HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

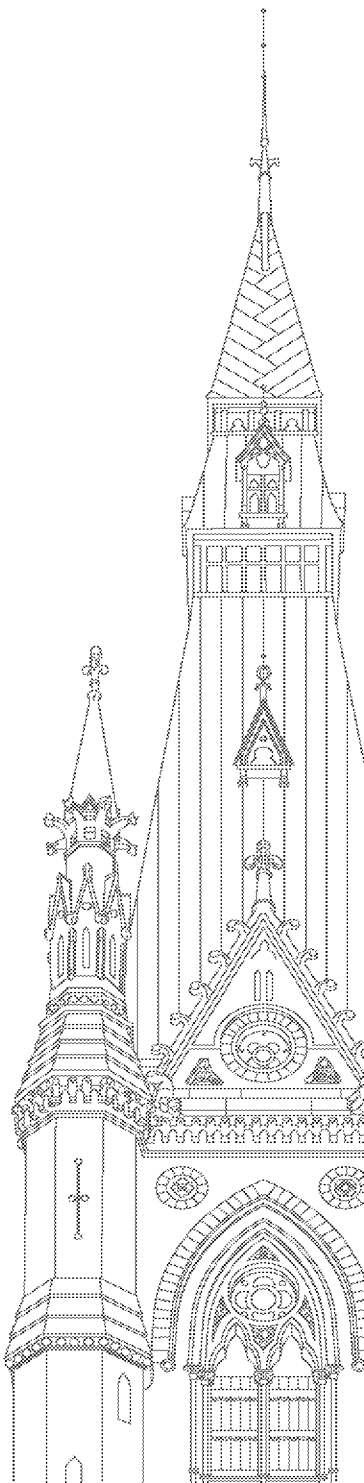
44th PARLIAMENT, 1st SESSION

Standing Committee on Procedure and House Affairs

EVIDENCE

NUMBER 083

Tuesday, June 13, 2023



Chair: The Honourable Bardish Chagger

Standing Committee on Procedure and House Affairs

Tuesday, June 13, 2023

● (1835)

[*English*]

The Chair (Hon. Bardish Chagger (Waterloo, Lib.)): Good evening, everyone. I call the meeting to order. Welcome to meeting number 83 of the Standing Committee on Procedure and House Affairs. The committee is meeting today to study the question of privilege related to the member for Wellington—Halton Hills and other members.

As I've mentioned in the past, and mostly for our guests today, keeping your earpiece in is the best way. If you choose not to keep your earpiece in, because you know both official languages, just leave it to the side. As always, please answer in the language of your preference. If there is time taken to listen to the interpretation, that time will not be taken away from you. It will be returned to the member. Just take your time to hear what is being asked of you and then respond.

What you have to offer is obviously really important to PROC committee members, because we've asked for you to be here. I want to thank you for responding so quickly to our request to appear. It means a lot to us. Your willingness to be here in the evening definitely demonstrates that you recognize the importance of the work we are doing.

Tonight we have with us, from the Canadian Security Intelligence Service, David Vigneault, director, and Cherie Henderson, assistant director.

Mr. Vigneault, I believe you're bringing opening comments. You have up to 10 minutes to share those comments.

The floor is yours. Welcome to PROC.

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

[*Translation*]

Thank you, Madam Chair.

Madam Chair, members of the Committee, good evening.

I am pleased to join you again today, with my Assistant Deputy Minister Cherie Henderson to continue our discussion on foreign interference.

Since my last appearance in March, media reporting on this topic has continued. The release of information in this way can create misunderstanding, confusion, and fear among victims of foreign interference. It also makes it more difficult for CSIS and our partners to do our jobs, which is exactly what our adversaries want.

Today, I would therefore like to provide the Committee some insight on the business of intelligence and to reassure you and Canadians of CSIS' commitment to countering foreign interference.

[*English*]

As you know, CSIS has long advised Canadians of the threat from foreign interference, and from the People's Republic of China in particular. We have reported on foreign interference in every annual operational and public report for the last 30 years, and published unclassified reports, including "Foreign Interference and You", in over seven languages. It has been the focus of extensive outreach and awareness efforts with communities, universities and the research sector. In short, foreign interference is not a new phenomenon to CSIS or to the Government of Canada.

As foreign interference threats have grown and evolved, so have our responses. We know that Canada's democratic institutions are targeted more now than they were 20 years ago. To effectively counter these threats, CSIS has leveraged the full suite of its authorities to investigate and reduce threats and advise government. It is also an active participant in the security and intelligence threats to elections task force, or SITE, working with federal partners to combat foreign interference targeting our elections.

Importantly, intelligence must be shared to have an impact. CSIS is mandated to advise the government on threats, and it does just that. CSIS has produced thousands of intelligence reports on foreign interference and briefed extensively on this threat.

CSIS has also prioritized equipping elected officials with the information they need to identify foreign interference, so they are better prepared to protect themselves. We do this by providing briefings that are tailored to the individual circumstances and provide detailed information on the tactics, tradecraft and methodologies used by foreign states against elected officials in Canada. We strive to provide them with as much detail as they need to mitigate the threats they face. Any threat to the personal safety of an individual is always immediately referred to law enforcement and the proper authorities.

CSIS began these efforts in earnest in 2015 and has significantly expanded them since 2021. In 2022 alone, CSIS conducted 49 briefings with federal elected officials and has briefed numerous provincial and territorial premiers, mayors and officials at all levels of government. The CSIS Act, however, prohibits the disclosure of classified information in these briefings. This is a legislative gap that must be addressed.

The National Security and Intelligence Committee of Parliamentarians has recognized CSIS's track record on foreign interference. Its 2019 annual report found that "CSIS has consistently conducted investigations and provided advice to government on foreign interference."

The committee has referenced our briefings on foreign interference to numerous ministers, federal partners and other public and private institutions. The committee also noted the considerable resources and wide range of tools that CSIS employs to investigate, report on and counter foreign interference threats.

[*Translation*]

CSIS does not hesitate to deploy the other tools at our disposal, including investigations, threat reduction measures and cooperation with our domestic and international partners to counter foreign interference. While what I can say about such operational matters is limited, I can assure you these efforts are robust.

CSIS is committed to continuing these efforts, in accordance with the Minister of Public Safety's recent direction that threats to the security of Canada directed at Parliament and parliamentarians continue to receive CSIS' highest attention.

[*English*]

Intelligence is a complex business. In our line of work, an organization's credibility is developed over years and is closely and delicately guarded by the rigorous practice of intelligence tradecraft. Protecting sensitive sources and methods ensures the safety of those sources and preserves our ability to continue to collect intelligence and protect Canadians.

CSIS collects intelligence from open sources, technical intercepts, human sources, partners, interviews and other investigative techniques. Intelligence professionals continuously assess the information and build an intelligence picture over time. The source of the information and its reliability, our ability to corroborate the information, and historical trends and context are just some of the considerations that are weighed in assessing intelligence.

The threshold for sharing intelligence and advice is not an exact science. Some intelligence that is shared is called "raw" intelligence, which may be uncorroborated by other information or may come from a new and untested source. Uncorroborated intelligence may prove to be highly credible in time, but requires rigorous validation.

All intelligence products include appropriate caveats and reliability assessments to inform the recipient. By pulling all the individual pieces together, we have a better understanding of the threat picture, including any intelligence gaps that remain.

Assessed intelligence products are shared to inform decision-making by the Government of Canada. We are highly responsive to the government's intelligence priorities and requirements, and we adjust our collection according to changing threats to ensure we meet the government's needs. My colleague, the national security and intelligence adviser, recently noted to this committee the importance of having decision-makers not only read intelligence but also receive advice on how to act on it.

The appropriate response may vary in any given scenario and must always consider the need to protect highly sensitive sources and investigations. It is also important to remember that intelligence is not evidence, although it can provide important information for law enforcement action.

It is essential that intelligence meets the needs of its clients and consumers. The national security and intelligence adviser also noted that there are improvements to be made to continually refine how intelligence remains a pillar of decision-making. My officials and I are committed to getting this right.

Foreign interference is a perennial problem that has grown in scale and complexity in our digital world. Canadians are not alone in facing this threat. The world is changing, with a return to states exercising hard-power interests and attacks against democratic values. A weakened rules-based system increasingly characterized by disruptive events is just as ripe for exploitation by state influencers as it is by extremists. As security practitioners, we are acutely aware of these connections. Emerging technologies such as artificial intelligence will only further exacerbate these challenges.

Protecting our values and prosperity in this new world is the priority of Canada and our allies. The stakes are high. This is a fight for democracy, which requires us to build societal resilience against foreign interference and bolster our democratic institutions. To do this, we need the appropriate tools and authorities to counter threats and protect Canadian values.

Informed and trusted discussion among communities, academia, businesses and governments at all levels is necessary to properly calibrate our responses and ensure our tool kits are fit for purpose. Addressing foreign interference and protecting Canada's national security requires input from all corners of Canadian society. Countering this systemic, national threat requires partnership with all Canadians.

● (1840)

[*Translation*]

CSIS is a committed partner in this effort and will continue to fulfill its mission to keep Canadians safe and secure.

With that, I will be pleased to answer your questions.

The Chair: Thank you, Mr. Vigneault.

[*English*]

I appreciate the pace at which you were speaking. I know in the past when you've joined us, you've spoken quickly. That has not helped with the two official languages. I would appreciate that we continue that pace.

As always, regardless of the language in which the question is posed, you have the ability to answer in the language of your choice. When it comes to interpretation, that time will not be taken away from the member. If we can just maintain that pace to ensure that anyone listening.... I'm sure that there are many people listening, because this is a very important topic, and it's important that we maintain the pace.

I would also appreciate it if all members remembered, when switching from one language to another, to slightly pause between one language and the other. It allows people watching virtually, online or later.... It would be appreciated.

Thank you for providing me those 45 seconds back from your 10 minutes.

Now we will enter into six-minute rounds, starting with Mr. Cooper and followed by Mrs. Sahota, Madame Gaudreau and Mrs. Blaney.

Mr. Cooper, go ahead through the chair.

● (1845)

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

Thank you, Mr. Vigneault, for appearing once again, and thank you, Ms. Henderson, for being here this evening.

Mr. Vigneault—through you, Madam Chair—on page 27 of the Johnston report, Mr. Johnston states that an issues management note was sent from CSIS to the then minister of public safety, Bill Blair, his deputy minister and his chief of staff in May 2021, warning that member of Parliament Michael Chong, another MP and their families in China were being targeted by the Beijing regime.

Is Mr. Johnston's report accurate in that regard?

Mr. David Vigneault: Madam Chair, the report is indeed accurate.

Mr. Michael Cooper: Mr. Johnston further states on page 27 that the IMU was not seen by the minister, his chief of staff or the deputy minister, because they did not have access at the time to what he called the "Top Secret Network e-mail".

Is Mr. Johnston correct in that regard?

Mr. David Vigneault: Madame Chair, that's the understanding I have from what Mr. Johnston said after having a discussion with Minister Blair. That is the understanding I have of the report.

Mr. Michael Cooper: Do you have any knowledge or information that Minister Blair had knowledge of that IMU at the time?

Mr. David Vigneault: Madam Chair, I did not have any specific discussions with Minister Blair about that note.

Mr. Michael Cooper: Minister Blair has a very different version of events.

He said, first of all, that there is no email account. That is precisely contrary to what Mr. Johnston states in his report. How can what Mr. Johnston concludes be reconciled with what Mr. Blair told this committee on June 1?

Mr. David Vigneault: Madam Chair, my understanding of how the information flows from an agency to a minister is that this is sent to the department. In this case, the Department of Public Safety was the department supporting the minister. That would be one of the most usual ways that information reaches a minister on a topic like this.

It would be unusual for the minister to receive classified information directly through electronic means.

Mr. Michael Cooper: It was sent by electronic means. Is that right?

Mr. David Vigneault: Yes. The way that we, CSIS, would be communicating this information to the department for onward transmission to the minister is by secure electronic means.

Mr. Michael Cooper: That's presumably why, for example, his deputy minister would have been sent the IMU, in addition to the minister and his chief of staff.

Again, Minister Blair says there's no email account. He further stated that whatever is brought to his attention is determined by you, the director of CSIS. That's exactly what he said. Is that accurate?

Mr. David Vigneault: Madam Chair, I think it is true that a lot of the information that is exchanged between CSIS and the minister comes directly from me or from one of my senior officials in different organized briefings.

However, I think it's important to note here that we also have a lot of exchanges of documentation. The exchanges of documentation come, as I mentioned earlier, mostly through electronic means to the department, so that it is able to be printed and made available to the minister.

These would be the two most common ways that we exchange information.

Mr. Michael Cooper: Minister Blair went further. He said that you, as the director of CSIS, would decide what to brief him on, and that he would wait for you to advise him.

Secondly, he said, "The director determined that this was not information the minister needed to know, so I was never notified of the existence of that intelligence, nor was it ever shared with me." That's what he said on June 1.

Did you determine that this was information—that information being the IMU—the minister did not need to know?

● (1850)

Mr. David Vigneault: Madam Chair, in this specific case, there are two ways that the information will be shared. One is when we have intelligence reports. Those intelligence reports are written and shared with the department to be curated for the minister. It will depend on the department's decision from time to time to see what the minister will have access to.

It's also important that when we see we have something of high importance...we have instituted this process called an "information management note". That would be shared to bring attention to something more specifically. That was the purpose of this note. It was to bring it to the attention of the people to whom it was destined to go.

I would like to add, Madam Chair, that it's clear that Minister Blair in his testimony mentioned that he did not see that note, and I have no reason to doubt that.

Mr. Michael Cooper: However, he said you determined that the information was something he didn't need to know. From what I understand from the answer you just provided, that's not the case, and you didn't make that decision.

Mr. David Vigneault: Madam Chair, that could be an accurate description. I think the fact that we did an issue management note speaks to the notion that we wanted to highlight the information.

The Chair: Thank you.

I hope that hearing the beep, and the fact that we had another question following that beep, has demonstrated my intentions, as chair, to show that if one person speaks after the other, I will also be courteous in providing it.

I will return the courtesy if it is given to the chair. If the courtesy is not offered to the chair, it will not be returned, so the onus is on members to have the courtesy returned. I hope that is understood by my comment at the top of this meeting.

Go ahead, Madame Sahota.

Ms. Ruby Sahota (Brampton North, Lib.): Thank you, Madam Chair.

My first question for Mr. Vigneault is with regard to the new ministerial directive that was given in May by Minister Mendicino. The directive given to CSIS means that you'll now have to investigate and, in addition to that, disclose—I guess you're generally investigating—any foreign threats against parliamentarians and/or their families.

There has been some talk by other witnesses, as well, about what this would mean. We have many questions as to whether you have started to undertake that work.

Have you started to contact parliamentarians? When would this new expanded process begin? If it has already begun, what does that process look like?

The follow-up question to that is what concerns or comments you might have regarding that, because there have been some concerns brought up that perhaps briefing us on every matter may also lead to some confusion at times.

Mr. David Vigneault: As I mentioned in my opening remarks, CSIS has been investigating foreign interference since its inception in 1984. It's part of the act. That includes foreign interference directed at elected officials. We have reported on this publicly, as I've mentioned, for over 30 years.

The ministerial directive I think is a helpful tool to help clarify the intent of the minister in how we are exercising these authorities. I can tell you that it has already been put in motion. We are developing plans and approaches to talk to other elected officials.

With that ministerial directive, it is also important to take into consideration...the limitations that I have mentioned. The CSIS Act is clearly limiting the ability of CSIS to share classified information. Between an act that is showing its age in terms of the ability to exercise our authorities and share information and the new ministerial directive, I think it's providing better clarity. We hope it will be helping CSIS's ability to share that information that is crucial for members of Parliament to have.

● (1855)

Ms. Ruby Sahota: Mr. Vigneault, are you suggesting that relevant updates need to be made to the CSIS Act as well, so that it goes hand in hand with the new directive?

Mr. David Vigneault: It has been recognized by a number of experts outside the government, and it has been recognized by Minister Mendicino and Minister LeBlanc as recently as a couple of weeks ago in their comments, that there is a need to review the CSIS Act. The National Security and Intelligence Committee of Parliamentarians, NSICOP, has noted the fact that the CSIS Act needs to be updated. Commissioner Rouleau in the commission of inquiry that took place last year noted that even though it was not in his terms of reference, he thought it was important to have clear reflection on the CSIS Act to make sure it's relevant for today. The Federal Court has also mentioned that the CSIS Act may be showing its age.

So I believe that, yes, indeed, having a modernized CSIS Act would be an opportunity for CSIS to respond much more fully to the wishes of parliamentarians.

Ms. Ruby Sahota: Thank you.

You said that processes have been undertaken. Have you briefed any parliamentarians under this new process?

Mr. David Vigneault: We have started. We've had one such instance of a briefing. We have a couple of others that are being prepared as we speak. There will likely be more in the future.

Ms. Ruby Sahota: You mentioned that in 2022, 49 briefings were provided. Were any briefings provided in 2021? If so, how many?

Mr. David Vigneault: Madam Chair, with your indulgence, I will take this question under advisement and bring back to the committee the specific number. I believe it is listed in our annual report, but I will provide the committee with the specific answer.

Perhaps I can add that I think what's important here is that since about 2018, we started speaking publicly and very clearly to Canadians about foreign interference by providing some of our analysis and some of our advice on how people and organizations could protect themselves. I think we are now at this evolution, given the nature of the threat environment, where we need to have further and more specific discussions with members of Parliament. We very much welcome the opportunity to do so.

Ms. Ruby Sahota: There has been some criticism regarding the approach that CSIS has taken to educating the public or providing these briefings and a better understanding to the consumer of intelligence. In addition to that, we know that we have public hearings coming up. I'm hopeful that CSIS will be involved in those public hearings and learn from diaspora groups.

We are learning from CSIS, and the national security adviser as well, that there are other countries that previously were not mentioned as state actors that are a threat to Canada when it comes to foreign interference. What are your comments on that? Why have new countries been added to the list?

Mr. David Vigneault: With regard to the first part of your question, Ms. Sahota, I think that working with diaspora communities is not only important but also the only way that we, Canada, will be able to have increased resilience against foreign interference. This is why, about three or four years ago, CSIS reallocated internal resources to create a stakeholder engagement group, which has been dedicated to engaging with these partners.

Thank you, Madam Chair.

The Chair: Thank you.

Madame Gaudreau.

[*Translation*]

Ms. Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): Thank you very much, Madam Chair.

I have a lot of questions, but I've consolidated them.

First of all, we've heard from a phenomenal number of witnesses on the interference issue. Since we began in November, that's four months, and they've been very intense. What I gather is that the warning threshold is too high and that CSIS prepares a massive quantity of briefing notes, thousands, that are intended for MPs.

We've been told that there's no intelligence culture within the Canadian government's national security apparatus, that funding for personnel and resources isn't necessarily there and that our intelligence services haven't adapted to the geopolitical situation since 2015. We've heard several examples of that.

What happened from 2001 to 2015? We know what has happened since 2015, but we're often told that the situation has existed for some 20 years.

● (1900)

Mr. David Vigneault: Thank you for your question.

You raise several points. I'll address them in order.

As regards intelligence culture, Canada is a fortunate country because it belongs to a number of collective defence organizations, such as the North Atlantic Treaty Organization, or NATO, because it has a unique partnership with the Americans and it's protected by three oceans. Unlike many other countries, we haven't had to concern ourselves greatly with defence or national security issues. That's an element of the culture. It isn't a bad thing not to have to combat as many threats as other communities, but it's a reality.

What happened in 2001 were the terrorist attacks conducted by Al Qaeda. We were forced to completely rethink how we viewed national security. Terrorist groups monopolized the attention of the United States. Enormous investments were made, not only in personnel and financial resources, but also in partnerships with foreign countries and communities within Canada. The emphasis was placed on the protection of Canadians against terrorist attacks.

Since 2015, if you read CSIS's annual reports, you'll see not only the quite significant way in which the emphasis that's put on terrorism and on a detailed way of viewing it has evolved. We discuss not only religious terrorism, such as that associated with Al Qaeda, but also ideological terrorism, which is associated with neo-Nazi groups, xenophobic groups and groups that direct their violence against women, for example.

We at the service have redistributed resources in such a way as to take these dynamics into account. That's also true with regard to the foreign interference issue. We have redistributed resources so we can face that threat. I believe that's an evolution that certain partners and commentators have noticed. I think it's reflected in the government's directives on intelligence requests, that is to say, on what intelligence it wants us to prepare, and in the resources that are allocated to CSIS.

The scales continue to tilt toward state threats, and new state threats have unfortunately been weighing on Canada since China emerged as both a major economic state and a geostrategically destabilizing one, and since the unjustified invasion of Ukraine by Russia. In a speech that I gave in 2018, my first speech as director, I mentioned that the threat that hostile states represent, which includes foreign interference, was the most significant threat to Canada's security and sovereignty.

Ms. Marie-Hélène Gaudreau: Thank you for your explanations. They help me put all this into perspective.

Who would you say determines CSIS's general policies and directions? Does CSIS advise the government on resource allocation? Or does the government asks you to examine certain issues? I'd like to get a clear understanding of the process.

● (1905)

Mr. David Vigneault: That's quite a serious question. I think it could be a topic for further study.

Intelligence priorities are very clearly established by cabinet. Cabinet makes a decision and sends its intelligence directives to us. In the case of CSIS, the Minister of Public Safety receives those directives and, considering CSIS's mandate, sends us ministerial directives. CSIS's mandate is clear, and the data collection mandates of other intelligence agencies are as well. Each minister therefore gives us ministerial directives. Apart from that, we discuss resource allocation. That discussion is carried on internally and not among departments.

Ms. Marie-Hélène Gaudreau: Thank you very much.

The Chair: Thank you.

Go ahead, Ms. Blaney.

[*English*]

Ms. Rachel Blaney (North Island—Powell River, NDP): Chair, before I start, I just want to let you know that I got bumped off. We have a bit of a wind storm here. If you could watch the interpreters to make sure that my sound is good, I would really appreciate that.

The Chair: I'm going to take that, before I go into your time, and make sure we do a sound check to make sure we're all okay.

I have a thumbs-up. Thank you for that courtesy.

The floor is yours.

Ms. Rachel Blaney: Thank you so much. The interpreters work hard for us, so I want to make sure we do right by them.

I want to thank the witnesses so much for being here today. I have a question.

Mr. Morrison was here earlier today and spoke about Mr. Chong's receiving a defensive briefing. When Mr. Chong came to our committee, he was very clear that it was very, very helpful. The problem, of course, was that he didn't know, while he was receiving that briefing, that he was a target and that his family, both in the country and outside of the country, were potentially a target. There are some really big concerns there.

Why was the choice made to give him this information but to not inform him of the concerns that it was indirectly addressing? The second part of that question is: How many members of Parliament got a defensive briefing?

Mr. David Vigneault: Thank you, Madam Chair.

I can say from the outset, going back to my opening remarks, that I believe that members of Parliament should be receiving more information. I think the world that we're in now requires that we adapt our approaches, and that includes CSIS.

I think the ministerial directive is going to be helpful there, but that will still have to be done within the context of the limits of the CSIS Act. I hope that this committee will have some perspective here.

The approach that was taken to brief Mr. Chong is the one that was available to the service at that point, which is having defensive briefings. I think it's important to note two specific elements of that. The first one is that a defensive briefing is carried out by a professional intelligence officer of CSIS who has access to all of that information. It is not just a generic briefing that is given. It's given by a trained, professional intelligence officer with knowledge of the classified information. It is tailored to the individual and is very much in that context.

That said, I think it's also important to know the limits that we have to brief classified information. I think that has been clearly highlighted in the case of Mr. Chong, and I believe that this is the kind of evolution that we will see, not just from a CSIS authorities point of view, but in terms of the culture we have related to national security, which is that we need to engage more. You have my commitment, Madam Chair, that CSIS is fully engaged in that.

Ms. Rachel Blaney: I still didn't get an answer as to how many MPs. I'm going to ask that again, but I also want to point out that I think what you said is interesting, that it was really targeted. Although Mr. Chong didn't know the whole story, the information was targeted.

How many MPs have been briefed? I don't need to know names; I just want a general, ballpark figure.

The other thing is that Mr. Chong said very clearly in this committee that it was extremely helpful. The briefing helped him have awareness, and he started to see things differently in terms of activities that were happening.

I'm just wondering if there is a plan to have defensive briefings for more MPs or, in fact, all MPs. Is there a general way that MPs can learn how to notice what's happening, so that we can also be part of the solution by letting the appropriate officials know?

● (1910)

Mr. David Vigneault: I would not be in a position to share the specific number of MPs. However, I think what is clear is that the commitment from CSIS and the specificity of the ministerial directive are to make sure that all MPs will be briefed, and that's a direction that we have and will carry out.

The member is raising a very important point as well. Those defensive briefings to all members of Parliament and I would say all parliamentarians, including in the Senate, are absolutely essential. The plans have been developed, and they have such plans that are almost ready to be put in place. CSIS will be an active participant in briefing all members of Parliament.

If I could add as well, Madam Chair, over and above the elected officials of the federal Parliament, as I mentioned, we have been engaging directly with elected officials at all levels of government, provincial, territorial and municipal, and I believe that we need to continue to do that, because what we have learned over the years is that the opportunity to engage in foreign interference is not limited to the federal level. There are very specific actions that are being taken at all levels of government, and I should have included municipalities on that list.

I believe the member is right to say that we need to increase the number of briefings by CSIS and by other organizations to help build resilience in Canada.

Ms. Rachel Blaney: Thank you for that. I have just a few seconds left. One of the things that have come up again is that misinformation attempts are particularly problematic in rural, indigenous and ethnic communities. The vulnerability is higher there because of the lack of information, and maybe a lack of reliable media sources. I'm just wondering if there is any work being done on addressing that huge gap.

Mr. David Vigneault: It is a very relevant point, because we have seen over the years the ability of media in languages other than French and English to be used and abused by different countries to accomplish their goals. This is why our foreign interference material that we produced last year has been published in seven languages—to be able to have information in the language of a number of diaspora communities that are directly targeted.

We are also working with first nations organizations to accomplish similar goals.

Thank you, Madam Chair.

The Chair: Thank you, Mr. Vigneault.

We will go, for five minutes, to Mr. Berthold, followed by Mr. Turnbull.

Mr. Berthold.

[*Translation*]

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

Good evening, Mr. Vigneault and Ms. Henderson.

Mr. Vigneault, I absolutely have to clarify some things that have previously been said. On June 1 of this year, Minister Bill Blair made a statement that I'm going to read to ensure that we understand each other:

> Allow me to clarify that the information was not shared with me. It was authorized by CSIS to be shown to me, but they determined.... I would leave that question as one that perhaps you might want to put to the director. The director determined that this was not information the minister needed to know, so I was never notified of the existence of that intelligence, nor was it ever shared with me.

Did you make that decision?

Mr. David Vigneault: As I mentioned a little earlier, CSIS and I conveyed the information to the Department of Public Safety along with the very specific directive to forward it to the minister. I don't doubt that the minister didn't receive it. His comment was very clear. However, it's important for the committee to understand that we shared the intelligence and the briefing note.

Mr. Luc Berthold: If I understand you correctly, you never advised anyone that this note should not be shared with the minister.

Mr. David Vigneault: That's correct.

Mr. Luc Berthold: Mr. Johnston's report reads as follows at page 27:

> The Minister indicated that when CSIS wanted to transmit sensitive information, they would request a briefing, take him to a secure facility and show it to him.

Is that how you proceed? It's not what I understood from your testimony earlier.

● (1915)

Mr. David Vigneault: I can clarify my response.

There are generally two ways to brief the minister: either orally via secured videoconference or in the same room, or by transmitting documents to the attention of the minister, which is very often done.

Mr. Luc Berthold: Are they sent via email?

Mr. David Vigneault: I generally don't send classified emails. I send classified documents, and we have discussions, but that's generally not a means of transmission that I would use.

Mr. Luc Berthold: This passage states:

> ...they would request a briefing, take him to a secure facility and show it to him.

Did that happen?

Mr. David Vigneault: As I mentioned, one of the common ways to transmit information to the minister is to have a meeting with him in the same room or via secure videoconference.

Mr. Luc Berthold: However, you aren't talking about a secure facility.

Mr. David Vigneault: I believe the minister meant that he was going to our offices at CSIS or to the secure offices of the Department of Public Safety.

Mr. Luc Berthold: However, it was at your request that those meetings were held in those places.

Isn't that correct?

Mr. David Vigneault: That can be done at the request of CSIS, the minister or the Department of Public Safety, depending on the subject matter that has to be addressed.

Mr. Luc Berthold: Mr. Johnston says this in that same report:

> [The minister] believes the Ministerial Direction in place at the time means that CSIS should have briefed him about this,...

This refers to that briefing note that we've been discussing since earlier on.

Is that the case?

Mr. David Vigneault: If there's any one thing that's very clear, it's that we're all learning about the events that took place. I think there could have been more information or more regularity in discussions between CSIS and the minister.

The pandemic was very hard on many people. CSIS was one of the only federal government organizations that worked almost solely from its offices. That did nothing to facilitate the exchanges.

Mr. Luc Berthold: I have another important question, Mr. Vigneault.

As regards this issues management note, do you send a lot of these types of notes to the minister every year?

Mr. David Vigneault: We may send none in any single week, but there are generally two or three a week.

Mr. Luc Berthold: The previous national security adviser told us that he had received 7,000 notes to read, and he scolded me for not having read them. He told me that sometime I should sit down on his chair and see how hard it was for him to manage all that information.

However, not that many notes are issues management notes like the one you sent the department concerning Michael Chong. There aren't 7,000 of those every year.

Is that correct?

Mr. David Vigneault: That's correct.

There aren't as many issues management notes. On the other hand, that's only one of the ways of transmitting information. There are other ways to communicate critical information to the minister. That isn't the only tool that's used.

Mr. Luc Berthold: Do you think that note is particularly important? Is it the kind of note that should usually draw the attention of the person who receives it?

Mr. David Vigneault: The service created that type of note only a few years ago precisely to draw people's attention to issues deemed to be of interest.

The Chair: Thank you.

That was a very good conversation. I was asked for a little more time, and I allowed it because the requester showed respect for everyone here, including the interpreters. When people respect me, I do the same in return. I believe we are all finding that this information is important. So we will continue along the same lines.

Mr. Turnbull, you have the floor for five minutes.

● (1920)

[*English*]

Mr. Ryan Turnbull (Whitby, Lib.): This is with respect to you, Madam Chair, and to our witnesses today.

Mr. Vigneault, I would ask you if you have read the Right Honourable David Johnston's first report.

Mr. David Vigneault: I have.

Mr. Ryan Turnbull: Do you agree with his findings, specifically the eight allegations that he's looked into that supposedly originated from CSIS leaks? Would you agree with those findings?

Mr. David Vigneault: Madam Chair, I know that the member has limited time, but I would rather that we be a bit more specific, as opposed to just speaking in general about the report.

I will make a specific comment. Generally speaking, yes, I agree with those findings.

Mr. Ryan Turnbull: The annex to Johnston's report refers to all of the intelligence in context that he gathered and all of the interviews that he's detailed in his report that have informed his interpretation of those facts. Would you say that they are fairly accurate from your perspective?

Mr. David Vigneault: That would be accurate.

Mr. Ryan Turnbull: Thank you.

That seems to coincide with multiple ministers and deputy ministers who were on the critical election incident public protocol, the national security and intelligence adviser and you. There seems to be a corroboration of at least four, five or maybe more sources that agree with the interpretation of the facts in these particular matters. I think that's important.

Mr. Vigneault, do you think partisanship has had a negative impact on the national security and intelligence community within the last few months as a result of these parliamentary proceedings?

Mr. David Vigneault: It's a very important question. I'll limit my comments to my position as director of CSIS.

I would say the politicization of national security is not just recent; it has taken place for a number of years now. It is not conducive to having the most significant and beneficial discussions to be able to put the country in the best possible position to defend itself against increased threats.

Mr. Ryan Turnbull: Therefore, when leaders are offered opportunities to review the facts in these matters, i.e. the annex to Johnston's report, would you say that it would be a good way to take out the partisanship, getting fundamentally related to the facts?

Mr. David Vigneault: Madam Chair, I would argue that any opportunity to better understand the threat picture that Canada is facing is an important opportunity.

Mr. Ryan Turnbull: If you had to compare the foreign interference attempts of Russia and China, who attempts to interfere more? How do their tactics differ?

Mr. David Vigneault: As I've said before, and I want to be respectful of committee, I am limited in what I can say in a public setting. However, I think there is a fundamental difference between the PRC Communist Party activities and Russia. The most fundamental one is the fact that, since the arrival of Xi Jinping as the president of China and the leader of the Communist Party, we have seen a growth in the ability and the budgets of the United Front Work Department.

The UFWD is a tool that was created at the inception of the Communist Party in the 1940s and has existed in Canada for a long, long time. Xi Jinping has described it as one of his magic weapons. The UFWD's main goal is to interfere in other countries' affairs. I would say that this is one of the most significant differences between the PRC and other countries.

Mr. Ryan Turnbull: You would agree that Russia still presents a threat.

Mr. David Vigneault: Russia has extremely advanced capabilities to engage in foreign interference activities. They are doing the same thing on espionage. The question may be: What is the intent behind those capabilities, and what are their specific objectives? Sometimes, Canada may not be the main objective.

● (1925)

Mr. Ryan Turnbull: Thank you.

Would you agree that, whatever form the public review process takes, whether it's a public inquiry or some other form of public process, public hearing, etc., we should do a comprehensive review of foreign interference, including China, Russia and other state actors?

Mr. David Vigneault: Madam Chair, I think, as an intelligence organization, of course, we look at foreign interference irrespective of the source of that interference. We look at the threats to Canadians. Of course we're going to be focused on that.

I can assure the committee, through you, Madam Chair, that CSIS will support any process that Parliament and the government decide to put forward. I think it's a critical issue for the government and for Canadians.

The Chair: Thank you.

Go ahead, Madame Gaudreau.

[*Translation*]

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

As an intelligence officer of a member state of the Group of Five, you are aware of what's happening in interference matters elsewhere in the world. We've seen that interference has been intense, organized and planned, particularly in the United Kingdom, France, Australia and the United States. You just discussed that.

Consider France as an example. Mr. Macron, a candidate in the 2017 presidential election, had his campaign hacked. You'll see what I'm getting at. It was orchestrated by Russia. The Direction générale de la sécurité intérieure, the DGSI, which is France's counterintelligence service, opened an investigation, and the French public was extensively informed about the situation.

Why, in Canada, did information have to be leaked for CSIS to urge the government to do the intensive work it's now doing?

Mr. David Vigneault: The member has brought up a good point.

That specific case of foreign interference in France occurred a year or two after the foreign interference in the American elections was revealed. It drew very keen attention, which encouraged Canada to establish the Security and Intelligence Threats to Elections Task Force, or SITE, to coordinate all intelligence. I think the necessary lessons have been learned.

I would draw your attention to the fact that CSIS provides many details on foreign interference in its annual reports and communications. I don't think that likely had the same media impact as the leaks, but a lot of unclassified and very specific intelligence has nevertheless been published.

If I may, I would also say that Canadian parliamentarians, media and universities weren't necessarily paying the same kind of attention to this issue as in other countries, although I believe their attention is now sharply focused and intense. I really hope that the committee's proceedings and the information that CSIS provides it will be useful in ensuring that Canada is better prepared in future.

Ms. Marie-Hélène Gaudreau: I hope we all stop burying our heads in the sand.

The Chair: Thank you.

Go ahead, Ms. Blaney,

[*English*]

Ms. Rachel Blaney: Thank you, Chair.

I'm going to come back to my last question, because I didn't hear anything about rural communities. I also thought I heard somebody say, "May I add...?"

If there's something that I missed, I would enjoy hearing it.

Ms. Cherie Henderson (Assistant Director, Requirements, Canadian Security Intelligence Service): Absolutely. Thank you very much.

I think it was a very important point that we were discussing, which was raised by the member, Madam Chair. What I wanted to pick up on was the point made in regard to that ongoing communication. When we go out and provide those defensive briefings, the intent is to allow the individual to become aware and to create that awareness of what they might be seeing that they would not normally recognize, potentially, as foreign interference. It's to increase that awareness.

It was also so that if they became aware, they could talk to us as well and get that back-and-forth. By being able to provide that information back to us, we can continue to make those briefings that much more valuable for all Canadians, all of our members of Parliament and all of the levels of government.

I think it's fundamentally important that this is not something we can do alone, and that everybody needs to support, engage and understand what the threat is. That's where those ongoing defensive briefings we were providing and will continue to provide can help create that greater engagement across the board.

● (1930)

Ms. Rachel Blaney: Thank you so much.

I want to come back to the diaspora communities that have been calling out and ringing the alarm bell for a great many years. We have heard from witnesses at this committee that many from those communities feel ignored and unsafe when they've gone to the RCMP. They have case files, but they just don't hear back.

I heard you talk about a stakeholder engagement group. Are there terms of reference? What is the strategy of that group? Could we see the terms of reference, if that's possible?

Mr. David Vigneault: I'll make an undertaking to bring back some more specific information about this group. It's a very important tool.

This is an area that I think is very important. CSIS is an intelligence organization that operates in a democracy governed by the rule of law. In other countries.... We're not independent and trying to behave in different ways. Our engagement with those communities is critical, and I welcome the work of this committee to do more of that in the future.

Thank you.

The Chair: Thank you.

Mr. Cooper.

Mr. Michael Cooper: Thank you, Madam Chair.

Mr. Vigneault, following up on my line of questioning and that presented by Mr. Berthold, I want to make sure that I fully understand what you have said with respect to the IMUs.

As I understand it, there are intelligence reports that are produced in the thousands each year, and then there are IMUs, of which, on average, two to three are produced a week. IMUs are produced because—and I am quoting you—you see "something of high importance".

Is that correct? Do I understand you correctly?

Mr. David Vigneault: That would be accurate.

Mr. Michael Cooper: Okay. Thank you for that.

When you see something of high importance by way of an IMU product that is addressed to a minister, that is because you would want the minister to see that IMU. Is that correct?

Mr. David Vigneault: The IMU is sometimes directed at the minister, but also sometimes it will be directed to other officials in the government as well.

Mr. Michael Cooper: When it is addressed to the minister, it would be because you want the minister to see it. Is that right?

Mr. David Vigneault: Yes, that would be accurate.

Mr. Michael Cooper: Okay.

I just want to go back to Minister Blair's testimony. I think it's just important to put it on record.

On June 1, he said, in specific response to the issue of the IMU concerning MP Chong, "The director determined that this was not information the minister needed to know".

He further went on to say, "In this case, they"—meaning you—"made an operational decision that...was not required."

He then added that he was not provided this because of your supposed operational decision, which he characterized as one that was "quite appropriately" made.

How do you explain the minister's testimony? It's not just a case of his not seeing it; he's talking about an operational decision that was made by you that he even went on to say was quite appropriately made, which was to not inform him.

Mr. David Vigneault: I think what is clear is that the process did not work.

I and other witnesses in front of your committee have spoken about the fact that with the way the intelligence is being ingested by different parties at the ministerial level, and also at all levels of officials, the system may often not be adequate. There is a need to make a significant improvement. I would venture to say that this is one such example, where the information was meant to be seen by the minister and was not.

I think it's a problem that we need to fix. It's a problem that is important because the people of CSIS and other intelligence organizations take risks to collect the intelligence. We need to make sure that it is available to the right people.

● (1935)

Mr. Michael Cooper: I certainly agree with you, Mr. Vigneault, that this is something the minister should have seen.

I have a lot of questions for the minister as to why he would make such statements that fly in the face of what you have said, by making very specific claims about certain operational decisions that he claims were quite appropriately made to keep him in the dark on a matter that you said is prepared in the way of a report when you see something of high importance. I could see why it was of high importance, given what we were dealing with, which was MP Chong and another MP and their families being targets of the Beijing regime.

We know that after the IMU was prepared, there was a CSIS memo of July 2021 that revealed that MP Chong and, I believe, other MPs were being targeted by Beijing. Jody Thomas, the Prime Minister's national security and intelligence adviser, when she appeared on June 1, said that memo from CSIS was sent to the PCO as well as to the deputy ministers of foreign affairs, public safety and national defence.

Was that memo sent to anyone else, to your knowledge?

Mr. David Vigneault: For sure it was those individuals. I don't remember if there were other individuals, but those would have been the most senior people who would have been the recipients of this.

Mr. Michael Cooper: Very briefly, was that memo an IMU document or product?

Mr. David Vigneault: If I recall correctly, this memo was what we call an intelligence assessment, so not raw information or raw intelligence, but an analysis of the intelligence available on a specific topic.

The Chair: Thank you.

Once again I have demonstrated that when we take turns I will provide leniency to make sure that we get through our round of questions.

With that, we'll go to Madam Romanado.

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

Through you, I'd like to thank the witnesses for being here.

Monsieur Vigneault, I will ask a couple of questions. Could you just answer yes or no to confirm, because I have multiple questions and limited time?

Can you confirm whether the IMU referenced for May 2021 identified MP Chong in any way?

Mr. David Vigneault: Unfortunately I'm not at liberty to speak about the classified nature of our information. I apologize to the member, but I'm not at liberty to speak in detail about specific information of a classified nature.

Mrs. Sherry Romanado: Can you confirm if the July 2021 intelligence assessment identified, in any way, MP Chong? I'm trying to get to the point of the question of privilege. Can you let me know if that intelligence assessment identified Mr. Chong?

Mr. David Vigneault: Unfortunately I cannot provide a specific answer. What I can say that's hopefully helpful to the member is that for the people who are receiving.... Sometimes we produce information, and even when it's very sensitive, names are included. Sometimes names are not included but are available to people who have the right need to know, so that process exists and is used frequently.

Mrs. Sherry Romanado: Monsieur Vigneault, "On June 28 2017, the National People's Congress passed the National Intelligence Law and outlined the first official authorisation of intelligence in the People's Republic of China".

I'm quoting directly from a Government of Canada website, where it says:

> The intelligence law highlights one important continuing trend within the state security legal structure put in place since 2014: everyone is responsible for state security. As long as national intelligence institutions are operating within their proper authorities, they may, according to Article 14, "request relevant organs, organisations, and citizens provide necessary support, assistance, and cooperation".

Can you elaborate with this committee if this changed the posture with respect to intelligence-gathering within CSIS?

Mr. David Vigneault: Indeed this was another significant milestone. It essentially codified and publicized the fact that the PRC, the Communist Party, saw everybody—every company, every citizen—as someone who needed to support intelligence services. The way the PRC is looking at its citizens, irrespective of the fact that they may have dual citizenship and irrespective of the fact they may have been living in another country for years—a couple of generations—they would apply the same standard to apply that law and they would be putting pressure on individuals to collaborate with the intelligence service if that was their desire.

Yes, CSIS took good note of that, and it changed the way we were looking at our analysis and our investigations.

● (1940)

Mrs. Sherry Romanado: According to testimony from Mr. Chong, he was made aware of direct threats to him in early May 2023, based on reports and a subsequent briefing. Again, not elaborating on the specifics, can you confirm that he was made aware of potential threats to him in early May 2023?

Mr. David Vigneault: I believe that the member is referring to the threat reduction briefing that I had with Mr. Chong. Yes, I believe the date is accurate—I can confirm—but that would be the first time that we would have shared that classified information with Mr. Chong.

Mrs. Sherry Romanado: In that regard, earlier in your testimony today, you said "intelligence must be shared to have an impact".

If that is, in fact, correct—if Mr. Chong was not made aware of any threats to him or his family until May 2023—would you agree, then, with respect to the question of privilege? If he was not made aware, how would he have been intimidated?

Mr. David Vigneault: I think, as I mentioned earlier, that it's an important point. CSIS had a few interactions with Mr. Chong, including at the point we had the intelligence, and the person engaging with Mr. Chong had the experience and knowledge to make sure that this intelligence was specifically tailored for Mr. Chong. It does not negate the fact that the specific and classified intelligence was not shared with Mr. Chong, but that defensive briefing was absolutely informed by that.

As has been mentioned, and I've said earlier, I think we're pointing here to a gap that exists that we need to find a way to resolve because of the ongoing threat of foreign interference in our democratic processes.

Mrs. Sherry Romanado: Thank you.

Hopefully, I'll have another chance.

The Chair: Thank you.

Mr. Calkins, you have the floor.

Mr. Blaine Calkins (Red Deer—Lacombe, CPC): Thank you, Madam Chair, and thank you, Mr. Vigneault, for being here again.

Madam Henderson, thank you.

I have just a few questions to help me understand an intelligence assessment report, which I think, if I understand correctly, comes from the secretariat. If I understood Mr. Rigby's testimony correctly, this information was collated and sent to the national security adviser, Public Safety, Foreign Affairs and National Defence.

What's the difference between that assessment and an IMU, the issues management note? What's the difference between those two?

Mr. David Vigneault: It's an important point, given the fact there have been a lot of references to different intelligence processes or documents.

Intelligence starts from collecting information. You have initial information. That will be what we call a raw intelligence product.

Mr. Blaine Calkins: You have data.

Mr. David Vigneault: We have data. We have information. It could come from different partners.

That information is used by intelligence analysts to create intelligence. You have one report that would speak to something specific we know.

A compilation of these reports, those building blocks, plus any other information, like open-source information, information from our allies or information from other intelligence services is then used by our specialists, our experts, and they will produce what we call an intelligence assessment, to try to paint a picture of a situation.

I think that was the July document that was referred to earlier.

The IMU, issues management note, is a tool. Given the fact that there's so much information and there are so many moving parts in our system, we have put in place this tool to draw the attention of different people, sometimes ministers but often the rest of the bureaucracy, to something we want to draw attention to. It may not contain any intelligence; it may just be something that is happening that we want to be mindful of.

● (1945)

Mr. Blaine Calkins: That's very, very clear.

You talked about this issues management note. It's been the topic of discussion, at least in the questions we've had. The former minister of public safety was here, we understand that, and has made some claims that seem to be contradictory, not only to what David Johnston said in his report but also to what we've heard. I'm trying to flesh this out, because what's at stake here is the safety and security of a member of Parliament.

When was this IMU, or when were these issues management notes...? When was this process established, roughly? Could you tell this committee? This is not something new, is it?

Ms. Cherie Henderson: We established issues management notes probably back in 2015, about that period of time. The intention was, because we have a very robust process for sharing intelligence and, as Mr. Vigneault has indicated, we have what we call a raw intelligence product and we have an intelligence assessment product, but those go to a very different audiences. Those go to all of the individuals within the S and I community. The IMU note was then created, because we wanted to make sure that we could inform on a specific event at a specific time.

Mr. Blaine Calkins: That's understood very clearly now.

These notes are well established. This is not something new. They've been around since 2015. Nobody can reasonably claim that this is a new process or that they failed to understand how this process works.

Is there a higher way to signal importance? From my perspective, I'm seeing this as a red flag on an email. When we send emails to each other, we mark priority or importance on emails. This, to me, seems like a red flag on an email, from a layman's perspective, but I can also send a read receipt, so that if somebody opens the document, it tells me they've actually read it.

Are you aware of that? Do you have any signal to indicate whether or not the information that was sent in the IMU in question was opened and read? Basic email service offers this. Does our intelligence sharing have a similar type of guarantee or certainty that the information, which is important enough to be flagged, is actually read?

Mr. David Vigneault: This is a very important point. What I think is clear is that if we have put in place a process to flag.... Here, in this specific case, the minister was very clear: He did not get the information. It means the process that was put in place—the support he was receiving from us or from Public Safety—did not, in this case, work.

Yes, there were the conditions of the pandemic, which should not be overlooked, but more fundamentally than that, if there's something of importance, if it does not work for the minister—and again, the minister was very clear about that—it is incumbent upon us, ourselves, his office and the Department of Public Safety, to find the right tool to put in place to make sure that critical information is seen by the minister.

I think this is one of the key measures that we need to put in place, to have this ability to adapt our processes when they're not working.

The Chair: Thank you.

Mr. Fergus.

[*Translation*]

Hon. Greg Fergus (Hull—Aylmer, Lib.): Thank you very much, Madam Chair.

Mr. Vigneault and Ms. Henderson, thank you very much for being with us.

[*English*]

Ms. Henderson, I'd like to go back to you to talk a little about these issues management notes, or IMUs.

Could you continue with your response—to Mr. Calkins, I believe—in terms of how the IMUs work? I'm going to ask a couple of questions. How do they work? Who is on the distribution list? Can you give me, not who specifically, but a vague number of how many agencies, departments or people are on that list?

Ms. Cherie Henderson: One thing that is important to understand is how the dissemination of the sensitive information works. It is not like a regular email back and forth. We have a very tightly controlled top secret system, which allows us to send information.

Within our own organization, our full organization is a SCIF. We all can have that right at our desktop, but in the average department they do not have that capability. Individuals actually have to go to a special protected room within that department, and only individuals who have verified access to that system can access it, read the information and print it off.

When we send out an IMU note, we actually send it to the department. The department, therefore, is the one.... there are specific individuals who have an email account, and they receive it. It would have been a specific individual within, for example, Public Safety or within, for example, PCO who would have access to that, be able to print it and then provide that information.

● (1950)

Hon. Greg Fergus: Thank you so much. That was very important.

It's a relatively wide distribution circulation, but under very specific and controlled access.

My question would be when you want something to be brought to the attention of a particular minister, how do you go about doing that with these IMUs?

Ms. Cherie Henderson: The requirement would be that we would send it to the department and we would then note on the note that this is to be shared with a particular individual. It could be the minister, it could be the minister's chief of staff or it could be the deputy minister.

They do not have access to that email system, but there are individuals within the department who would, and they would then be able to print it out.

Mr. David Vigneault: May I add something?

Hon. Greg Fergus: Please.

Mr. David Vigneault: Just to add another element to this, of course there's a lot of attention put on the issues management note, but the overwhelming majority of the information that the service shares with other departments would be our intelligence products. That would be going to an organization within the department. That organization is the one that would curate what needs to go to a minister.

When we step back from all of this, one of the lessons, if I can put it this way, is that this system may not be working as well as it should be to make sure that each minister gets the right level of awareness of our intelligence products.

I think my colleague, the national security and intelligence adviser, spoke to this, that we are doing something different. It's important, in fairness, for people.

I took Mr. Berthold's question earlier about the number of documents and so on. It is true that it is a very large number of documents. It is incumbent upon all of us to find the right way of making sure that the right information goes to the right people at the right time. This is not a science. That means we are collectively learning that this has not worked very well and we need to do much better with this.

Hon. Greg Fergus: My first question is this: Is the RCMP normally on this IMU distribution list?

Ms. Cherie Henderson: No, it is not normally. The IMU notes were originally designed in order to inform Public Safety and PCO. Recently we broadened that, and we look at it, as Director Vigneault has indicated, based on the need to know.

If there is something within a document that they need to know, we will share that, but it originally goes to Public Safety and PCO.

Hon. Greg Fergus: Thank you. Because we didn't have a full understanding of how the IMU works, I think that is an important answer and clarification to have to explain some of the testimony that we had this morning from the commissioner or the deputy commissioner in terms of why they weren't brought in the loop or brought into the circle for some of these products.

I'll continue very briefly.

When you want information brought to a particular minister's attention or a chief of staff's attention, what is the process?

I'll ask an easier question, because I don't want to go over the time. I will just be very quick.

There was a framework that was set this morning. They said we had developed our intelligence and security systems on the basis of responding to terrorism attacks. The world has changed. Some of the challenges for us are homegrown, and some others are from state actors or non-state actors.

Would you agree with that assessment in terms of how our system was designed, and that it has now changed?

● (1955)

Mr. David Vigneault: Very quickly, I think it's important, yes. I would say that, yes, it has been very much influenced. I think the evolution has been ongoing for some time about how we have to adapt our different processes around intelligence, sharing and focus, but I think we have done some of that work already. It's not over; it's not done yet.

Thank you.

The Chair: Thank you so much.

I guess sometimes confessions are good, and I think all of us know that I come from the Waterloo region. Last night the Denver Nuggets won the championship, and Jamal Murray was right there. He was born and raised in Kitchener, Ontario, as I was, so I am in the process of drafting an S.O. 31. I would appreciate it if members would keep their comments tight, so that I can do some of my other work while also paying attention to this work.

We'll make sure that all the time balances out, but kudos to Jamal Murray for bringing home the NBA championship for the Denver Nuggets.

[*Translation*]

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

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

Last week, we met the Sergeant-at-Arms because we're concerned about the protection and safety of parliamentarians. He told us that a memorandum of understanding was being developed between CSIS and the House of Commons regarding all intelligence-sharing matters. The purpose of that memorandum is to prevent what we've just experienced from happening again and perhaps to avert any potential incidents of the kind. The Sergeant-at-Arms added that a few details remained to be determined.

What kind of protection can we expect, since we're specifically talking about protecting MPs here?

Mr. David Vigneault: Protection from foreign interference is provided at various levels. I'm thinking in particular of protection for IT systems and physical protection. As I mentioned, we generally don't receive intelligence to the effect that parliamentarians are physically threatened. If that were the case, you could be sure that intelligence would be immediately forwarded to the authorities, and they would have been in the same situation as Mr. Chong.

Under the MOU that the Sergeant-at-Arms discussed with you, intelligence from CSIS and other government security and intelligence agencies will have to be merged in the best way possible to enable the right people to take the necessary protective measures. Those measures would include screening the people who work in your offices and providing increased support for MPs in doing that work. That's an example of the kind of information that has to be taken into consideration.

The work of the Sergeant-at-Arms will thus be to use intelligence from CSIS and from a number of other organizations to ensure that MPs are protected.

Ms. Marie-Hélène Gaudreau: I'm particularly concerned about artificial intelligence, cyber attacks and all that. My sense is that this is all moving faster than the machinery of our government.

Can you reassure us on that point?

Mr. David Vigneault: I'd like to reassure you, but unfortunately I have to say that technological capabilities are developing at a pace that, in some instances, outpaces our agencies' resources.

To increase awareness on this subject, our stakeholder engagement group recently had a meeting with a few hundred people, including journalists, on artificial intelligence and deepfaking.

Ms. Marie-Hélène Gaudreau: Thank you.

[*English*]

The Chair: Thank you.

Madam Blaney.

Ms. Rachel Blaney: Thank you.

I'm going to come back to the stakeholder engagement groups. You ended at a perfect place for me to continue my questions.

I'm curious about how people are selected for the stakeholder engagement group. What are the criteria, and do they change to reflect any sort of threat we might see from other countries? If a new country is becoming a threat, is there the flexibility to respond to that and make sure that the stakeholder engagement group is reflective of the issues we are facing?

Mr. David Vigneault: I have a couple of reflections on this. The group is a small group of dedicated professionals, and they rely on the support of the rest of the CSIS organization, and other organizations as well.

Specifically to the question, if there were to be a new specific threat vector, they would have the ability to get support from any other experts inside the organization to get the information and to find the right vehicle, the right venue, understanding also the sensitivity of some of these groups, including their nervousness to meet with an intelligence service and finding the right way of engaging. That sensitivity is one of the reasons they have been effective. They are trying to understand the situation, the specific reality of the group they will be engaging with and the individuals they will be engaging with. This is something that we continue to learn and try to get better at.

● (2000)

Ms. Rachel Blaney: Following up on that, does the diversity of the stakeholder engagement group reflect some of the groups that you're trying to reach? When I think about the testimony we have heard so far from some of these groups, they have talked about the fact that there is often a high level of fear preventing people from coming forward. They are concerned about their loved ones overseas. They are concerned about their own safety and that of their family.

We know a lot of those communities have a very poor relationship with previous governments and police in terms of the authoritarian governments.

How is this outreach? I think of these groups. They have been ringing the bells. They have been saying that this is happening and they weren't heard, so I want to make sure that the systems you are putting in place actually bring them in instead of just pushing them further away.

Mr. David Vigneault: The member is raising a critical lesson that has been learned, and we do strive to have a very diverse group of people who will be doing the engagement. When it's not possible, given the fact that we are engaging with lots of very diverse groups, we put a premium on people who will understand how to work with these communities and engage in long-term relationships.

We have met with a number of these groups. We try to be careful with what we say publicly, because we do not want these groups to be thinking that we are just doing this for PR reasons, but we also do not want the people who are interfering with their activities to put a target on their backs.

The Chair: Thank you.

We will go to Mr. Cooper, followed by Mrs. Sahota.

Mr. Michael Cooper: Thank you, Madam Chair.

Mr. Vigneault, David Johnston repeatedly claimed in his report that with regard to foreign interference in the 2021 election, "misinformation could not be traced to a state-sponsored source."

This is in stark contrast to what Mr. O'Toole informed the House, namely that CSIS briefed him that his party, several members of his caucus and Mr. O'Toole were targets of misinformation and voter suppression orchestrated by Beijing before and during the 2021 election.

How can Mr. Johnston's conclusions be reconciled with what CSIS informed Mr. O'Toole?

Mr. David Vigneault: Thank you, Madam Chair. I'll be trying to straddle the line on the classified information here.

The ministerial directive is quite clear that CSIS is to share all information that it has at its disposal, as it was with the case in question.

I mentioned earlier that sometimes we have information that needs to be corroborated, that needs to be vetted under rigorous practice. Without going into very specific details, I can say that there was some information that was shared in that briefing that may have been in that category, but it was important to respect the directive that all information be shared.

I think, in his testimony, the independent special rapporteur also mentioned that there may be other information that he would need to look at. The focus of the work was clearly on the 2019 and 2021 elections, but that doesn't mean it's to look at all of the intelligence available through CSIS or other agencies. This is one of these situations we're faced with now, the words of the MP in the House versus what was shared by CSIS versus what was provided by the rapporteur.

● (2005)

Mr. Michael Cooper: Thank you for that.

Now, there's quite a gap, quite a contrast, really, between what Mr. Johnston concluded, that he couldn't find evidence that the interference was state-sponsored, and what Mr. O'Toole was told by CSIS, which was that Beijing orchestrated a campaign that included misinformation, using, among other things, state social media accounts. That was also contained in a rapid-response mechanism report that, frankly, Mr. Johnston should have seen and couldn't explain how he hadn't seen when he concluded, as he did, that he couldn't find evidence that the interference was tied to the Beijing regime.

Mr. Johnston, as you also alluded to, stated in answer that he based his conclusions on the intelligence that he had. Are you suggesting that Mr. Johnston wasn't provided all relevant evidence and intelligence, or do you know?

Mr. David Vigneault: What is clear is that the focus of the work was on the integrity of the election in 2019 and 2021. I think that the work and the report clearly focus on that.

The discrepancy that the member points out is a very valid point. As I mentioned, the information that was shared under the ministerial directive was to be all information. That doesn't necessarily mean that it's information that we would have assessed as something with the right level of certainty about the action. That information was shared despite that. It's not necessarily information that had been previously put into intelligence reports, because it was still being developed. We still needed to confirm some of that information.

I totally understand the confusion that exists here. I think this is something that, with access to all of it, will be available.

Mr. Michael Cooper: Thank you for that.

You are quite right. It pertained to Mr. Johnston's report, and the subject of his investigation was specifically the 2019 and 2021 elections. The information that was shared with Mr. O'Toole pertains directly to the 2021 election.

Mr. Johnston already had his report in translation by the time he saw fit to interview Mr. O'Toole. Then he basically failed to address it and came, evidently, to completely erroneous conclusions.

Thank you, Madam Chair.

The Chair: That was more of a comment than a question. Is there nothing to add? Okay, I just wanted to confirm.

Madam Sahota, you have the floor.

Ms. Ruby Sahota: Thank you, Madam Chair. I think we can take it from there.

I still don't think we're being completely clear. I think there's a misunderstanding here that's happening at committee. You just said that, just because there is intelligence—in going back to the issue of the briefing that was given to Mr. O'Toole.... If CSIS believes that the source or origin of misinformation or an orchestrated campaign—whatever you would like to call it—believes that it may be linked to a foreign state actor, does that make it so?

Is that evidence that it is absolutely linked to that foreign state actor, or could there still be a possibility that the actor may be here in Canada and spreading that misinformation or orchestrating a campaign? It's to have clarity on that point.

Ms. Cherie Henderson: That's a very important question to dissect a bit.

When we collect any piece of intelligence, we are trying to build a picture, so every piece of intelligence is assessed on its own merit. In some cases, we will have a very solid source that we receive that information from, and in some cases we may not. We try to corroborate that information in order to build a better picture. Every piece of intelligence goes into understanding what the actual situation is, but sometimes you are still trying to build the picture, and you don't have a lot of really strong.... Our threshold in the service is to suspect that there's a threat, which allows us to investigate, so it could even be that we suspect this could be what's happening but we don't yet have that clarification to believe it.

● (2010)

Ms. Ruby Sahota: That's very helpful.

In this instance, when it comes to Mr. O'Toole's briefing, did you suspect, or did you know? What was he briefed on?

We know what he understood, and then I think this is exactly why.... For all of us, it is educational as to how these briefings should be provided and how it should be explained to members of Parliament why you believe certain intel to be so; or maybe it's an absolute evidence that, ah ha, we have backup to prove that this is where it's coming from. Based on the testimony that we've received from Mr. Chong, the briefings that were given to him were at a very high level. There wasn't a clear understanding or a clear picture of what was explained to him in some of the briefings he had received before the news reports came out.

In the case of Mr. O'Toole, we know what he believes, but did CSIS inform him that it believed that was the origin of the information, or was he informed that you had evidence, solid evidence that this was where it was coming from? Therefore, could David Johnston's conclusion, in your opinion, still be correct?

Mr. David Vigneault: I'll provide a couple of comments on this.

First, maybe just to correct the record, it has been mentioned in the media and other venues that the briefing to Mr. O'Toole was provided by me personally. That's not accurate. It doesn't make a big difference, but just to correct the record, it was provided by very senior CSIS officials.

That said, the very specific details of what was shared with Mr. O'Toole, unfortunately are classified, so I cannot provide the member with that level of specificity. However, what I think is clear, as I mentioned earlier, is that we provided all of the information we had, and that includes information that, as my colleague Ms. Henderson mentioned, may still be need to be fully validated. That is why these discussions about intelligence matters sometimes require a lot of very specific discussions and details. Those nuances are very critical so as not to create confusion, some of which, unfortunately, we do have at the moment.

Ms. Ruby Sahota: All of that evidence pertaining to this briefing, then, and the evidence that led you—or whoever briefed Mr. O'Toole on the information that was gathered—to believe...was all given to Mr. David Johnston.

Mr. David Vigneault: Madam Chair, as I mentioned earlier, a lot of information was shared with the special rapporteur. However, the focus of his review was not to look at each and every specific instance of members, so some of that information would not have been part of the specific work of Mr. Johnston.

As I said, if information has not been fully validated by CSIS, we would be very careful about sharing it, since someone may draw conclusions based on information that we have not validated yet. I think that explains a bit the situation that we're in now and some of the confusion that exists in the public domain.

Ms. Ruby Sahota: That was very helpful, so it was not validated. Thank you.

The Chair: Thank you.

We are entering our fourth round.

[*Translation*]

Go ahead, Mr. Berthold.

Mr. Luc Berthold: Thank you very much, Madam Chair.

Mr. Vigneault, we're going to address a really interesting topic, your organization's estimates. In 2020-2021, CSIS's budget was $676 million.

Is that correct?

Mr. David Vigneault: I'll have to take the member's word on that, but that seems to be about the right figure.

Mr. Luc Berthold: The main estimates showed additional amounts to combat foreign interference. The figure is $648 million for the 2022-2023 fiscal year.

Is that correct?

Mr. David Vigneault: No, I don't think so.

How much did you say?

Mr. Luc Berthold: I said $648 million.

Mr. David Vigneault: That's the total service budget, not the foreign interference budget.

● (2015)

Mr. Luc Berthold: I said that budget included additional stated amounts.

Mr. David Vigneault: All right.

Yes, that seems right, in that case

Mr. Luc Berthold: So that represents more than $20 million less than in 2020-2021.

Is that correct?

Mr. David Vigneault: Yes, that's correct.

Mr. Luc Berthold: You therefore have a budget of $648 million to gather intelligence and have agents on the ground preparing reports. That information is then shared with people who use it as a basis for making decisions.

Is that correct?

Mr. David Vigneault: Intelligence work includes those elements, but many more factors are obviously included in the spending amount the member mentioned.

Mr. Luc Berthold: But that's the main focus of the service's work.

Isn't it?

Mr. David Vigneault: Our work comprises the collection, analysis and transmission of intelligence.

Mr. Luc Berthold: I was surprised to learn during the discussions that the information that comes from CSIS falls into black holes. The government spends $650 million a year without establishing a clear and direct process for using all the information that's gathered. We heard that from the deputy minister of Global Affairs Canada and the present national security adviser.

As the director of an intelligence agency that costs taxpayers $648 million a year, how do you feel, after all your efforts and after gathering intelligence from your agents in the field, about the fact that all that information falls down black holes? Doesn't that seem somewhat unacceptable to you?

Mr. David Vigneault: I can say that one of the most gratifying things for us is knowing that the work done by everyone at CSIS and all those in the intelligence community helps protect Canadians. That's very important for us. We are passionate about that, and our employees are very devoted.

Certainly, having a system that wrings the most out of every scrap of information absolutely deserves special attention. Right now, I think we're taking the opportunity to ensure that resources and efforts are channeled toward ensuring that we protect Canadians in a world where threats against Canadian interests are unfortunately increasing.

Mr. Luc Berthold: Right now—and we've seen this in some of the other testimony—the government and Minister Blair seems to want to make CSIS responsible for the fact that this information wasn't shared with the right people at the right time.

You've answered many questions about Minister Blair, but he has definitely attributed responsibility to you for the decision not to send him the information. How do you explain that?

I'm not talking about the fact that he wasn't made aware of it. You're not denying that. And yet Minister Blair nevertheless said that I should ask the director of CSIS why that information concerning Michael Chong wasn't shared with him.

Don't you think that comment is a bit much?

Mr. David Vigneault: I think I had the opportunity to answer the questions. Yes, we shared the information, but it didn't make it to the minister. That failing should definitely be corrected in short order.

Mr. Luc Berthold: This is my last intervention this evening, and I'd like to ask you a final question.

Regarding this black hole, what message would you like to send to the deputy ministers to whom you send these internal management notes?

We won't be solving anything this evening. There won't be any new legislative changes. However, do you have a message to send to all those people this evening so they clearly understand that an internal management note is the first thing they should read every morning when they get to their offices? If they see one on their desks, it's because it's important.

Mr. David Vigneault: I think that the message for all of us, including CSIS, is that we have to improve our processes. Clearly, they haven't always been effective.

My message would also be that the world has changed. The threat to Canada and its population has changed. We, all of us, have to do better. That's really the message I'd like to send.

I have to say that I've been reassured by the fact that people took note of that analysis. Everyone is aware of the fact that we all have to work better together to protect Canadians.

Mr. Luc Berthold: However, you didn't have to take the rap for the incompetence of certain deputy ministers.

● (2020)

Mr. David Vigneault: I don't have a response to that comment, Madam Chair.

Thank you.

The Chair: Thank you very much.

Mr. Vigneault, you've been very cooperative. You responded very quickly to our request that you appear here. We are going to take up a little more of your time this evening so everyone can ask you questions. So I'd like to thank you, you and Ms. Henderson, for your cooperation.

Mr. Turnbull, you have the floor for five minutes.

[*English*]

Mr. Ryan Turnbull: Thanks, Madam Chair.

In Mr. Johnston's report, he identifies shortcomings that I think have been long-standing in terms of the flow of information, and he identifies communication gaps. When Ms. Thomas was here, she talked about how CSIS actually collects and sits on a lot of intelligence for a period of time.

One of the things I've been wondering is how long it takes to build a profile or a dossier of information, on average, before you actually share it. How long do you sit on intelligence before you share it?

Ms. Cherie Henderson: It really depends on the investigation we're engaged in.

As I indicated earlier, when we start an investigation, our threshold is that we suspect...because of information we have started to collect. Depending on that piece of information—and each piece of information, as I noted, is assessed on its own merit—we look at it and how it fits into the greater picture.

It really depends on each piece of information. Sometimes we could get something we would want to share right away, but sometimes it will take a bit longer because it hasn't hit the threshold of being validated. Really, it impacts our credibility. If we just sent everything out immediately without having a proper look at it and an assessment of it, it could really impact the credibility of our organization and the ongoing information we share.

It really depends on what we're collecting, how the investigation is moving forward and the quality of the sources that we are working with.

Mr. Ryan Turnbull: There is sort of a threshold where you suspect something that then gives you licence to investigate and gather additional intelligence. You're piecing together a picture, and then there's another threshold you reach where you say, okay, now it's time to actually share this up the chain with other parties, i.e., ministers' offices and so on. Is that right? What is that threshold?

Ms. Cherie Henderson: Yes, that's right, and as I indicated, it really depends on the seriousness of the actual threat we're looking at and the amount of information we have to support our assessment of the seriousness of the threat.

One thing I would also add is that when we're doing an investigation, we begin with the building block pieces on the suspect, but sometimes we get to a point at which we recognize that the threat is serious enough that we actually need to go to a federal court and get a federal court warrant in order to be able to investigate the threat that much more.

As we're going through the process in each investigation, it depends where we are in the investigation at what point we start sharing that information.

When we're talking specifically about foreign interference, that is something we have been building a picture of for a very long time, as an organization. That's why we have been trying to push out a lot more information. We have also been speaking a lot more publicly about this, because of the fact that it is a very serious threat that we're facing in our country.

Mr. Ryan Turnbull: Thank you.

What mandate and accountability does CSIS have for briefing deputy ministers and/or ministers?

I assume that within the CSIS Act you may have very specific accountabilities and a mandate that says that when you hit a certain threshold, you have to communicate that. Maybe there is a protocol for communicating. I am assuming so, but maybe you can clarify.

Ms. Cherie Henderson: That's a very interesting question.

Mr. David Vigneault: I mentioned earlier that there are two different ways we share that information. One will be with intelligence reports, raw intelligence and assessed intelligence.

Also, at the deputy minister level, I sit at a number of different deputy minister committees where some of that information is shared directly. References are made to specific reports, to tell people, "You should take a look at this information. It's of relevance."

The national security intelligence adviser said that with some of those gaps that have been identified recently, she has put in place a new process where we are meeting weekly to discuss specific reports that have been flagged, to make sure that the level of awareness is there and that actions can be taken very quickly, directly.

It is not just a single way of sharing. It's also not defined in the CSIS Act, to answer the question of the member. It is based more on professional expertise.

● (2025)

Mr. Ryan Turnbull: Based on what you said, it seems to me that the sources of CSIS leaks that we've experienced over the last few months are particularly problematic if they're coming out and haven't been corroborated and verified or gone through the process that you just described.

Would you say that is the problem with how things have been spun in the media? It seems to me that they've been taken out of context.

Mr. David Vigneault: I'll make a couple of points.

The first one is that intelligence professionals and the people of CSIS take their work extremely seriously. Those leaks have been damaging to the morale and reputation of the organization. Investigations are ongoing. I really hope that soon there will be information that will be public. An individual or individuals may or may not be from CSIS. It's clear that there was information from CSIS and also from the Privy Council Office.

I believe it is important to have a specialist to be able to help people to understand and contextualize the intelligence and to put it in the right context.

The Chair: Thank you.

Madame Gaudreau.

[*Translation*]

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

I've gotten answers to many of my questions, and I only have two left. I can see that we have a lot of work to do.

Many countries have two intelligence agencies. Earlier I mentioned France's Direction générale de la sécurité intérieure and its Direction générale de la sécurité extérieure.

The United States has its Federal Bureau of Investigation, the FBI, and their Central Intelligence Agency, the CIA, which are well known.

The United Kingdom has its MI5 and MI6, sections 5 and 6 of Military Intelligence.

Has Canada reached the same point? Does it need domestic and international intelligence services.

Mr. David Vigneault: That question has been raised many times in recent decades.

One thing that people don't necessarily know about CSIS is that it has a significant international component. Even though it's a single agency that has been given a very specific mandate, it isn't limited by geographical constraints when gathering intelligence on threats against Canada. CSIS agents are thus posted temporarily or permanently around the world to do the work that's asked of them.

Many countries have developed their procedures by establishing two agencies. Could there be a reason to review CSIS for that purpose? As I told you, the review currently under way should be quite open.

However, to be very honest with the member, I'd say this isn't necessarily the first solution I would consider for correcting potential deficiencies and better protecting Canadians.

Ms. Marie-Hélène Gaudreau: Madam Chair, since I have a little time left, I'd like to ask Ms. Henderson a question.

Ms. Henderson, you said at another committee meeting that there was a lot of information on the Internet that can help people understand more clearly, do prevention and so on.

Based on everything we've seen, I've come to understand that I never would have taken the time in my life to read this kind of information or that I might have to know more about the strategies associated with any particular threats that might concern me.

What action plan could CSIS recommend to me so I could be sure I was equipped and informed? How can you be transparent enough to avoid potential threats?

[*English*]

The Vice-Chair (Mr. John Nater (Perth—Wellington, CPC)): We'll provide some time for a response.

● (2030)

[*Translation*]

Ms. Cherie Henderson: Thank you very much for that question.

[*English*]

I think the first part is actually the awareness piece. I think that's what we're starting to have, that conversation in Canada. The first part is making sure that you understand that one. Because of who you are and the position that you have within the government, you are somebody who they would be interested in. I think Canadians on the whole don't really think that people are going to be interested in us and trying to get access to us, but they are. We are a very strong nation. We have a lot of good work going on. We are considered a moderate power that can engage. People want to, or hostile states want to, have access to you and be able to know what we're thinking and see how they can influence us.

I think that's the very first point. It's just to be able to be aware. It's not to be fearmongers, but it's to be aware and to understand what's going on around you.

Then you move from there into understanding, making sure you have the proper protection of your systems and making sure that if you see anything you report it and have those conversations and discussions.

It's an ongoing evolutionary process. The more we all learn, the better we can prepare and protect ourselves. That's including you and including the members in your offices. It's not just you; it's making sure the people in your offices are all aware and can protect themselves as well. That's where we start from.

As we gather more information, we can get to a point at which we can bring in the police. We can get to that point. It starts, really, with each of us as individuals recognizing that people are interested in us and will try to get access to us.

[*Translation*]

Ms. Marie-Hélène Gaudreau: Madam Chair, thank you for allowing me more time. There have been a lot of distractions around the table, and it's hard to focus at this time of day.

The Chair: So next time I'll take back the two minutes that I gave you this evening.

Ms. Marie-Hélène Gaudreau: No, the distractions came from the group as a whole.

The Chair: All right. Thank you.

Go ahead, Ms. Blaney.

[*English*]

Ms. Rachel Blaney: Thank you so much, Chair.

I have just one question.

There has been discussion and testimony from both of you today about the intersection between consumers of intelligence and receivers and preparers of intelligence. One of the things we've heard is that one of the challenges is around political awareness. If you're preparing information for a political world, how do you make sure the information makes sense, and what are you looking for that's meaningful?

We have heard testimony from some of the national campaign managers, who said that during the election, the interactions they had to learn about foreign interference and be briefed really felt like ticking a box. It didn't really give them what they needed to assess the issues more fulsomely. I'm just wondering what work is being done to prepare for the next election, to understand how politics works on the ground and how to have appropriate information to guide people to do things correctly and to be able to identify when there is a threat.

Mr. David Vigneault: When we talk about threats to our democratic processes, political parties are absolutely critical elements. It is very recent, through the work of the security and intelligence task force, the threats to elections task force, that this process has been put in place where there will be people with the clearance to receive classified information.

I listened with interest to the commentary of the political party members who testified, and I think they shared very important points when they asked how they can make use and sense of and be able to do something with the intelligence. I think it's something that not only CSIS but the other members of the security and intelligence community and the Privy Council Office, who are responsible for that level of interaction.... I think it's something that will be a priority to review, to make sure that we all get better at giving the information and the ability to use that information.

Ms. Rachel Blaney: You're saying it's a priority, but you didn't say if there are any concrete actions that are happening right now to address that. It seems to me that we should always be preparing for the next election.

Mr. David Vigneault: I can mention the fact that it has been announced by the Minister of Intergovernmental Affairs that the SITE task force has been stood up for the by-elections that are currently under way.

I would say that one of the very needed actions will be to get the report from SITE and then to make those adjustments as required. I think it's fair to say that it's more work that will be carried out after the by-election.

● (2035)

The Chair: Thank you.

We have gone past the time, but as Mr. Cooper has signalled to me that we need just a bit more time, we will go to the Conservatives and Liberals to finish up this round. Will two—max three—minutes be enough, Mr. Cooper?

Mr. Michael Cooper: That would be good. Thank you for that, Madam Chair.

I want to put on notice—and I emphasize "notice"—a motion, and I'd ask that it be taken up next week so that we can have a debate around it.

Let me say very briefly, Madam Chair, that until it does what Parliament has called on it to do three times—and that is to call an independent public inquiry into Beijing's attack on our democracy in two federal elections, the targeting of sitting members of Parliament and the intimidation of Chinese-Canadians, the failure of this Prime Minister to take meaningful action to combat it and indeed evidence that the Prime Minister turned a blind eye to it—this government has a lot to answer for. This is the only committee, the only forum, in which questions are being asked and witnesses are being called to get to the bottom of Beijing's interference.

With that, Madam Chair, the motion that I will be putting on notice is as follows:

> That, in relation to its order of reference of Wednesday, May 10, 2023, concerning the intimidation campaign orchestrated by Wei Zhao against the member for Wellington—Halton Hills and other members, the committee hold at least eight meetings, of at least two hours' length, between Tuesday, July 4, 2023, and Friday, September 8, 2023, on dates to be determined by the subcommittee on agenda and procedure, for the purposes of hearing witnesses and considering related committee business.

Thank you, Madam Chair.

The Chair: Thank you, Mr. Cooper.

We will take notice of that motion and make sure it's circulated.

With all of the witness names that have been shared and so forth, we have witnesses for this Thursday. We believe that we will be able to have a meeting on Tuesday morning with witnesses.

This Thursday, we will be notified by the House of Commons on whether we have resources on Tuesday evening. Should we have those resources, this is when I would take up this notice of motion.

I would also welcome other thoughts. I think it was kind of you to provide notice and to allow us to come to the conclusion of this meeting by finding time next week for suitable resources.

Is everyone good? That's excellent.

To end us off, Mrs. Romanado, there are three minutes for you.

Mrs. Sherry Romanado: Thank you very much, Madam Chair.

I understand we will be discussing this notice of motion next week. I understand also that Mr. Chong stood up in the House yesterday and said he was hoping that PROC would deal with this before the House rises.

However, Mr. Vigneault, I want to get clarity, because we've been receiving conflicting information with respect to some of these briefings.

The motion with respect to the opposition motion in February 2021 ended up flagging the subcommittee members on human rights. An IMU was prepared in May 2021, which you mentioned did not reference the name or identify Mr. Chong. However, that prompted a briefing from CSIS with Mr. Chong on June 24, 2021—a defensive briefing. Subsequent to that, Mr. Chong initiated three meetings with CSIS: August 5, 2021, February 25, 2022 and July 18, 2022.

Madam Henderson, you mentioned that part of bringing defensive briefings to members of Parliament is to educate them and their staff on some of the tactics used by state actors.

Would you say that it could be accurate that CSIS was trying to solicit information from Mr. Chong to augment the intelligence you were gathering?

● (2040)

Ms. Cherie Henderson: The purpose of the personal security briefings is so that individuals are aware of what's happening around them. We hope that if they are aware, then, yes, they will discuss with us. The original intent is not to try to get information from them at all. It is to create that awareness among the individuals, so that they can protect themselves if they see anything. Then, if they so choose, they can come back and talk to us about it.

Mrs. Sherry Romanado: In that regard, we heard this morning that the then NSIA, Mr. Morrison, stated that no MPs were named. However, in the Johnston report, on page 27, it clearly indicates that the current NSIA has acknowledged to Mr. Chong that her predecessor at the time received the memorandum that described the potential action against Mr. Chong. That also references the May 2021 IMU. I'm not quite sure...because there's a conflict of information here.

We're being told that the IMU and the assessment did not reference any specific MPs, yet the report says that it did. We have some people saying it does, and we have other people saying it's not. I'm not quite sure. This is public information, so I'm trying to get.... Again, I'm not asking what was in it, but there's some conflicting information here.

Mr. David Vigneault: I will try to, hopefully, provide a little clarity.

The IMU did in fact contain specific names. The July report that I think you referred to was an assessment. The specific names were not included in that. As I mentioned, those names are available if there is a need for someone to know, understand, decide or determine, "Okay, I need to do something with this." Those names are then made available. On a question of accountability and making sure we respect people's privacy, we would not put people's names in those reports all the time.

Madam Chair, hopefully that helps the member with so many different reports and so many different references.

Mrs. Sherry Romanado: Thank you, Madam Chair.

The Chair: Thank you.

With that, Mr. Vigneault and Ms. Henderson, it was really nice of you to take the time to be here with us. Thank you for being generous with your time. You provided us with more than we anticipated. On behalf of all PROC committee members, I want to thank you for your service and your time.

If there's anything else you would like to add, please just share it with the clerk, and we will have it provided, in both official languages, to all members.

With that, we wish you the best, and thank you for your service. Members, we will see you on Thursday.

The meeting is adjourned.