law of the Security of Information Act, and the partnership agreements with our partners to protect information, we have for a number of years now been talking publicly about foreign interference. That's why I do believe that a more organized discussion about these issues is what will make Canadians resilient.

Mr. Mark Gerretsen: Some of the information is public and can be discussed in public, but some can't. Some of the reports are classified for various different reasons, but some people can get access to those reports, obviously the Prime Minister, members of cabinet, the official leaders of each political party. If they have the information that comes from those classified sources, can they act on it or are they restricted in acting on it because the information is classified?

Mr. David Vigneault: Mr. Chair, I testified to this issue a few days ago in front of another committee, and I'll say a couple of things in reaction to this.

First, this is uncharted territory. We have never done it before, so we're all learning together.

Second, I think that people with the right security clearance, with the need to know, are indeed able to get briefings on these matters.

Third, I think that while respecting the law, there are opportunities and abilities for people to make some decisions based on that information without having to reveal it publicly.

Mr. Mark Gerretsen: That's what I was getting at. It's interesting. You made that comment at another committee, and this came up in a CTV exchange on June 9, just a couple of days ago.

The interviewer said—they were talking about the leader of the Conservative Party—"just because your leader is briefed on this intelligence does not mean that he can't act," which is what you've just said here. The interviewer went on to say, "In fact, it means he could act on that information. You had thought last week when we did an interview then"—the interview was with Mr. Chong—"that would not be the case."

Mr. Chong then went on to say, "I think they're not correct"—referring to you—"in saying that. Here's why: What the Prime Minister is asking Mr. Poilievre to do is to essentially tie his hands behind his back. Here's why. The Prime Minister is asking Mr. Poilievre to go through the Treasury Board Secretariat's policy on government security. That's the same process that other individuals, for example, on NSICOP, have gone through. That process would require Mr. Poilievre to sign an undertaking and to swear an oath of secrecy not to divulge this information to anyone else and, therefore, not be able to tell anybody else to act on this information to hold individuals accountable."

The host of the show then said, "Respectfully though, am I supposed to believe you over the director of CSIS?"

Michael Chong replied, "Yes, you are."

I'm not going to ask you to comment on that, because I know you're not going to want to weigh in on this, but you have made it very clear today that if you do receive information, even if it is classified information, you can use that information to make decisions, even if you're not allowed to reveal that information.

● (1150)

Mr. David Vigneault: Mr. Chair, that is my understanding.

I have a lot of respect for Mr. Chong and his remarks. I would welcome a discussion with him to maybe have a chance to better understand his point of view.

Mr. Mark Gerretsen: Thank you.

The Chair: Thanks very much, Mr. Gerretsen.

[*Translation*]

Ms. Gaudreau, the floor is yours for two and a half minutes.

Ms. Marie-Hélène Gaudreau: Mr. Vigneault, let's get back to what you said you would like to see.

I was just thinking about a parliamentary committee with oversight, and just enough power to be non-partisan and prevent things like leaks to newspapers.

Do you have any more comments on that?

Mr. David Vigneault: Mr. Chair, while pondering the member's question, I've thought of a few different models.

One example comes from our partners in Australia who, at regular intervals of just a few years, has a non-governmental third party review of all agreements and statutes governing national security. Their purpose is to ensure that, depending on the status of the threat, the tools in the tool box are the right ones and kept up to date. The aim of this kind of exercise is to take stock of the situation outside of electoral periods.

I've said several times over the past few years that Canada has been lucky, and that the threats it has faced were different from what other countries have experienced. Our geography, the three oceans bordering the country, and the fact that we have the United States as an economic and military partner, have enabled us to avoid the severe threat level that other countries have had to deal with.

So Canadians haven't had—and I'm delighted about this—to think about these questions in the same manner and with the same urgency as others. However, the world has changed and all the trends that have made Canada a prosperous, safe and sovereign country have been headed in the wrong direction for a few years now. I firmly believe that a different way has to be found to discuss these threats, including in Parliament, and that it has to be well-thought-out.

Ms. Marie-Hélène Gaudreau: In short, you mean that you really have to do an analysis of the Five Eyes' models in order to come up with one for us to be prepared to deal with the threats.

I've run out of speaking time.

Thank you.

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

[*English*]

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

Ms. Lindsay Mathyssen: Thank you.

Following up on Mr. Gerretsen's question, has the Prime Minister had the full unredacted NSICOP report for 11 weeks now?

Mr. David Vigneault: Mr. Chair, I would take the words of the MP, but for a period of time for sure.

Ms. Lindsay Mathyssen: There's no action. Okay. I was just double-checking.

I would like to give notice of a motion, Mr. Chair, in the time that I have. It's just notice, and we'll be sending it around shortly:

> Given the recent findings of the NSICOP Special Report on Foreign Interference in Canada's Democratic Processes and Institutions, the Standing Committee on Procedure and House Affairs order the production of all relevant memoranda, briefing notes, e-mails, records of conversations, and any other relevant documents, from departments and agencies, including the Canadian Security Intelligence Service and Communications Security Establishment Canada, concerning interactions with Conservative Party of Canada officials and representatives on the topic of foreign interference; and its impact on the outcome of the 2020 and 2022 leadership races, provided that:
>
> (i) both agencies tasked with gathering these documents apply redactions according to the Access to Information and Privacy Act;
>
> (ii) these redacted documents be deposited as soon as possible, but not later than Sunday, June 23, 2024, with the clerk of the committee to be distributed to all members of the committee in both official languages.

The Chair: We've got it.

I understand you're not choosing to move that motion, Ms. Mathyssen, so there remain—

Ms. Lindsay Mathyssen: I'm giving notice. I have to—

The Chair: Yes, absolutely. There remain 45 seconds in your questioning, if you'd like it.

Ms. Lindsay Mathyssen: Actually, I wouldn't mind building off what Madam Gaudreau was asking.

When I was in Taiwan on a trip, there was a great deal of discussion, of course, about what they face in terms of bombardment, foreign interference and the education of their own public that they move forward with. Have there been workings with the Government of Taiwan to learn from that, to educate their own public, even the idea of a minister of digital affairs?

● (1155)

Mr. David Vigneault: Mr. Chair, very quickly, I would not comment specifically on the interactions of CSIS with partners, but I can reassure the member that there have been indeed a number of partners in government who have engaged specifically on these issues with partners in Taiwan.

The Chair: Okay.

Thank you very much, Ms. Mathyssen.

[*Translation*]

Mr. Berthold, you have the floor now for five minutes.

Mr. Luc Berthold (Mégantic—L'Érable, CPC): Thank you very much, Mr. Chair.

I find it very ironic, yet again, to see the NDP jumping to the government's defence even though we've moved several motions to produce documents over a period of several weeks. Each time, the NDP voted with the government to prevent the production of documents. I therefore find it rather ironic that my NDP colleague should be introducing a motion today.

Mr. Vigneault, in your opening remarks, you mentioned the importance of not politicizing national security issues. I will return to that, because it's important to point out that politicizing national security issues doesn't mean you shouldn't talk about them; it doesn't mean that the opposition can't discuss them or ask difficult questions. What it really means is that certain information is being used to promote partisan interests.

Is that what you meant when you talked about politicizing national security issues?

Mr. David Vigneault: Mr. Chair, by and large, that's exactly what I wanted to say.

Allow me to reiterate that my current position involves a duty of confidentiality. Nonetheless, when partisan interests are taken into consideration, which is normal in a democracy—and we're lucky enough to live in a democracy—the fundamental questions can be somewhat blurred. From my standpoint, things do indeed become more complicated when they are politicized.

Mr. Luc Berthold: If the government turns a blind eye to some information, if it refuses to look at classified information to avoid embarrassing its party, if it refuses to act when it has information about a candidate who may have received support from a powerful hostile power, if it blames another association or simply refuses to shoulder its responsibilities, that amounts to politicizing debate on national security.

Would you agree?

Mr. David Vigneault: Mr. Chair, I don't think anyone will be surprised to hear that I won't be commenting on what the member said.

On the other hand, I can say that the discussion being held right now and the work being done by this committee are essential if Canadians are to be better protected against foreign interference and numerous other threats.

Mr. Luc Berthold: Please, Mr. Vigneault, it's important.

I wouldn't want people to think that the political debate surrounding the issues we are currently talking about is limited to the work of the committee or that it is only the result of some leaks. Decisions that might be made by a government that has partisan interests could also politicize the national security issue. It's undeniable.

Mr. David Vigneault: Mr. Chair, I'm going to exercise my duty of confidentiality with respect to these comments, but I appreciate the member's question.

Mr. Luc Berthold: Mr. Vigneault, who, within the machinery of government, can decide to declassify information considered confidential or top secret? I don't know how it works, but who can decide that information previously considered secret is now public?

Mr. David Vigneault: That's a very good question, Mr. Chair, but it's one to which there is unfortunately not a very good answer, insofar as there is no policy on declassification.

Let's take the Canadian Security Intelligence Service as an example. Information from the Canadian Security Intelligence Service is subject not only to the Canadian Security Intelligence Service Act and the Security of Information Act, but also to our practices and commitments. So the government does not have a policy on this, and there is no authority that can order a declassification.

Mr. Luc Berthold: Is it true that in the event of a serious national security matter, the Prime Minister can use the information and make it public?

Mr. David Vigneault: Generally speaking, in my experience, the disclosure of information is done in collaboration with the agencies.

I'll give you a very concrete example. The first time we named some of the countries involved in this incident, it was classified information. We did the work required to allow us to say that now, based on publicly available information and its impact on our operations, we can begin to say more about it.

It was therefore an iterative process, but it was not based on a government policy.

● (1200)

Mr. Luc Berthold: I don't have a lot of time left, so let's cut to the chase. It was nevertheless a directive from the Prime Minister that enabled you to release the information to the MPs who had been targeted by foreign interference, and to disclose information that had previously been withheld from these MPs.

Mr. David Vigneault: Mr. Chair, to be more specific, we used section 12.1 of the Canadian Security Intelligence Service Act, which is about reducing threats. That is the process, which is based on the CSIS Act, that enabled me to have the initial discussion with Mr. Chong.

Mr. Luc Berthold: You mentioned, earlier on—

The Chair: Unfortunately, Mr. Berthold, that's all the time you have. I'm sorry.

Ms. Romanado, the floor is now yours for five minutes.

[*English*]

Mrs. Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.): Thank you very much, Mr. Chair. Through you, I thank the witnesses for being here.

Monsieur Vigneault, you mentioned that your team met with over 70 MPs to brief them in the past couple of years. Is that correct?

Mr. David Vigneault: Yes, Mr. Chair, it is correct, 70 parliamentarians, and I think that, for Canadians, we're talking about more than 1,000 people we engaged with.

Mrs. Sherry Romanado: Can you confirm that the parliamentarians who were victims of this cyber-attack were all met with?

Mr. David Vigneault: Mr. Chair, I will have to go back to review that information specifically to confirm.

Mrs. Sherry Romanado: Will you undertake to do that? The directive of May 2023 was clear that all parliamentarians who are targets are to be made aware, so I would like to make sure that all parliamentarians.... We have some who will be coming as witnesses on Thursday, and we will be asking them if they were met with by CSIS to be briefed.

Mr. David Vigneault: Mr. Chair, I will undertake to confirm whether the MPs were met. However, I think it's very clear as well, in my testimony and from what was presented to this committee, that there was, as I said, the expectation when we were sharing the information that the specific information would be shared by the House of Commons. Also, the ministerial directive issued to CSIS came about two years later than...the incident, so I think it's important to keep these two points in mind in reflecting about what was done here.

Mrs. Sherry Romanado: Mr. Vigneault, you've had two years to be able to brief. You've had over a year since the directive in 2023 to get in contact with these members and senators who were affected. When I'm looking at what we've been hearing during this study, it's almost like the Shaggy song *It Wasn't Me*. I have the House of Commons saying it wasn't them; I have CSE saying it wasn't them and CSIS saying it wasn't them. In the meantime, parliamentarians, both in the Senate and in the House of Commons, are sitting here as targets.

There seems to be a real breakdown, and no one wants to take responsibility for the fact that the parliamentarians, the very people you say are targets of foreign interference, are actually not being briefed. This is a very big concern of ours. I understand that you want to learn from it, but in the meantime, our adversaries who are doing this are getting away with it.

What structure needs to be put in place to ensure there is a constant dialogue with the very people who are being targeted, whether by state actors or non-state actors? Maybe I have information that you don't have. It seems that is missing. When we say it's the House of Commons that was responsible for letting the parliamentarians know, what about the Senate? Is the House of Commons IT group responsible for the Senate as well? There seems to be a lot of “it's not my problem” or “I did my part of the assembly line" but at the end of the day, it's not getting done. What do we need to do to get it done?

Mr. David Vigneault: Mr. Chair, in my remarks and my previous comments, I think I've been clear that the outcome that we have seen here is not the one that members of Parliament or senators in the IPAC would have wanted. It's definitely not the outcome we would have wanted, because our work on national security is to make sure that we are enabling people to defend themselves and to do our work.

Therefore, the undertaking I've given this committee is that I, with my partners at CSIS, with CSE, and with the House of Commons and the Senate, will learn from this and look at how we are aligning the different authorities, because we also have to respect the mandates and laws that govern our actions. How do we combine these to make sure that the outcome is different in the future?

I was very sincere, Mr. Chair, when I made that offer before. That's probably the best answer I can provide to the member.

● (1205)

Mrs. Sherry Romanado: I have no more time, so I'll ask more questions during the in camera session.

Thank you.

The Chair: Thank you very much, Mrs. Romanado.

Colleagues, we are going to suspend—

Mr. Blaine Calkins (Red Deer—Lacombe, CPC): Mr. Chair, can I just ask a question of my committee colleagues before we do this?

The Chair: Is this a point of order, Mr. Calkins?

Mr. Blaine Calkins: I'd like to know the rationale for and purpose of moving in camera. The director has basically said that we want to have a public conversation with this—

The Chair: Mr. Calkins, I'm sorry to interrupt, but I'm going to suspend.

We can discuss this while we are suspended briefly.

We do have an agreement from the committee to be in camera. It's very unconventional for us to be discussing changing that practice. We could, of course—

Mr. Blaine Calkins: We can talk about it, can't we?

The Chair: —have a motion put forward, should it be desirable, to change—

Mr. Blaine Calkins: I move that we stay in public.

The Chair: —our setting, but I'm going to suspend briefly so that we can talk as colleagues—

Mr. Eric Duncan (Stormont—Dundas—South Glengarry, CPC): We just moved something.

The Chair: I'm going to suspend briefly so that we can talk as colleagues, and then we're going to decide what colleagues want to do.

[*Proceedings continue in camera*]