HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

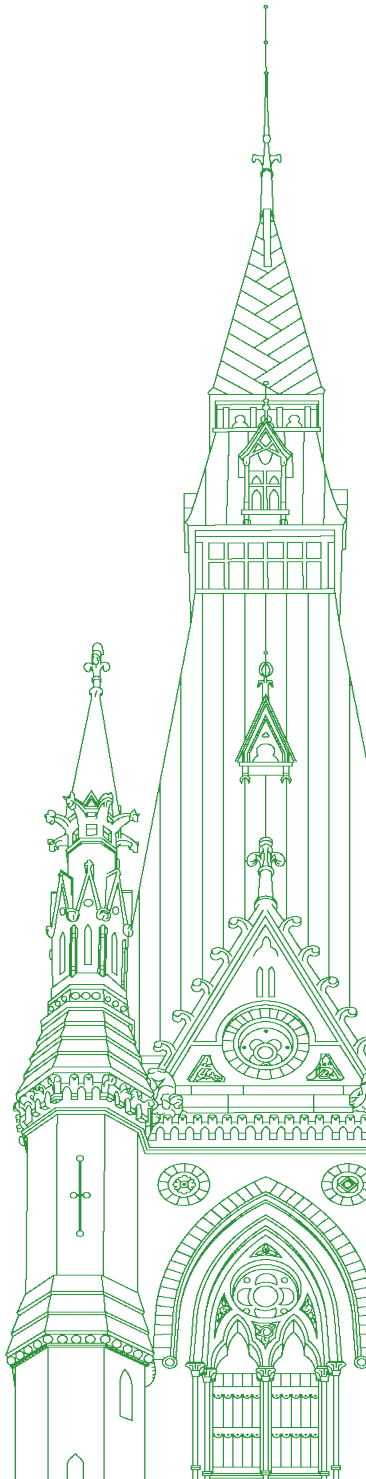
Standing Committee on Procedure and House Affairs

EVIDENCE

NUMBER 118

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Tuesday, June 4, 2024



Chair: Mr. Ben Carr

Standing Committee on Procedure and House Affairs

Tuesday, June 4, 2024

● (1100)

[*English*]

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

[*Translation*]

I hope all of you had a good weekend in your ridings.

Colleagues, welcome to meeting number 118 of the Standing Committee on Procedure and House Affairs.

The committee is meeting today to discuss the question of privilege related to cyber-attacks targeting members of Parliament.

[*English*]

Colleagues, we are all very well aware of the new regulations for audio devices. Please take good care to make sure that when they are not in use, you are placing them on the stickers provided in front of you on the table, either to your left or to your right.

I notice that we have a number of non-permanent members at the committee. Welcome to those who are here as substitutes today.

Colleagues, we have had a couple of very productive meetings. We have been dealing with some sensitive and difficult issues. Despite that, the conversation has been respectful. We've been able to maintain a good dialogue between those asking questions and the witnesses we've had. I hope we can continue in that spirit today.

[*Translation*]

We have a lot of witnesses this morning.

[*English*]

They are no strangers to us. They were with us not too long ago.

I would like to welcome back Eric Janse, Clerk of the House of Commons; Stéphan Aubé, chief executive administrator; Michel Bédard, law clerk and parliamentary counsel; Patrick McDonell, Sergeant-at-Arms and corporate security officer; Jeffrey LeBlanc, deputy clerk of procedure; and Benoit Dicaire, acting chief information officer, digital services and real property.

Mr. Janse, you and your colleagues will have 10 minutes collectively to begin the meeting. Following the conclusion of those remarks, we will go into our first round of questions.

[*Translation*]

Mr. Janse, the floor is yours.

[*English*]

Mr. Eric Janse (Clerk of the House of Commons): Thank you very much, Mr. Chair. It's a pleasure to be back before the committee, this time on a different topic than last week's and with a slightly different cast of characters before you.

We are appearing today regarding the prima facie contempt arising from the cyber-attacks by a foreign-backed entity called Advanced Persistent Threat 31, allegedly supported by the People's Republic of China and targeting members of Parliament. We trust that our testimony today will assist the committee in its consideration of this important question.

In his May 8, 2024, ruling, the Speaker broke down the question of privilege into two distinctive parts. The first was the issue of the lack of notification of members regarding the cyber-attack, and the second was the attack itself.

In his ruling, the Speaker noted that, since the attack, processes and protocols regarding the notification of members had evolved. The Speaker, notably, referred to the May 2023 direction from the former minister of public safety respecting threats to the security of Canada directed at Parliament and parliamentarians. He also mentioned this committee's recommendation, contained in its 63rd report, that members of Parliament be notified by CSIS of the foreign interference threats targeting them.

In the second part of his ruling—that is, the cyber-attack itself—the Speaker found the matter to be an attempt to interfere with the work of parliamentarians, and he ruled that the matter was a prima facie question of privilege.

● (1105)

[*Translation*]

In reaching his conclusion, the Speaker referred to the prima facie question of privilege raised by the member for Wellington—Halton Hills, which was the subject of a ruling from the Speaker's predecessor on May 8, 2023. In that case, the member was the subject of threats of reprisal by foreign actors for positions he had taken during debates.

In his ruling finding a prima facie case of privilege, the Speaker stated that the matter raised by the member squarely touches upon the privileges and immunities that underpin the collective ability to carry out parliamentary duties unimpeded.

At the culmination of its study on this prima facie question of privilege, this committee presented its 63rd report to the House on April 10, 2024. While the report is not yet concurred in, it contains many recommendations. As the committee considers this latest question of privilege, it may seek to build upon the conclusions of that report and provide further recommendations to the House.

[*English*]

Three of the recommendations in the 63rd report were directed at the House administration.

The first suggested that training on foreign interference be developed and offered as part of the members' orientation program and on a continual basis. This had been in development for some time, and I am pleased to say it is currently being offered to caucuses and will be part of the next orientation program.

The second sought a contact person to be assigned by the House administration to liaise with members on all matters related to foreign interference threats. The third, related recommendation suggested that a protocol be developed to inform the whips about foreign interference threats.

I note that agreements with our security partners relevant to these recommendations are already in place. We will be happy to provide further information about these later on during the meeting.

[*Translation*]

This new question of privilege provides the committee with the opportunity to consider some additional elements that were brought to light regarding cyber-attacks toward members individually and to the House as a whole.

Cyber-attacks have several objectives, one of the most obvious being to disturb our technical systems, and as such impacting the ability of members to do their work. They can attempt to steal confidential information, impacting members' ability to work on sensitive files. These attacks might also be seen as attempts to intimidate members, therefore also interfering with the business of the House. When individual members are the subject of various forms of obstruction, the House as a whole can be impeded.

As indicated by the Speaker in his ruling, these types of attacks are more and more common. The issue raised by the member for Sherwood Park—Fort Saskatchewan related to cyber-attacks by a foreign entity targeting emails, but other modern technology may be used to disturb parliamentary proceedings. In some cases, the entities behind the attacks can be identified, and in other cases they cannot.

[*English*]

Another element to consider is the difficulty for the House to assert its rights when a foreign entity is the sponsor of reprehensible actions. Furthermore, if the House can, to a certain extent, mitigate the impact and risks when attacks target its own systems, when other systems, such as personal emails, are used by members to fulfill their duties, the House's ability is limited. Members can currently use various tools to fulfill their parliamentary functions, some supported by the House's IT services and others not.

[*Translation*]

When examining a question of privilege, the committee typically avails itself of the usual powers as it would when conducting any study. In terms of privilege, it will seek to establish the facts. It can propose remedies and proposals by way of recommendations in a report presented to the House.

I will now ask my colleague, Benoit Dicaire, acting chief information officer, to provide further information on cybersecurity at the House of Commons.

Mr. Benoit Dicaire (Acting Chief Information Officer, Digital Services and Real Property, House of Commons): Thank you, Mr. Clerk.

Thank you, Mr. Chair.

I'm here today to talk to you about cybersecurity in the House of Commons, specifically to give you information on our evolving cybersecurity posture and the House administration's commitment to protecting the institution and its users from cyber-threats.

The cyber-threat landscape is constantly evolving and becoming increasingly complex and challenging. The proliferation of technologies in this new digital reality is introducing significant growth in new threat vectors. In addition, the sophistication of threat actors is driving the House of Commons administration to continuously evolve and adapt our cybersecurity program to reduce emerging risks.

[*English*]

The House administration IT security team has a specific mandate to strengthen Parliament's cyber-resilience against a continuously evolving digital threat environment. Its role is specifically to protect the availability of IT resources, to ensure the continuity of parliamentary operations and to protect the confidentiality and integrity of the infrastructure system and its users, including members of Parliament and their data, whether in Ottawa, in constituencies or while travelling or working remotely. The House administration IT security team's mandate is for parliamentary information and devices only. Our role does not extend outside of members' legislative functions.

● (1110)

[*Translation*]

Parliament's cyber-resilience relies on an integrated approach based on proactive measures such as ongoing monitoring, intelligence, threat hunting, vulnerability management, the development of incident response guides and regular exercises.

It is equally important to take reactive measures to ensure our ability to effectively detect incidents, threats and security breaches, to respond quickly when they are detected and to rely on them as they occur.

[*English*]

This approach is inspired by internationally recognized standards and best practices, such as the ISO 27000 series, the NIST cybersecurity framework, ITSG-22 and ITSG-33. It ensures that security controls and processes are in place to mitigate cyber-risk and to respond adequately to cyber-incidents.

In addition, this integrated approach is supported by various critical partnerships to effectively collaborate, share information and strengthen our cybersecurity posture. I will share more information about these partnerships in the in camera portion of this meeting.

That concludes the public portion of our introduction. We would be happy to take questions or answer any concerns.

Thank you.

The Chair: Thank you very much, Mr. Janse and Mr. Dicaire.

Colleagues, I have just a quick reminder. I briefly suggested last meeting that it would be helpful to the chair if, when you ask your questions, you have a timer in front of you or if the colleague next to you has a timer. It's certainly not required, but it means I don't have to speak over you to interrupt and keep you focused. I know sometimes that can be a distraction, but it's helpful for the efficiency of the meeting.

Mr. Genuis, the first six minutes are yours. I turn the floor to you.

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

We're here to discuss the fact that 18 parliamentarians were targeted by APT31, a Chinese state-affiliated hacking outfit. I was one of the 18. The attack targeted parliamentarians involved in the Inter-Parliamentary Alliance on China, which is, I should note, a great and important legislative network that brings together legislators from various countries and continents across different political traditions to work on issues related to the CCP.

I should have been informed about this attack but wasn't. My questions will focus on the notification of members. The government's public statements have suggested that they were aware of this attack. They chose not to inform members. They shared some information with the House administration.

Can you confirm whether and when the government shared information about this attack with the House administration?

Mr. Eric Janse: Thank you for the question, Mr. Genuis.

Indeed there were exchanges between security partners and the House administration at that time. We can perhaps provide some more details during the in camera portion, Mr. Genuis.

I think what was pointed out during the report—and certainly we can confirm from our end, and our security partners can on their end—was that if a similar situation were to occur today, things would be done differently from how they were when this incident occurred.

Mr. Garnett Genuis: The government could have informed members directly. From my perspective, there's no reason why they shouldn't have. Saying that they told somebody else looks like an excuse.

In the context of informing the House administration, was whether or not members were informed discussed? Did they express an expectation that members would be informed? Did they express an expectation that members would not be informed? Was that an issue in the conversation?

Mr. Eric Janse: I hate to do this, Mr. Genuis, but I'd like to suggest that perhaps this can be addressed in the in camera portion.

Mr. Garnett Genuis: I won't press the point more than to say that it's a question of political accountability for the government whether or not they sought to get this information to members. If they had asked you not to share the information with members, I think that would be germane to the public conversation around this issue. If they had made other comments.... You know what you know, and I don't know it, so I'm not going to press you beyond your comfort level. However, I think whatever advice the government gave around whether members should be informed is a matter of legitimate public interest.

● (1115)

Mr. Eric Janse: It's a fair point. Again, in order to provide a truly fulsome response to your question, we would prefer to do so during the in camera portion.

Mr. Garnett Genuis: Maybe we'll follow up, and at that time the committee can decide what information should be shared publicly.

One thing has really bothered me about it. I think most members were attacked through their parliamentary accounts. I was not. I was attacked through my personal account. It was related to my parliamentary work, of course, but my personal email account, which is not published, was nonetheless targeted.

The response we heard early on in a media comment by the Speaker's office was that there was nothing to worry too much about because the attack had been thwarted. My understanding—and perhaps you could clarify this—is that House of Commons security is not involved in monitoring or protecting the personal non-parliamentary accounts of members in any way. The Speaker's office and the House of Commons administration would not in any way be able to say whether the attack on a personal account had been successful.

Could you comment on that?

Mr. Eric Janse: I can confirm that the House administration does not in any way monitor personal emails.

The Chair: You have about 90 seconds, Mr. Genuis.

Mr. Garnett Genuis: Okay.

In terms of the protocols that were in place and that are in place now, there have been multiple cases in which there were threats and members were not informed. Those protocols have changed, if I understand right, such that if this event were to happen today, members would be informed immediately. Can you confirm that? Also, does the directive mean that members would be informed of threats to them that took place prior to the introduction of the new directive and that might still be relevant to them today?

Mr. Eric Janse: I'll give a high-level answer, but I can get into a bit more detail in the in camera portion.

Indeed, there would be quicker communication with members than in the past, but there is still an issue of threshold. As my notes and the Speaker's decision alluded to, there are an awful lot of attacks, unfortunately, on the House. We wouldn't want CSIS to have a satellite office at the House, because giving constant representations to members would be required.

If this were the case today, as opposed to two or three years ago, it would be handled differently.

Mr. Garnett Genuis: I have 15 seconds left.

That still seems fairly unclear. I understand there are a lot of threats. However, if an individual member, because of work they're doing on a foreign policy issue, is specifically targeted by a foreign government—not a generalized threat—it would seem reasonable to me that the member has a right to know, especially when they can take remedial action to protect themselves in both their parliamentary and non-parliamentary accounts.

You're saying it's still not a certainty they would be told.

Mr. Eric Janse: I hate to do this, but we can get into that during the in camera portion. I can give you a more fulsome response.

Mr. Garnett Genuis: I think it's a matter of significant public—

The Chair: Mr. Genuis, I've been courteous with the time.

Colleagues, in the event that you find you're getting to your final 20 or 30 seconds at the beginning of a round, feel free to give the time back to the chair. I'll simply add it to your time later on so you can have more efficiency in the lines of questioning. I certainly don't want to cut off any type of productivity.

Mr. Genuis, thank you very much.

Mrs. Romanado, the floor is yours for six minutes.

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

I'd like to thank the witnesses for being back at PROC.

I have questions that I anticipate you will only be able to answer in the in camera portion, so I will save some of those for then. Once we do a full round, if it's the will of the committee, we might want to start that in camera session a little sooner, rather than asking questions that unfortunately can't be answered in public.

The CSE has provided PROC with a timeline of events that walks us through this situation and provides us with dates for when this came about.

Mr. Dicaire, we understand a parliamentary email account is being monitored, obviously, but what is the protocol right now in the event the House of Commons receives a call from CSIS or CSE saying they have reason to believe a parliamentarian's private email has been targeted? Walk us through what would happen, because there seems to be some information in this chronology that shows, despite multiple contact points with the House of Commons administration, that things were not done, or it took a couple of days before action was taken. If you could walk us through this, it would be helpful.

● (1120)

Mr. Benoit Dicaire: Thank you for the question, Mrs. Romanado.

It doesn't happen often with partners on the cyber front because they understand our mandate when it comes to specific threats regarding the personal identity of members. It's not coming from a lot of instances because usually our interactions with partners are through our mandate specifically. As you know, some of these agencies have specific mandates, and they only interact with us when it matters to Parliament specifically.

We take information from various partnerships. When we speak in the in camera portion, I can allude to this more. Any information coming to the parliamentary cybersecurity team would be triaged and handled. We would look at the level of risk tied to the threat specifically. If it is a physical threat, we would liaise with my colleague the Sergeant-at-Arms. If it is foreign interference or that type of scenario, we would go to our Sergeant-at-Arms specifically.

Most of our relationships, from my perspective, are on the technology side. When it comes to technology elements, we very rarely get an interaction specifically targeting someone. It's mostly targeting infrastructure—these types of scenarios.

In general, that's probably the best answer I can give in public. Maybe Stéphan can add something.

Mr. Stéphan Aubé (Chief Executive Administrator, House of Commons): Through the board in 2014, we modified the acceptable use policy to clearly articulate the process if ever a member's personal information was targeted. With the cybersecurity group, in all cases when a member's information is put at risk, the discussion first happens with the member's office and directly with the member. This is the process that is documented and was approved by the Board of Internal Economy for specific threats to members.

If ever we need to access content—and the content would not be shared from the members to the House administration because we need your authorization to do so—then after that we can escalate this to the House officers. If we feel that the House infrastructure is at risk and we need to protect the institution, we will then get into that discussion.

The document we follow for incidents pertaining to members is the acceptable use policy of 2014.

Mrs. Sherry Romanado: Monsieur Aubé, there was an acceptable use policy in 2014, but these events happened in 2021. If there was already a policy in place that clearly articulated the protocol to follow in the event of a possible non-House of Commons IT cyberattack, as in the case of MP Genuis, why wasn't he contacted? You just mentioned that you need the approval of an MP in order to access that information. How come he was not made aware?

Mr. Stéphan Aubé: Our mandate from an IT security perspective focuses on Parliament and the legislative role of the member. We are not engaged currently in the personal protection of a member's information. In the case of such an event, if I don't have access to the information, I can't follow the protocol. Members whose House infrastructure was affected would have been notified.

● (1125)

Mrs. Sherry Romanado: You just mentioned that you currently are not engaged with IT systems that are outside of the House of Commons. Is that correct?

Mr. Stéphan Aubé: I mean outside of the House of Commons mandate.

Mrs. Sherry Romanado: Thank you.

The Chair: Thank you, Mrs. Romanado.

[*Translation*]

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

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

I'm going to start with a brief introduction because a lot of incidents have occurred in the past few hours. I've written them down in concise form.

In this past month, we've learned that a number of MPs were targeted and that their personal emails were subject to foreign state schemes to extract sensitive information. The objective, one imagines, was to blackmail those members or to use that information for malicious purposes. We know that.

Yesterday we learned that the National Security and Intelligence Committee of Parliamentarians had sounded the alarm. It's quite clear that the government hasn't done enough. So something has to be done about that. It's very important.

My impression—and we can all see this—is that the Prime Minister isn't taking these issues seriously enough. Some MPs are actually benefiting as a result, given that it's even possible to cause foreign interference. I'm shocked to be discovering that today.

In the meantime, we've learned that false documents are now circulating. Documentaries that you're no doubt aware of are circulating, probably in Russian, particularly on the Internet, about the Olympic Games that will soon be held in Europe. European media have online copies. We're talking about fake news and falsehoods, and they're incredibly realistic. One series is even designed to keep people confused. We're a few days away from the European elections, which will involve more than 700 million people. Imagine the impact that will have on those people.

One year later, I'm trying to understand why the members of the Standing Committee on Procedure and House Affairs are here again today to address this interference and are required to take a giant step forward. I don't think we're properly equipped to do that. That's what I notice when I talk to people.

I understand now that parliamentary privilege really embraces everything that's related to our work, in our ridings, in committee and elsewhere.

Now we're talking about personal information being gathered via a Gmail account. We agree that this is a big deal. People are coming to look at our invoices and who we are. They can find out everything. This is an enormous source for gathering personal information. The potential for blackmail could also be enormous.

How is this different from what's happening to the member for Wellington—Halton Hills?

Mr. Michel Bédard (Law Clerk and Parliamentary Counsel, House of Commons): Thank you for your question.

I'm going to cover the parliamentary privilege aspect. Then my colleagues can provide you with more details on the mandate of the House of Commons Administration as it pertains to our IT infrastructure.

With respect to parliamentary privilege, the Speaker of the House of Commons acknowledged the situation in that decision. We're talking about acts of interference and threats made against a member of Parliament related to his parliamentary duties. The Speaker ruled that this constituted a prima facia question of privilege, even though the attack involved the personal email of the member in question.

As you said, there's a potential risk of threats and all kinds of acts of interference, even if the member's personal tools are used. However, in the context of parliamentary duties, the mandate and capacity of the House of Commons administration are limited as to the instruments that may be deployed.

Mr. Aubé, do you have any comments that you would like to add?

Mr. Stéphan Aubé: Thank you, Mr. Bédard.

Considering our capacity to act in this matter, what we can do is protect the institution and ensure that Parliament continues to operate.

The technology infrastructure was established within this framework in order to protect Parliament and to ensure its proper operation.

We do this to support the duties performed by members when they're in their riding offices, travelling or on Parliament Hill and when they interact with their fellow citizens.

As for people's private lives and international relations, however, we can't respond to that type of situation. Other agencies within government are better equipped to do so.

Our mandate is to protect Parliament—

● (1130)

Ms. Marie-Hélène Gaudreau: I apologize for interrupting, but I don't have much time left. I want to say that I'm absolutely reassured about my role as a parliamentarian. I've experienced it.

Who can help us?

You say that there are other possibilities, that other agencies can help you do your work. You have to do it everywhere. We can't say that your work solely concerns my role as a parliamentarian when I'm here. It continues when I'm at home.

Who helps us? Who helps you?

The Chair: You have roughly 20 seconds left to answer that question, Mr. Janse.

Mr. Eric Janse: All right.

I'd say it's teamwork. There's the House of Commons administration, our partner on Parliament Hill, and then there are our partners in the security field, such as our partners in cybersecurity and police services. It's really thanks to our partnerships with all those groups that we can meet all these challenges.

The Chair: Thank you, Ms. Gaudreau.

[*English*]

Ms. Mathyssen, you're online with us today. We'll turn to you for six minutes. The floor is yours.

Ms. Lindsay Mathyssen (London—Fanshawe, NDP): Thank you. I appreciate joining you virtually, as difficult as that sometimes is.

I want to continue with Madame Gaudreau's line of....

I'm concerned, of course. She referenced the news that came out of the report relating to members of Parliament being influenced, and the line between our personal and parliamentary existence and work. I guess you could say that we are very political, partisan actors. I certainly want to ensure that my parliamentary work doesn't interact with my partisan, political work. I keep those separate. Of course, I don't run that partisan work or NDP fundraising activity—whatever you may call it—through my parliamentary email, yet that is being highly impacted by foreign interference. We're seeing this in conversations that have just been released in the media about the Conservative leadership race.

Can you talk about the personal attacks we're receiving and how we're supposed to continue to separate them and ensure we are not bad actors as we try to do both sides of our work in this role?

Mr. Eric Janse: Maybe I'll start. It's a very good question, Ms. Mathyssen, and obviously something the committee will want to reflect on.

As to what's bringing us here today and Mr. Genuis's case, traditionally questions of privilege on parliamentary proceedings are related to the chamber or committee. In this case, it was work Mr. Genuis did with an outside organization but that very much—how can I say this?—influences or assists his work in the chamber or in committee. As a result, in part, that's why the Speaker decided this is a prima facie case and deserves more study.

I don't know if my colleagues want to speak to this.

Pat.

Mr. Patrick McDonell (Sergeant-at-Arms and Corporate Security Officer, House of Commons): If I understand the question correctly, it's that you may be receiving a harassing email on your personal accounts or in your personal life and not on the parliamentary side of things. Is that right, Madame Mathyssen?

Ms. Lindsay Mathyssen: It's more about the separation we have. We are political; we are partisan, and that work has to happen outside of the parliamentary precinct and the controls you have. How do we assist you with that separation, but also in the protection of both sides of our lives?

Mr. Patrick McDonell: My area is responsible for both sides. On the personal side, if you have a security concern, you can come to my office and we will analyze it and reach out to the appropriate security agency, whether it be CSIS, the RCMP or the police force of local jurisdiction. However, we don't have a separation in the Sergeant-at-Arms's office between what's parliamentary and what's personal. Our only concern is the safety and security of members of Parliament.

● (1135)

Ms. Lindsay Mathyssen: The NSICOP report that was just released made reference to members of Parliament who are wittingly or semi-wittingly providing intelligence to foreign governments. If we don't know what's happening on the personal side, how are we supposed to know to communicate with the Sergeant-at-Arms, for example, on those issues and those threats? If we don't perceive them in that way, it gets fairly complicated.

Mr. Patrick McDonell: Yes, and I take your question as being that the communication on your personal side is overt in nature and not covert in nature. Of course when it's covert, it's much more difficult to detect.

Ms. Lindsay Mathyssen: I'm trying to get at the NSICOP report that's been released. How are we supposed to ensure that we are not providing intelligence in the personal space as well? Are you working with institutions like CSIS? Further to that question, have you seen barriers that this committee could deal with to help with the complicated cases that the NSICOP report revealed just this week?

Mr. Patrick McDonell: We have orientation sessions coming up. Public Safety is coordinating with us, and we're bringing in CSIS, CSE and the RCMP to give briefings to the caucuses.

Also, we've stepped up our security awareness area. At the last Board of Internal Economy meeting, we were given more resources so we can do a better job at briefing members of Parliament on current threats and can keep them up to speed on what the current threat environment is.

Ms. Lindsay Mathyssen: A lot of this is entirely on the individual. This is on the MPs themselves to know.

The Chair: Ms. Mathyssen, I'll afford Mr. McDonell a very quick response, but you're out of time.

Ms. Lindsay Mathyssen: I'm sorry. I forgot to push my timer, Mr. Chair.

The Chair: That's not a problem.

Mr. McDonell, do you want to respond very quickly?

Mr. Patrick McDonell: I always think that security is a shared responsibility, and the more we know to serve you with, the better job we can do providing security for members.

The Chair: Thank you very much.

We are now in our second round, so we're down to different periods of time.

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

Mr. Garnett Genuis: Thank you, Chair.

When it comes to protecting the security of our democracy, I'm concerned that this government in particular is trying to pass the buck and avoid responsibility.

House of Commons IT, as I understand it, has a very specific and narrow mandate, which is to protect the IT systems of the House of Commons. Is that correct?

Mr. Eric Janse: Yes.

Mr. Garnett Genuis: We've received unclassified information regarding conversations that happened between the government, government representatives and the House of Commons. They suggest that the government provided information to House of Commons IT of a largely technical nature and said they were aware of these attacks. They gave some information that IT could use in the context of protecting members from those attacks, insofar as they related to the House of Commons IT system. Is that correct?

Mr. Benoit Dicaire: That's correct.

Mr. Garnett Genuis: The government has said, as an excuse for not informing members, that they thought it was up to the House of Commons to do it. It seems to stretch any evaluation of reasonableness to think that the technical information given to House of Commons IT would lead to those IT professionals saying they're going to leave their cubicles, go upstairs and start talking to members of Parliament about these threats. That doesn't seem, to me, to be the job of House of Commons IT professionals. Would you agree with that?

● (1140)

Mr. Benoit Dicaire: We action everything that is sent to us depending on risks and those elements.

I think we can probably provide more information about specific information that we received through this unclassified briefing in the in camera portion, but publicly, I can say that these types of interventions are kind of like piecing a puzzle together. It is not that we specifically provide you with information about the following—

Mr. Garnett Genuis: Well, yes. I guess what I'm trying to get at is who's generally responsible for what because we don't want buck-passing when it comes to security. We want people to take responsibility for the things they're responsible for.

Maybe I'm stereotyping, maybe I'm wrong, but it doesn't seem to me that it's likely the job of IT professionals at the House of Commons, who are given technical information for responding to threats, to take that information and go around the halls saying they need to let members of Parliament know. That seems like a function for security experts in the government to be evaluating, not technical IT folks in the House of Commons.

Am I right about that? I see folks nodding.

Mr. Stéphan Aubé: That is the case, Mr. Genuis. We take the threats that are identified for us. We hunt for them, and then once we've hunted for them, if we find them, we address them. If they're impacting members, we will do that. However, as to the threat actor who's coming to us and their intention, we're not aware of this. We're just dealing with the actual threat.

Mr. Garnett Genuis: Right.

The Government of Canada, in its communications around this, has tried to blame you for its failures to communicate with members of Parliament about threats. It has tried to say that the people with a very narrow and specific mandate around the House of Commons IT system should have taken it upon themselves to assess and measure the threat and to inform members. What you're confirming is that you have a specific mandate for protecting the House of Commons IT system. It doesn't include my personal email, and it also doesn't include broader assessments of security threats and of what is or is not in the public interest to inform members of.

If you're comfortable, answer this question: What is your response to the government's communications that seem to want to direct the blame to you instead of taking responsibility for the decision to not inform members?

Mr. Stéphan Aubé: It would be best to deal with that in camera, sir.

Mr. Garnett Genuis: Okay. You are fully protected with regard to whatever you say before this committee, but I don't want to put you in more of an uncomfortable position than the government already has. I have a great deal of respect for the work done by House of Commons employees, but expecting someone to do something that's not their job isn't fair or reasonable.

As has been said, you're not tracking my personal emails. You're not addressing my security in those kinds of situations, and you're not our security agencies. The House of Commons is not a security agency. It's the government's responsibility to communicate with members about these matters, and it failed to do that.

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

[*Translation*]

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

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

Thanks to the witnesses for being here today to answer committee members' questions.

The purpose of my first question is to understand the situation.

Apart from the members of the Institute of Public Administration of Canada, or IPAC, who were targeted, do you know of any other parliamentarians outside that organization who were also targeted during that period?

Mr. Benoit Dicaire: Just to clarify matters, are you referring to Canadian parliamentarians?

Hon. Mona Fortier: Yes, I'm referring to Canadian parliamentarians.

Mr. Benoit Dicaire: No, no other Canadian parliamentarians were targeted. There's no additional information on the matter apart from what's been mentioned.

However, parliamentarians from other countries were targeted.

Hon. Mona Fortier: Great. Thank you very much.

As a member of Parliament, I'm obviously very concerned about what occurred during that period and what may still be happening.

What should MPs do if they receive a disturbing email?

Mr. Benoit Dicaire: I want to thank the member for her question, Mr. Chair.

That's a good question, Ms. Fortier. Protocols have been established and put in place. I'll focus specifically on those regarding emails since you mentioned them.

We have many services in place, including cybersecurity services, which are accessible 24 hours a day, 7 days a week, and which anyone can call to have a specific email analyzed. We've also organized several awareness campaigns on the subject.

I don't know if you saw it, but you can select the “phishing” icon in the email app when you want to flag a suspicious one.

● (1145)

Hon. Mona Fortier: As you know, this issue was raised a few years ago. Since then, we've received a departmental directive requiring MPs to be immediately informed when a threat is detected.

First, has that directive improved the information flow to the House of Commons? Are MPs now better informed?

Second, do you think the result would have been different if this had occurred after the directive was issued?

Mr. Stéphan Aubé: Mr. Chair, here's the answer that I can give you.

When we're informed of a risk, we do our duty and communicate with the MP.

Most of the time when we're contacted, we have to approach the case as a technical threat, without knowing who's behind the attack against the parliamentarian.

I can't comment on the question as to whether it's an intergovernmental influence risk because that's not the focus of my work. We don't know those things.

Hon. Mona Fortier: Mr. Dicaire, earlier you discussed threat levels and seemed to be talking about a grid.

Would you please explain the reasons why you encourage communication with the member or parliamentarian?

Mr. Benoit Dicaire: The information that's communicated to us is highly technical in every case. In a way, it's an analysis issue where we have to determine whether someone in particular has been targeted or if a group of individuals or a specific infrastructure has been targeted. The intervention level is then determined based on the risk level of the situation.

As Mr. Aubé said, if the information shows that someone is being targeted by a threat that's defined in the policy on acceptable network use, we will directly inform the MP's office of that threat. I could cite you examples of direct actions that the cybersecurity team takes. In one of those cases, one of the members of that team telephoned the MP's office to validate specific aspects of the information that was received.

That's more or less what the protocol associated with that type of situation looks like. We examine the effectiveness of the defence mechanisms. Then, if there's still a residual risk, we inform the MP's office directly.

Hon. Mona Fortier: I'm going to ask a fairly simple question. When a situation requires you to contact an MP's office, do you contact the MP first before reaching that individual's team?

Would you please explain your approach? I think that would help clarify certain aspects regarding the MP's team.

The Chair: You have about 20 seconds to answer the question, Mr. Aubé.

Mr. Stéphan Aubé: Thank you, Mr. Chair.

When a specific MP is attacked, our first reaction is to contact that person. If we're unable to do so, we speak to the MP's chief of staff. If we can't reach the chief of staff, we talk to someone on the team. Then we ask that someone contact the member to have him or her contact us.

We discuss these matters directly with the members. That's our approach.

Hon. Mona Fortier: Thank you.

The Chair: Thank you, everyone.

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

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

I admit I am very concerned about our democracy. A bill is about to be passed. We have to make a major change, and that frightens me.

I'm also concerned that your capacity to act in the performance of your duties is limited. We will be going in camera soon. Since you're the ideal people to propose potential solutions, I'd really like to know what you need in order to prevent this type of situation, to act and to take measures.

That means going so far as to tell us what the role of parliamentarians is when propaganda finds its way into our personal accounts, when even I can't determine what's true and what isn't. When series are designed to influence millions of people who watch them, that's not good. It should set off alarm bells.

I'd like to tell the people watching us that I think it's important that we include all the recommendations you'll be making in our report.

However, I'll have very specific questions to ask in the next few minutes.

Thank you very much, Mr. Chair.

● (1150)

Mr. Eric Janse: I'd like to answer that question briefly.

Ms. Marie-Hélène Gaudreau: Of course. You have the time to do it.

The Chair: The floor is yours, Mr. Janse.

Mr. Eric Janse: I'll give you a more comprehensive answer shortly. Then we can discuss it at greater length.

As the Sergeant-at-Arms has mentioned at two or three previous meetings of the Board of Internal Economy, considerable resources have been approved, especially for the Office of the Sergeant-at-Arms. That also has an impact on other services related to security and cybersecurity.

For the moment, we think we're in good shape. We'll be providing you with specific answers to your questions soon.

Ms. Marie-Hélène Gaudreau: I'd also like to say that what has been put in place to date works very well. I attended a briefing session organized by the Canadian Security Intelligence Service, and the Office of the Sergeant-at-Arms has also provided some support. The warning sign is there; we need to heed it.

Thank you.

The Chair: Thank you, Ms. Gaudreau.

[*English*]

Ms. Mathyssen, it's over to you for two and a half minutes.

Ms. Lindsay Mathyssen: Thank you.

On this question of privilege, we weren't alone in finding out about the hack through the media. Other members of the IPAC—Belgium, New Zealand, Australia and others—found out about that hack, as I understand it, through public reporting as well. Their governments are on different sides throughout the political spectrum. They did not inform their members in a majority of cases.

What are we doing to inform ourselves about or learn from the other investigations and other parliaments studying this issue? How are we moving that into our own studies, and how do we deal with this locally?

Mr. Benoit Dicaire: That is a great question, Ms. Mathyssen. In the in camera portion, I can talk a bit more about our partnerships.

I can definitely state publicly that we have partnerships with other parliaments that were impacted by these types of attacks. Our dialogue is always constant with partners in those parliaments.

Ms. Lindsay Mathyssen: We're seeing, obviously, that there are various levels of understanding of how serious this is. Even in the NSICOP report I referenced before, which has been in the media, there's a different interpretation of the intelligence.

How are you being given the ability, as a non-intelligence-gathering organization, to come to conclusions about the scope of foreign interference? Do you have adequate resources? This is often a conversation we have, even having it within the harassment study. Do you have the appropriate resources you need? Is something required so we can better inform this committee going forward as we report?

Mr. Eric Janse: It's a very good question, Ms. Mathyssen.

For the moment, we feel that we are properly resourced with what the Board of Internal Economy recently accorded us. That could change going forward, but speaking on behalf of my colleagues here, I think for the moment we feel that we have the resources required.

Ms. Lindsay Mathyssen: Is there a discomfort in the interpreting of this intelligence on the part of the House of Commons and security agencies because of your nature of not being an intelligence agency?

Mr. Patrick McDonell: We have an excellent relationship with the security agencies. There's absolutely no discomfort on our part when we deal with our principal partner for intelligence, which would be CSIS.

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

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

Mr. Eric Duncan (Stormont—Dundas—South Glengarry, CPC): Thank you, Mr. Chair.

Thank you to the witnesses for being here this morning.

I have a couple of questions.

I want to recognize that I'm asking this question in a public setting. I want to set the premise that I'm not requesting that you divulge any specific names of members or foreign state actors in your response.

The Speaker ruled that the failure to notify Mr. Genuis and the other MPs targeted in this case amounted to a prima facie question of privilege. The House administration, the government and security agencies were aware of both specific members and a specific threatening foreign state actor, but members were not informed until external revelations came to light, in this case through the FBI and Department of Justice in the U.S. Mr. Genuis rightly raised the point of who has the responsibility to speak to members about this.

That aside, I want to ask each of you a yes-or-no question, for reasons of not divulging anything from a security perspective or anything under review.

Are any of you aware of any other past or current cases in which you, in your respective roles, were informed by the CSE, CSIS, the FBI, any security agency or anyone in the federal government that an identifiable foreign actor targeted or is targeting an MP or group of MPs, but the individuals being targeted have not been informed of that threat? If you know about a specific member or members and a specific foreign state actor, are you aware of any outstanding notifications that have not been sent to members yet?

● (1155)

Mr. Benoit Dicaire: I can answer from a cyber perspective. No, we aren't.

Go ahead, Pat.

Mr. Patrick McDonell: It would be no, sir.

Mr. Eric Duncan: There are no outstanding claims that you're aware of.

In this case, you were aware of members being targeted and aware through security agencies who the specific.... There are no other outstanding cases that three months down the road we're going to hear about through a whistle-blower or in a media report that says x, y and z happened. There's nothing outstanding about members not being notified that you're aware of.

Mr. Patrick McDonell: Anytime our principal partner for intelligence contacts us and provides us information in regard to a member of Parliament, we put it in immediate contact with that member of Parliament.

Mr. Eric Duncan: Mr. Janse, I want to ask you a question.

The committee adopted a document production order directed to the government and the House administration. The order permits government departments to make redactions consistent with the Access to Information Act. Since the House of Commons is not a government department nor subject to the Access to Information Act, given your role, can you confirm that the House administration will be providing us with the unredacted documents in response to this order?

Mr. Eric Janse: That's certainly our intent.

Michel, did you want to add anything?

Mr. Michel Bédard: We received the production order from this committee. The way we read the order is that the House administration is considered a department, so we are to apply the principles that were set out in the order respecting redactions. If the committee wants to provide further clarification on the production order, we'd be happy to implement the production order as adopted by the committee.

Mr. Eric Duncan: In the way you read it, you're a department, but the House of Commons, as we read it, is not a department and is not an agency, so it would not be encompassed within the directive of this committee.

Mr. Michel Bédard: Sir, respectfully, when committees adopt production orders, we have to interpret them. When we read the order, the way it was written.... It's not unusual in an act of Parliament that the House of Commons is deemed to be a department for a very specific purpose, but in general and because of the separation of powers, very clearly the House of Commons is not a department. How we read the production order is that we were assimilated into a department for the purpose of the order, so we were to suggest redactions to the committee.

The production order refers to acts of Parliament. That's not clear, because it refers to the "Access to Information and Privacy Act". Those are two separate acts. When dealing with production orders, we always have to interpret them when there's ambiguity. If there's any need for you to consult the administration and our office when drafting such a production order, we'll be happy to assist to make sure the intention of the committee is reflected in the order.

The Chair: Mr. Duncan, I'm afraid that's all the time allotted to you in this round.

Mr. Collins, I have you for the final five minutes before we suspend briefly.

It's over to you, Mr. Collins, for five minutes.

Mr. Chad Collins (Hamilton East—Stoney Creek, Lib.): Thanks, Mr. Chair.

Let me start with what the threshold is when we understand that a member has been attacked in any shape or form. We read in the report that these instances happen quite often, probably on a daily basis, with actors who are seeking to undermine our efforts in moving our business forward.

What is the threshold from the "team"? I heard the word "teamwork" today. What's the threshold from the team as it relates to notifying members? What's considered a minor threat? What's considered a threat that raises a red flag internally for you to say that a member needs to be informed?

● (1200)

Mr. Benoit Dicaire: I can speak briefly about the cyber portion, and then my colleague can probably speak about the risk around physical threats.

Anything touching members' data, members' information, is deemed to be critical, so we see if there is anything around those parameters. Sometimes it's about targeting digital identities instead of infrastructure, a service or an application specifically. If there's anything around a member's data, we would contact the member's office directly.

Other categories boil down to the risk factor or residual risk. Are protection mechanisms in place and able to protect the infrastructure to ensure the continuity of operations? That lessens the risk in our ability to protect ourselves, but should something be of risk, residual risk, then we would contact the member's office.

Mr. Chad Collins: Did the 2014 protocol that was referenced earlier meet the threshold?

Mr. Stéphan Aubé: I would prefer to deal with that in camera, sir. I need to talk about the incidents to give that answer.

Mr. Chad Collins: Okay, fair enough.

This is a large organization, and someone in one of their answers referenced teamwork. Of course, the report references all the areas that are involved when there's a sharing of information. There's a lot of collaboration and a lot of hands on the steering wheel at that point. For us, I think it's important to understand who's driving.

Can you talk about the hierarchy of shared responsibilities that all areas have? Can you talk about the relationships you have? When one area asks for information from another and it's not provided, who steps in to sort those things out?

Mr. Eric Janse: That's a very interesting question, Mr. Collins. It is absolutely a collaboration. I don't know if there's a hierarchy per se, but it's a collaboration with different groups that have specific mandates. I think it's a question of sharing information and then often collectively deciding what should be the actions and what should be done as a result thereof.

Mr. Chad Collins: In terms of the collaboration that occurred, we've read that in some instances information was asked for and either there were delays or the information wasn't shared. In those instances, who steps in to resolve that? I don't want to call them conflicts, but something has broken down in the collaboration you've talked about. What happens in those instances? Who within the hierarchy—because there is a hierarchy within the organization—is responsible for sorting out that kind of issue when the collaboration or communication breaks down?

Mr. Benoit Dicaire: I think collaboration is really strong in the partnerships. I can attest to that. We have protocols in place associated with the sharing of information. As Stéphan referenced when it comes to sharing members' data, we are not doing that explicitly without your consent. Sometimes there are requests to share data that require consent. At that particular time, we don't necessarily share it unless there's a risk associated with it and consent is given by the member's office.

It also depends on the type of activity. We talked about the threat landscape earlier. A lot of investigation work needs to happen, and it's about piecing the puzzle together. Sometimes the relevancy of the information is not clear at the time of the request, so we have to clarify with the information we have at the time.

Mr. Chad Collins: I'm not necessarily talking about—

The Chair: Mr. Collins, there are just a couple of seconds left. If you want to get a quick final question in, I'll permit it.

Mr. Chad Collins: Sure.

I think the issue is internally—not with the member—when information is asked for. Let's say CSE asks House of Commons IT security staff for information and it doesn't come. Someone has asked for that information for a reason. They're trying to get to the bottom of things, so to speak.

Can we find out in camera or in our open session why that information wasn't shared by someone?

● (1205)

The Chair: Please be very concise.

Mr. Benoit Dicaire: We'll do this in camera, sir.

The Chair: That is nice and concise. Thank you.

Colleagues, we will suspend for a couple of moments and then go in camera.

Just as a friendly reminder, when we go in camera, only authorized staff, members and witnesses can be present in the room. I'll have a couple more brief things to say about that, but we'll take a very brief pause to set up for our next panel.

Ms. Mathyssen, I believe you will have to sign in with a new link. We'll have the clerk assist you with that.

Colleagues, this was another productive hour. It was meaningful, informative and efficient. Thank you for your co-operation. We'll see you back in a couple of minutes.

[*Proceedings continue in camera*]