HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

44th PARLIAMENT, 1st SESSION

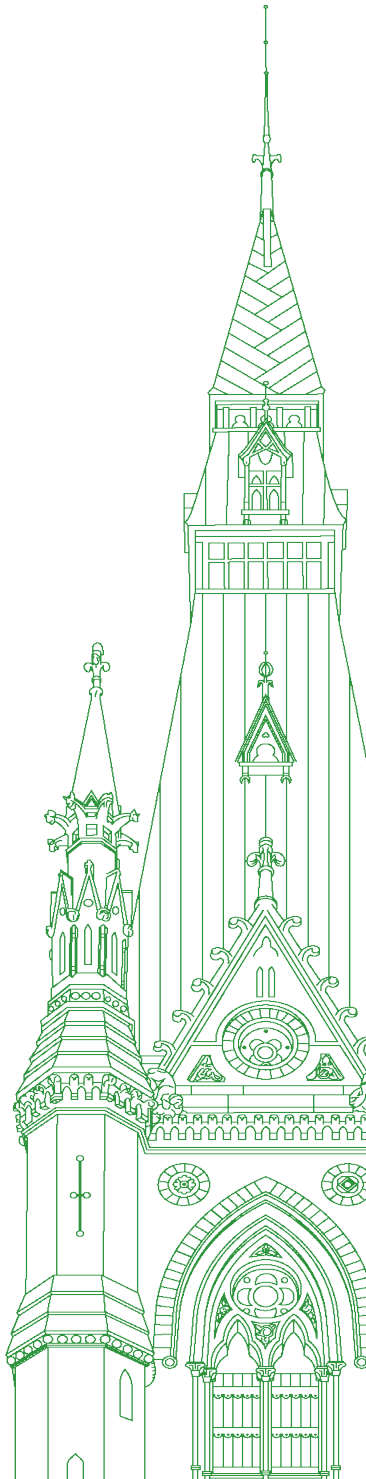
Standing Committee on Procedure and House Affairs

EVIDENCE

NUMBER 119

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Thursday, June 6, 2024



Chair: Mr. Ben Carr

Standing Committee on Procedure and House Affairs

Thursday, June 6, 2024

● (1100)

[*English*]

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

[*Translation*]

I hope the last few days have been pleasant for you.

[*English*]

Colleagues, we are gathered for the 119th meeting of the Standing Committee on Procedure and House Affairs.

[*Translation*]

The committee is meeting again this morning to continue its study of the question of privilege related to cyber-attacks targeting members of Parliament.

[*English*]

Colleagues, I think we are all pretty good now about the rules on audio, but I am going to remind you very briefly every time. Please make sure you place your earpiece to the right of you. If you need more instructions, you have them.

I will also offer a friendly reminder that it is helpful, I think, for the efficiency and productivity of the committee, to have a timer in front of you. If you don't, it's all good. I'll have one, but I think it helps sometimes.

As in the last meeting, I have no issue, colleagues, with rolling over some time. For example, if we're in the first round and there are 30 seconds and you don't feel that you can get a quality question in with 30 seconds, that's okay. Give it back to the chair, and I'll roll it into the next round. It still keeps us in proper time. I think it's fair and more productive, instead of having to rush through things, to just roll it over. That offer always exists.

We are joined today for the full two hours—the first will be in session, so public, and the second will be in camera—by the senior leadership of the Communications Security Establishment.

I would like to welcome Caroline Xavier, chief, CSE, as well as Rajiv Gupta, associate head, Canadian Centre for Cyber Security.

Welcome, both of you.

You will have 10 minutes collectively to provide opening remarks. Please ensure your questions and your remarks are through the chair.

With that, I will turn it over to you.

Ms. Caroline Xavier (Chief, Communications Security Establishment): Thank you, Mr. Chair, for the invitation to appear this morning.

My name is Caroline Xavier, as stated. I am the chief of the Communications Security Establishment, also known as CSE. I am joined by Rajiv Gupta, the associate head of CSE's Canadian Centre for Cyber Security, also known as the cyber centre.

I'd like to begin by providing the committee with a brief overview of the evolving threat landscape. Following this, I will speak to the mitigated threat activity that targeted Canadian parliamentarians and how CSE has been working and continues to work to support parliamentarians and protect our democratic institutions more broadly.

[*Translation*]

Canada's adversaries are increasingly using cyber-threats to conduct espionage, move their foreign policy objectives forward and influence Canadian public opinion to their advantage.

Although we believe cybercrime continues to be the most likely cyber-threat affecting Canadians and Canadian organizations, the cyber-threat coming mainly from China—as well as from Russia, Iran and other countries—is more strategically significant.

[*English*]

Allow me to be more specific. The cyber-threat emanating from the PRC is significant in its volume and sophistication. PRC-sponsored cyber-threat actors will almost certainly continue targeting industries and technologies in Canada to give the PRC an advantage for its strategic priorities, whether political, economic, in security or in defence.

In parallel, Russia's invasion of Ukraine in February 2022 gave the world a new understanding of how cyber-activity is used to support wartime operations. It has demonstrated how nation states are increasingly willing and able to use misinformation and disinformation to advance their geopolitical interests.

Since 2021, the CSE has also observed that state-sponsored cyber-threat actors with links to Russia and the PRC continue to conduct most of the attributed cyber-threat activities targeting foreign elections. In the fourth iteration of our threats to democratic processes publication, released in December 2023, we outlined examples of cyber-activity against the democratic process that we have observed globally since 2021. These include distributed denial of service attacks, or DDoS, against election authority websites and electronic voting systems, unauthorized access to voter databases to collect private information, and spear phishing attacks against election officials and politicians, among others.

Given this observed activity, in the last few years, the CSE cyber centre has publicly released over eight alerts, four cyber-threat bulletins, and seven joint cybersecurity advisories with allies, all related to Chinese or Russian state-sponsored cyber-activity.

Canada's high degree of global connectivity and technological integration with our allies increases our threat exposure. Furthermore, Canada does not exist in a vacuum, so cyber-activity affecting our allies' democratic processes will also likely have an impact on Canada's.

In relation to the committee's study, I'd now like to provide a brief overview of the CSE's role and relationship with the House of Commons IT team.

The CSE takes its mandate and legal obligations very seriously. Under the cybersecurity and information assurance aspect of our mandate, the CSE acquires, uses and analyzes information from the global information infrastructure, or from other sources, to provide advice, intelligence, guidance and services to help protect electronic information and information infrastructure. Accordingly, pursuant to the CSE Act, the CSE and its cyber centre share intelligence and information with service providers and government clients, including appropriate authorities in Parliament.

In June 2022, the CSE received a report from the FBI, detailing emails targeting individuals around the world, including individuals who have been outspoken on topics relating to activities of the Chinese Community Party. The report included technical details and the names of 19 parliamentarians who had been targeted by this activity. However, from January to April 2021, more than a year earlier, the cyber centre had already shared reports with the House of Commons IT security officials, specifically detailing a serious matter of technical indicators of compromise by a sophisticated actor affecting House of Commons IT systems.

Upon receipt of this information, the CSE shared specific and actionable technical information about the activity with the House of Commons IT security officials, as well as with the Canadian Security Intelligence Service, or CSIS. Because of this information, the CSE and the House of Commons worked together to thwart the attempted compromise by this sophisticated actor.

● (1105)

[*Translation*]

We respect the fact that the House of Commons and the Senate are independent, and its representatives are responsible for determining the timing and the manner in which to communicate directly with MPs and senators. Last week, the committee's clerk received a complete chronology of events describing measures the Communications Security Establishment took to inform and assist parliamentary officials in their efforts to detect and mitigate cyber-threats. It is important to highlight that the Communications Security Establishment's engagement with House of Commons IT security stakeholders came well before the aforementioned Federal Bureau of Investigation report.

[*English*]

As the central technical resource for cybersecurity advice, we provide near real-time notifications, including to the House of Commons and Senate IT teams, and we have helped parliamentary IT security officials take quick and appropriate measures within their systems to protect their network and users against this and other threats.

When a cyber-threat is identified, the cyber centre sends out different types of notifications, including cyber flashes, which are urgent notifications delivered via email, daily updates about malware and vulnerabilities on a partner's IP space via the national cyber-threat notification service, and monthly summaries of national threat notification service data, showing how a subscriber's cyber hygiene ranks against anonymized peers in their sector.

When requested, we provide cyber-defence services and maintain an open line of communication to mitigate potential threats. To detect malicious cyber-activity on government networks, systems and cloud infrastructure, the cyber centre uses autonomous sensors, including network-based sensors—

● (1110)

[*Translation*]

Ms. Marie-Hélène Gaudreau (Laurentides—Labelle, BQ): I raise a point of order, Mr. Chair.

I am truly sorry to interrupt the witness. However, I missed a great deal of information, because the pace is too fast for the interpreter, whom I thank, to keep up. I've been thinking for two minutes that—

The Chair: Very well, that's fine. I will stop the timer for a moment.

[*English*]

Ms. Xavier, could you try to slow down your speech just a bit? I think we're having a gap in the translation, which is making it a little more difficult for some members to hear.

I've paused the time. You have about three and a half minutes remaining. If you could do your best, that would be great.

Go ahead, Mr. Genuis.

[*Translation*]

Mr. Garnett Genuis (Sherwood Park—Fort Saskatchewan, CPC): When my colleague was speaking French, the English interpretation wasn't working.

The Chair: I think it's working now.

[*English*]

Colleagues, we'll give this another go.

[*Translation*]

If there are still problems with the interpretation, please let me know and we will pause momentarily again to solve it.

[*English*]

Ms. Xavier, there are three and a half minutes remaining.

[*Translation*]

Ms. Caroline Xavier: Okay. I apologize for the interruption.

[*English*]

When requested, we provide cyber-defence services and maintain an open line of communication to mitigate potential threats.

To detect malicious cyber-activity on government networks, systems and cloud infrastructure, the cyber centre uses autonomous sensors, including network-based sensors, cloud-based sensors and host-based sensors. These defences protect systems of importance from an average of 6.6 billion attempted malicious actions per day.

CSC continues to monitor Government of Canada networks and systems of importance for cyber-threats. We are working in close coordination with government partners, including relevant security agencies.

We deliver foreign intelligence-informed cyber-defence.

[*Translation*]

Finally, I would like to call members' attention to the solutions available to them. Indeed, the Canadian Centre for Cyber Security offers parliamentarians a support service, in addition to holding regular information sessions for political parties on cyber-threats, as well as providing a dedicated point of contact at the centre for accessing cybersecurity support.

[*English*]

Since 2017, the CSE has established four unclassified reports on cyber-threats to Canada's democratic processes, and our "National Cyber Threat Assessment 2023-2024" highlights how online foreign influence activities have become a new normal, with adversaries seeking to influence elections and impact international discourse related to current events.

Since 2014, interdepartmentally, the CSE's cyber centre has worked closely with Elections Canada to ensure that our election systems and infrastructure remain secure. The CSE also continues to work as part of the security and intelligence threats to elections task force, SITE. Cyber-incidents such as ransomware, DDoS and supply chain compromises are becoming more frequent across all industry sectors, and these incidents are negatively impacting our prosperity, privacy and security. That's why Bill C-26 is so important. It would give the government new tools and authorities to better bolster defences, improve security across critical federally regulated industry sectors, and protect Canadians and Canada's critical infrastructure from cyber-threats.

Four sectors are subject to the mandatory cyber-incident reporting in Bill C-26: finance, energy, telecommunications and transportation. These were all prioritized due to their importance to both Canadians and other sectors. They are critical enablers. Bill C-26 will improve our ability to protect ourselves from both the threats we observe today and the threats we will face tomorrow.

The federal government intends to launch its updated national cybersecurity strategy, which will communicate Canada's long-term approach to addressing evolving threats in cyberspace. Central to the new strategy will be a shift in focus towards a whole-of-society approach to Canada's national cyber resilience, where public and private entities and all levels of government work in close partnership to defend against cyber-threats, including threats to our institutions. The government also recently announced the defence policy update, "Our North, Strong and Free", which proposes a significant new investment in the CSE through budget 2024.

Finally, an important aspect of Canada's whole-of-society approach to our collective security includes practising good cyber hygiene, including safe social media practices, especially in those public roles. The cyber centre has released guidance on ways to protect yourself online. It also has cybersecurity resources for elections authorities, political campaigns and Canadian voters. I really encourage you to take a look at our website, getcybersafe.gc.ca. I would also encourage organizations that have been impacted by cyber-threats to contact the cyber centre, so that it can help share threat-related information with partners to help keep Canada and Canadians safe online.

Further, to make cyber-incident reporting easier for Canadians, the CSE is also working with its federal partners to establish a single-window solution for reporting cyber-incidents, with the ultimate goal being to ensure that Canadians can always find the help they need. This was a key recommendation this week from the Auditor General.

To conclude, the CSE and the cyber centre remain active in their collaboration with all partners, including the House of Commons, to improve Canada's cyber-resilience and protect our democratic institutions. We will continue to monitor any developing cyber-threats and share threat information with our partners and stakeholders, as always.

● (1115)

[*Translation*]

Once again, thank you for your invitation to appear before you today. We are pleased to be able to contribute to this important discussion and give you an overview of the way the Communications Security Establishment and the Canadian Centre for Cyber Security both work every day to protect Canadians and their democratic institutions.

Thank you for your attention.

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

[*English*]

Mr. Genuis, you will start us off for six minutes in our first round.

The floor is yours.

Mr. Garnett Genuis: Thank you, Mr. Chair.

Can you confirm that the government informed the House of Commons administration about the cyber-attack?

Ms. Caroline Xavier: I can confirm that when we became aware in 2021 of some anomalies that we were seeing with regard to potential cyber-activities towards the House of Commons, we did, indeed, inform the House of Commons IT security team.

Mr. Garnett Genuis: Thank you.

Can you confirm that you told them which parliamentarians were targeted?

Ms. Caroline Xavier: What I can say is that when we were informed in June 2022 by the FBI of all of what we were informed by them about, the list of parliamentarians, we did, indeed, share that list of parliamentarians with the House of Commons IT security team. We also shared it with CSIS.

Mr. Garnett Genuis: Thank you.

Did you inform the House of Commons administration, similarly, about the source of the attack?

Ms. Caroline Xavier: As mentioned in the chronology that was provided to the clerk, we made it clear that, since January 2021, we've been seeing a sophisticated actor doing cyber-activities towards the House of Commos. We provided 12 reports to the House of Commons. We also held meetings with the House of Commons and CSIS. As part of those various activities—the meetings and reports we provided—we were able to share information that was going to be important in order to continue to mitigate the threat.

Mr. Garnett Genuis: Thank you, ma'am, but I'll repeat the question, because you didn't answer it. The question was quite specific.

Did you inform House of Commons administration specifically about the source of the attack?

Ms. Caroline Xavier: Whenever we have a cyber-incident, we work immediately to focus on mitigating the threat. Once we are continuing to address the threat, we, from a CSE perspective, work hard to try to better understand where the threat originated. As we continue to learn that information, we share it with service providers and those who need to know, especially if it's going to be helpful to continue to mitigate the threat.

Mr. Garnett Genuis: That wasn't a general question. It was a specific question about what you did in this case.

Did you inform House of Commons administration about the source of the attack?

Ms. Caroline Xavier: As part of the various meetings and reports we provided, we were able to share with the House of Commons IT security staff what we believed at that time to be the originating source of the threat.

Mr. Garnett Genuis: Okay. That was a long way of saying yes, if I understood your response correctly.

According to your testimony today, you shared, with House of Commons administration, the source of the attack—this being APT31.

Ms. Caroline Xavier: I believe it would be more appropriate to discuss some elements of the threat during the in camera portion of the meeting.

Mr. Garnett Genuis: I just repeated what you said in your previous response, to clarify it. We shouldn't need to shift in camera for you to confirm that what you said a minute ago was correct.

Did you in fact tell us a minute ago that you informed House of Commons administration that APT31 was the source of the attack? Is that what you said earlier, or did I misunderstand?

● (1120)

Ms. Caroline Xavier: What I shared was that, when we know the originating source, or when we have a general understanding of the original source, we share that information with service providers and those who need to know. As part of that, we shared over 12 reports with the House of Commons IT staff and held several meetings.

As part of those meetings, we were able to share information linked to the originating element.

Mr. Garnett Genuis: I don't know what you're trying to say to us, ma'am. I don't think it's a complicated question. It's a clear and specific question. People are going to draw conclusions if there's prevarication here.

The question is this: Did you or did you not, at some point, in a meeting, say clearly to House of Commons administration that the source of this attack was APT31?

Ms. Caroline Xavier: As I said, as part of the many meetings we held and the reports we provided to the House of Commons, we provided what was at that time believed to be the originating source.

We now know—because it is 2024 and we have much more information and collective knowledge—that this was an actor by the name of APT31.

Mr. Garnett Genuis: Okay. Did you at any point inform House of Commons administration that it was APT31, and at what point was that?

Ms. Caroline Xavier: From January 2021 all the way until.... I forget the exact date, because I don't have the chronology in front of me, but it was almost a year in advance of the time in 2022 when we got the FBI report. We were aware that APT31 was of concern for us from January 2021. As part of the conversations we had with the House of Commons, the presentations we made to them and the reports we shared, we identified APT31 as, potentially, the actor at that time.

Mr. Garnett Genuis: Okay. You're telling us now, at the end of this round, that you did inform the House that it was APT31. It's just yes or no.

The Chair: Please answer in about five seconds.

Ms. Caroline Xavier: I think, Mr. Chair, that I've answered the question.

Mr. Garnett Genuis: It's a yes, then, or is it a no?

The Chair: Unfortunately, Mr. Genuis, that is time.

[*Translation*]

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

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

Ms. Xavier and Mr. Gupta, thank you for being here and helping us shed light on this issue.

I will continue along the same lines. I'd like to know when you discovered ATP 31, or advanced persistent threat, was an issue.

Ms. Caroline Xavier: Thank you very much for the question.

As I said before, since the start of January 2021, we observed anomalies, troubling cyber-activities. We then contacted the House of Commons cybersecurity analysts to advise them of our concerns on a technical level. As we gained understanding of what was happening, we submitted 12 reports to them, met with them and also met with our colleagues from the Canadian Security Intelligence Service, or CSIS. We participated in conversations and advised the House of Commons that a nation-state actor was involved, and that it was in fact ATP 31.

Hon. Mona Fortier: Did it happen at that time or later? That's what I'm trying to understand.

Ms. Caroline Xavier: It happened between January 22, 2021, and—

Hon. Mona Fortier: It was done with the House of Commons, correct?

Ms. Caroline Xavier: Yes, that's right.

Hon. Mona Fortier: You talked about the fact that you had meetings and shared information. Is that what you do when you notice something, a specific situation, activity from a group? What type of information do you send to the House of Commons when you detect a threat?

Ms. Caroline Xavier: We send a great deal of information, as much as we can, especially when it is not classified. Sometimes, we declassify information if sending it is useful.

I will ask Mr. Gupta, who was present during some of those conversations, to shed a bit more light on the type of information we send.

● (1125)

Mr. Rajiv Gupta (Associate Head, Canadian Centre for Cyber Security, Communications Security Establishment): Thank you, Mr. Chair.

[*English*]

When you have classified intelligence reporting, there's a lot of context and information, and then there's often a tear line, so there is another set of information that you can provide to an incident responder or to another organization to enable it to take immediate action in resolving an incident. In the lead-up to the incident, we would be sharing tear-line information: "Here is a sophisticated threat actor," which, in cybersecurity terms, typically means a nation-state and is super important. It definitely reinforces the seriousness and the importance of the event.

However, all we're allowed to share, because of the intelligence, are the technical indicators. We didn't have the email addresses, so we would share the things that would be needed to find the email addresses. That's what we shared with the House of Commons, and we worked with the House of Commons collaboratively to figure out exactly what was going on, because typically you have a thread you need to pull.

Hon. Mona Fortier: If it's through working with the House of Commons that you're trying to find out what's happening, then whose role is it? Does the House of Commons need to come back to you and say, "Here's what we found?", or do you have to tell them, "Let's find something?" How is that relationship?

Mr. Rajiv Gupta: We started the thread-pulling by saying, "Hey, this is what we know. You can go find your emails." We didn't have the emails. We had the thing to look for the emails with. They would go and look for that. That's what they did, and then they came back with that information. Every time we found something new, they understood the scope of the incident. That's how we work collaboratively with the House of Commons, and we've worked collaboratively with the House of Commons for a decade or more.

[*Translation*]

Hon. Mona Fortier: During this incident's time frame, you had regular contact. The chronology of events you provided to committee members shows that, on February 18, 2021, a decision was made for CSIS to work with the House. The Canadian Centre for Cyber Security's cyber security events management team provided CSIS with a list of technical questions to help it analyze suspicious activity.

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

Ms. Caroline Xavier: Thank you very much for the question.

We take our role very seriously. For us, it's important not to keep Canadians' private information with CSE data, because our role plays out on the international stage. When we understand that the origin of the threat to Canada is coming from abroad, it's very natural for us to pass the torch to CSIS, because it has the mandate to act within Canada. We therefore take very seriously the fact that we do not intervene, and we are careful not to manage personal information. The reason why we passed the torch to CSIS in that situation was because the incident had to be managed here, in Canada.

Hon. Mona Fortier: Does the Communications Security Establishment know whether a follow-up was done with parliamentarians to make sure they had been warned, that they understood the measures to take and that their questions regarding the threat itself were answered?

Ms. Caroline Xavier: As my colleague Mr. Gupta said, when we manage an incident involving an institution, we maintain a continuous relationship in order to better understand the threat. It also provides us with information.

With the exception of the House of Commons, an institution could manage everything internally and inform us of the incident only after it is resolved. It's also possible that it will not inform us at all.

The Chair: Thank you, Ms. Fortier.

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

Ms. Marie-Hélène Gaudreau: I did not hear your opening remarks correctly, so I may ask some questions.

If we come back to the beginning, the Communications Security Establishment's mandate involves protecting digital infrastructure. Your clients include the government, public administration, National Defence and some of the companies you mentioned. Is that right?

Ms. Caroline Xavier: Thank you for your question.

Yes, our mandate involves protecting Canada's government systems and critical infrastructure, but we also have an international mandate. Even if our mandate does not involve protecting individuals directly, you will find information on our website about ways to improve individual cyber-hygiene.

Our first mandate is to protect Canada and Canadians, especially government systems, industry, critical infrastructure and government communication sectors, among others.

● (1130)

Ms. Marie-Hélène Gaudreau: I see. Given that we are going through a rather significant shift, MPs are becoming key players. Are they on the list of people to whom you offer services?

Ms. Caroline Xavier: Yes, they are. Since 2019, we've offered parliamentarians the opportunity to get support from the Canadian Centre for Cyber Security, especially if they've had problems after a cybersecurity incident. That is also part of the services we offer, but it is important for parliamentarians to contact us if they want our help.

Ms. Marie-Hélène Gaudreau: Could you explain to me what these services include?

Ms. Caroline Xavier: As I said before, we are very careful not to collect Canadians' information. That means when Canadians or parliamentarians contact the Canadian Centre for Cyber Security for support, it is very important for everything to go well, so that we can offer the support required for managing an incident without going into their private lives.

Ms. Marie-Hélène Gaudreau: When it comes to disclosed information, do you think the House of Commons administration has enough details to be able to engage directly with the members involved?

Ms. Caroline Xavier: I do not want to answer for the House of Commons administration, so it would be better to ask them the question directly.

That said, as Mr. Gupta noted, we have a very good relationship with the House of Commons administration. We've worked with them since 2012, and the relationship is constantly improving. In 2016, we implemented a memorandum of understanding to properly maintain this relationship.

Ms. Marie-Hélène Gaudreau: People from House Administration came to talk to us about advanced persistent threats, or ATPs. From what I gathered, the information disclosed was insufficient. I pictured a situation in which information was provided, but it's like finding a needle in a haystack.

My understanding is that the protocol and information pertaining to ATP 31 had evolved significantly. Can you provide me with a more in-depth explanation of the matter?

Ms. Caroline Xavier: I will ask Mr. Gupta to answer you, because as I said, he was very involved at the time, in 2021. I think he may be able to give you a better answer.

[*English*]

Mr. Rajiv Gupta: I think, to be able to understand the implications, as I mentioned, we shared a series of reports over the first few weeks that would help us pull the thread and understand what was going on. This was in 2021. This was pre-vaccine COVID, so it was very difficult to get people into rooms. We were working, but not necessarily everyone was in the office, so we booked a classified meeting to make sure that the full implications were met. We can talk about that maybe in the in camera session, but that's how we go about it. We share the information we can, and then we try to book classified meetings to make sure that all the full context is well understood.

[*Translation*]

Ms. Marie-Hélène Gaudreau: Very well.

Regarding the Federal Bureau of Investigation's report in June 2022, I have a very simple question for you: Do you have enough human resources and technical capacity? Things are moving fast, and you described to what extent strategies and strategists can differ significantly. Do we have what we need?

Ms. Caroline Xavier: Thank you for the question.

I'm very proud of our organization. We have extraordinary people who work very hard for Canadians. The additional funds included in the 2022 budget helped us move our cybersecurity activities forward and fulfill our mandate. The additional funds proposed in the 2024 budget would give us additional resources to do our work for Canadians. For us, that's a vote of confidence from the government regarding our ability, and we are very proud of it. We are committed to meeting the demand.

● (1135)

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

The Chair: Thank you, Ms. Gaudreau.

[*English*]

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

Ms. Lindsay Mathyssen (London—Fanshawe, NDP): Thank you, Mr. Chair.

Thank you to the witnesses. I appreciate your being here with us today.

This may be a bit of a repetition, but just so it's clear in my own mind too, you talked about the first communications with the House of Commons when you found out about the attacks in January 2021. Our concern, of course, is that there was a significant amount of time—and I certainly understand, in terms of the conversations that have been had, that you learned more as time went on, and you were reporting that. That's great. I think the key point here, though, is that at whatever point, none of this was reported to the individual MPs in question. This is what we have to investigate. We have to determine if this is the problem.

Could you go over again, for my own sake, why it's so important that there is almost that divide that occurs? There's this space where you're not directly communicating with the members once it's determined that there is this sophisticated actor, as you've labelled them. Why is that intermediary position so important? Why couldn't there have been maybe a joint communication with the members of Parliament who were impacted? Are you maybe looking at the advantages or disadvantages of that? This is constantly a learning process. I understand that as well. How will things maybe change in the future? Are you considering how we can move forward from this?

Ms. Caroline Xavier: Thank you very much for the question.

One thing that's worth mentioning here is that we work really hard to try to ensure we inform Canadians and businesses as much as possible with the various publications that we put out. As mentioned, since 2017 we've put out three updates on "Cyber Threats To Canada's Democratic Process" and, in addition to that, four editions of the "National Cyber Threat Assessment". Those are documents that help highlight some of the threats we're seeing and observing based on a whole bunch of research as well as the observations that have occurred in Canadian systems as well.

With that, one thing we also do is that we actually hold quite a number of information sessions, and we've held some with parliamentarians, supported by others like the service and the RCMP. We're very happy to be able to do joint information sessions with whoever would like us to be present, to educate them on the cybersecurity domain in particular, because the more people are aware of what the threats are, the more resilient we become as a country and as individuals.

The issue, though, is that we really are respectful of the independence of the House of Commons and the Senate, and we're really respectful of the role that the House of Commons administration plays in supporting parliamentarians. This is why we go through them, as we do for many service providers and other institutions that we deal with. We go through them, and we're at their service if they would like to have more support from us. We would be more than happy to continue to hold sessions with parliamentarians should the House of Commons administration want our assistance to do a joint session. We're definitely available to do that.

As a matter of fact, the public safety department has been in touch with the Sergeant-at-Arms, and there are three sessions currently scheduled for caucus that we'll be part of, for example, with Public Safety as well as the RCMP and the service. This is to show you that these are services that we are prepared to do, but we are just trying to continue to be very respectful of the processes that are in place and, more importantly, the independence of the House of Commons in this role.

Ms. Lindsay Mathyssen: I certainly appreciate that. Our caucus is getting a briefing, I think, next week. However, that's more of.... These info sessions are very general, and it's very different from when individual MPs themselves are targeted. Again, is there a shift in terms of...? I understand absolutely that the independence of Parliament is key, but that's actually what we're talking about here in terms of the threat or this potential breach of privilege that has been the concern of these studies and this meeting. That's what's at stake here as well.

To make it more specific, is there an idea that we've learned from this and said it was a problem? Clearly, the people involved were not told in the way that they needed to be. Are changes being made to ensure that breach of privilege potentially is not a future issue?

● (1140)

Ms. Caroline Xavier: Thank you very much for the question and the clarification.

We are an organization that considers itself very much a learning organization, so we continue to look for ways to improve. This is part of that learning, to be able to see where we can improve our processes, in addition to all the external review bodies and various reports that are going on with regard to other issues, like foreign interference.

We will continue to learn from this to improve those processes and work with the House of Commons to identify a better way forward.

In general, though, when it comes to identifying an individual who may be impacted by a cyber-incident because we learned of it from a foreign source, we pass on that information in general to the service, as I mentioned earlier, for the reason that then it becomes a domestic issue and is not within our wheelhouse. It is also not the way in which we function with respect to our act. Sometimes the RCMP will be engaged, especially if it's going to be something that requires a law enforcement lens. In this case, we did pass it on to the House of Commons as well as to CSIS, so that they could pass on the information to the necessary MPs.

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

Okay, folks. We are entering our second round.

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

Mr. Garnett Genuis: Thank you, Chair.

I have to start by saying, in response to the round of questions with Ms. Mathyssen, that I find it laughably ridiculous to say that the government institution has so much respect for parliamentarians that they kept secrets from those parliamentarians about their own safety. That's not how you manifest respect in the relationships that I'm a part of—by keeping vital secrets from people.

Ma'am, when Parliament was briefed about aspects of this threat, did you expect the House of Commons IT department to inform members of Parliament about the specific threats?

Ms. Caroline Xavier: Our understanding, or, yes, I guess my expectation would be that if I'm passing on information to a partner, a partner will do what is necessary to address the content of the information that is provided—

Mr. Garnett Genuis: I'm sorry, ma'am. You really prevaricated in my last round. I'm going to push you more, because prevaricating in response to questions is a matter that touches on the privileges of parliamentarians.

It was a very specific question. Did you expect them to brief members of Parliament who were threatened about these threats?

Ms. Caroline Xavier: When we pass information on, the expectation is that it will be of use to others. The expectation would be that, given that we shared a list of names, somebody will act on it, whether it's to CSIS or, in this case, the House of Commons.

Mr. Garnett Genuis: I'm sorry. That's not the question. That's not the question at all. It wasn't about whether you expected them to act on it. The House of Commons IT's job is to protect the IT systems.

Mr. Chad Collins (Hamilton East—Stoney Creek, Lib.): I have a point of order, Mr. Chair. I'm interested in the answers. I don't think the witness has been given full opportunity to provide them—

Mr. Garnett Genuis: Then use your round. Come on. Learn the rules here, Mr. Collins.

I have five minutes. Then you have five minutes.

Mr. Chad Collins: Maybe you could just have some level of decency here in terms of allowing the witness to fully answer a question.

The Chair: Mr. Collins, I hear you on the point of order.

Mr. Genuis, I would ask that when a member is raising a point of order, you allow them to finish.

Mr. Chad Collins: That would be great—some respect.

Mr. Garnett Genuis: You show some respect for the rules. It's my time.

The Chair: I did stop the clock, Mr. Genuis, so that point of order has not caused you a loss of time.

There are three minutes and 10 seconds remaining.

I turn the floor back over to you, Mr. Genuis.

Mr. Garnett Genuis: Thank you, Chair.

If Liberal members aren't interested in drilling down to get to responses, that's on them, and that's evident from this disruption.

To the witness again, it's a very specific question. The specific question is this: Did you expect House of Commons IT to take that information and go and brief parliamentarians who were threatened?

● (1145)

Ms. Caroline Xavier: I'm going to pass on the information and ask if Rajiv would like to answer, given that, as I said, he was present at the time and would have a better understanding of what the expectation was.

Mr. Garnett Genuis: Is that because you don't know? I'm happy to hear from him, but is that because you don't know the answer to the question?

Ms. Caroline Xavier: It's because I wasn't personally present. My expectation is that, yes, if I'm passing some information on to an institution or the House of Commons, they are acting on it, and that they're taking that information and passing it on—

Mr. Garnett Genuis: Do you understand that that's not the question? The question is not whether they were going to act on it. The question is whether they were going to pass that information along to parliamentarians. You can't even tell me if you expected them to pass the information along to parliamentarians. That's the question: Did you expect them to take that information and tell me and others about it?

Ms. Caroline Xavier: When we passed on the information, including the names, when we became aware of the names in June 2022, our expectation was that we gave them the information, as well as actions that could be taken to mitigate it, and they would act on it.

Mr. Garnett Genuis: Again, you're not answering the question. The question is not whether you expect them to act on it. The question is if you expected them to brief parliamentarians. Did you expect them to brief parliamentarians, yes or no?

Ms. Caroline Xavier: If one of the actions was to brief parliamentarians, then the expectation is that, yes, they would have done that.

Mr. Garnett Genuis: Was that one of the actions? Did you suggest to them that they brief parliamentarians? It's yes or no.

Mr. Rajiv Gupta: I was not present at the discussion. However, I have worked with HOC in the past. Expectations are based on—

Mr. Garnett Genuis: It's not about what you did in the past. I'm just looking for a yes-or-no answer to a simple question, and I'm trying to get to it in five minutes. Just because of who you work for, you're not exempt from the requirements to answer questions at parliamentary committees.

This is the question: Did you expect, and did you communicate an expectation to House of Commons officials, that the information would be shared with parliamentarians—yes or no?

Mr. Rajiv Gupta: In working with the HOC, they have stressed from day one over the decade plus that we've worked with them, that the independence of the HOC is super important. They understand their clients.

Mr. Garnett Genuis: Yes or no?

Mr. Rajiv Gupta: We've worked with them many times. My understanding is that, having worked with them in the past on incidents and seeing what has happened, we have discussed this with them, and they have gone and done that job.

Mr. Garnett Genuis: Did you expect them—

Mr. Rajiv Gupta: Based on past evidence, my expectation was that we would have that same discussion, and that based on their understanding of thresholds.... I don't know the threshold for when the HOC's Sergeant-at-Arms will go and actually brief a person—

Mr. Garnett Genuis: Did you communicate an expectation or not?

Mr. Rajiv Gupta: We communicate the threat and the context, so understanding that this is the exact threat—

Mr. Garnett Genuis: So you didn't communicate an expectation.

Mr. Rajiv Gupta: An expectation to go and brief.... We wouldn't tell them to go and brief, as in, “You have to go brief now.” We would tell them, “This is really important, and your members are at risk.” These are the types of things we would say. We don't say, “Go and brief.”

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

That's the end of the five minutes.

The floor will now go to Ms. Romanado for five minutes.

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

We received the chronology of events that you provided us. Thank you very much for that.

Based on the chronology and your testimony today, it appears that the communication between the cyber centre and the House of Commons IT was pretty much almost a one-way dialogue. I'm seeing repeated indications that the House of Commons IT did not provide you with feedback or did not provide the cyber centre with follow-up, despite requests.

Can you confirm that was in fact the case between January 22, when you started to see this activity, and the time that the FBI provided the report?

Is that correct?

Ms. Caroline Xavier: I will ask Rajiv to answer that question.

Mr. Rajiv Gupta: Thank you very much.

From our understanding.... You can see the chronology; the timeline is laid out.

We were reaching out for information. We don't know what happened on the other side in terms of how long it takes to get that information. As I said, it's a collaboration. We've worked well with the HOC in the past and have tons of respect for their folk.

I think that when we did get together to meet, information was shared. There was that sharing of information. You can see on the timeline when that occurred.

Ms. Caroline Xavier: I would add that it's not abnormal in any cyber-incident that we deal with, especially with critical information or a private sector company, that the information is perceived as one way, because they are managing their issue. They're living it. It's not abnormal for them to take the time they need to eventually get back to us or possibly not tell us. This is how that sometimes happens.

Mr. Rajiv Gupta: One item I'd like to add is that this was a very sophisticated threat actor on HOC networks. We found the very early stages. The tracking links are the first stage. The next stage would be a dropper. The next stage would be actual exploitation software, which would have been very serious.

We would like to reinforce that the steps taken between HOC and ourselves prevented a compromise of HOC networks by this sophisticated threat actor.

● (1150)

Mrs. Sherry Romanado: You're mentioning the HOC network. We understand that in the case of MP Genuis, his personal email was actually also targeted. We understand from House of Commons IT that they're not monitoring, obviously, the personal emails of members of Parliament.

I'm assuming CSE has the ability to see, regardless of whether it's HOC email addresses or if it's a personal address—you don't have to divulge how you do what you do publicly—but there seems to be a gap somewhere, because members of Parliament obviously have personal email addresses to do partisan activities and personal activities. In this case, there seems to have been a gap between who was flagging to the MP that their personal email was receiving spam mail.

With the rest of my time, I'd like to turn it over to MP Collins. I know he has some questions as well.

Thank you.

Mr. Chad Collins: Thank you, and thanks to the witnesses for their attendance today.

You talked about a team approach. Mr. Gupta talked about the decade-long relationship that you have, working with partners. You mentioned the word “partner” several times in your opening. It's a team environment. Someone mentioned, in one of the responses to the questions, a memorandum of understanding.

Why was that put in place? Does it address any of the questions and issues that have been raised in today's meeting or last meeting?

Ms. Caroline Xavier: When we're going to be doing work with an entity that is in Canada in particular, or any entity with whom data may be exchanged that we may need to collect to be able to do some analysis to identify the threat in a better way and better understand the origins, a memorandum of understanding or an instrument of some sort is often put in place to really clearly outline how and why the information will be shared.

This is linked back to the fact that our mandate works really hard to protect the privacy of Canadians and not infringe on those rights. In particular, especially as an organization may take on some of the services we offer—host-based sensors, network-based sensors and cloud-based sensors—depending on the services that an organization takes on, that is the other reason an MOU would be put in place. It's the exchange of information that is happening or possible support to a monitoring element, so that we can continue to educate, learn from it, and clearly outline how the data is being managed.

The Chair: Mr. Collins, unfortunately that's the time, but I do have you for five minutes at the very end of this round.

[*Translation*]

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

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

Ms. Xavier, I have three questions to ask you and I think I have enough time.

Earlier, I was reassured when I asked if services were sufficient, specifically in terms of human resources. I went back and found out that on October 11, 2023, not so long ago, the CBC said that the Communications Security Establishment was in crisis. It’s not against anyone. We’re trying to be constructive. Has the situation changed so completely that you can now tell me you’re able to adjust if the House administration or even the legislation change?

Ms. Caroline Xavier: Thank you for the question.

I’m not sure which CBC article you’re referring to. However, I can tell you that, during an interview with Ms. Bureau, if memory serves, we talked about the resources and skills the Communications Security Establishment needs and is looking for.

In that interview, I said that the Canadian Centre for Cyber Security and the Communications Security Establishment were not the only ones looking for those skills. In fact, those skills are very sought after throughout Canada and the world, because everything is becoming digital.

I think it’s worth mentioning that there is immense interest in the Communications Security Establishment. That is why we feel very capable in distributing our resources, based on the budget allocated to us.

Ms. Marie-Hélène Gaudreau: That leads me to ask: How is it that we are here today with my colleague, Mr. Genuis? Information was divulged, but we were expecting individuals, including Mr. Genuis, to be up to date. We’re doing it today. What did we miss? What do we have to fix? That’s essential.

You have 30 seconds left answer my questions.

● (1155)

Ms. Caroline Xavier: Thank you.

As I said, as an organization, we like to keep learning and do things better. During your study, you will develop some recommendations. From there, we may be able to do better. The Communications Security Establishment does not set policy. In fact, we are given actions to execute, and we do our best to do so.

Ms. Marie-Hélène Gaudreau: Thank you.

Mr. Chair, I would still like to ask the Communications Security Establishment to provide us with specific information for the benefit of the report, because you obviously know what you’re talking about.

The Chair: Thank you, Ms. Gaudreau. I also thank you for acting as chair by reminding the witness of how much time you had left.

[*English*]

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

Ms. Lindsay Mathyssen: Thank you.

I'll just go back to this conversation that was had about information seemingly going one way from CSE to the House of Commons. You said this is normal. You will inform an institution, but you said that you don't expect a return on that information, or you allow them to deal with what's happened. Did I hear that correctly?

Ms. Caroline Xavier: Yes. As mentioned, a cyber-incident is usually a moment of crisis for an organization. As a result, our job is to be there as a support. Sometimes we're the ones contacting an organization to say to them that we are seeing something that is of concern. Sometimes they have identified the cyber-incident, and we call them and ask if there is anything we can do to help. Sometimes we do have that regular, ongoing, two-way communication.

However, sometimes a company might choose to have an external service provider provide them the support, so then we're just more in monitoring and wait and see....

It's not automatic that an organization will come to us or continue to want to engage with us. It's not because they're not wanting to. Sometimes, especially when dealing with cybercrime, we're dealing with ransomware. We don't encourage the payment of ransomware, and sometimes that's another reason a company might not want to deal with us, as a government entity. They're afraid that it could mean something.

Although we are not all law enforcement—we're not a regulator—we work hard to build trusting relationships, and I feel that we do that on a daily basis. However, I don't want to mislead anybody to think that means that we know all the elements of cyber-incidents that happen in the private sector, for example, or with critical infrastructure.

Ms. Lindsay Mathyssen: I understand, and I don't expect there has to be a freedom there in terms of choice, but doesn't that put potential critical infrastructure at further risk, if there isn't a follow-up on your part?

Ms. Caroline Xavier: We actually do continue to follow up with the entities. We continue to call them or work with them, and I don't want to leave anybody with the impression that there aren't relationships that exist. On the contrary, we have very great relationships with critical infrastructure, especially the energy sector, the telcos and the banks, where we meet with them regularly to talk about threats and to learn from each other about the threats they're facing. There are great relationships and governance bodies that exist to be able to work through understanding.

Having said that, though, we will continue to support and offer our support, but we can't force them. This is where, as I said in my opening remarks, Bill C-26 is really important in the four critical infrastructure sectors that have been identified as part of that bill, because they're really important to Canadians in the critical infrastructure space.

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

Mr. Genuis, we'll go to you for five minutes.

Mr. Garnett Genuis: Thank you, Chair.

Witnesses, did you impose any caveats on the information you shared with the House of Commons?

Mr. Rajiv Gupta: Typically on our reports there is a caveat that will say that you can't share this further without the explicit authority of CSE. That would probably be the caveat. I'd have to look at the reports.

Mr. Garnett Genuis: Okay.

If the reports contained a caveat saying that the information can't be further shared without CSE's permission, then how in the world would they have shared that information with parliamentarians without CSE's permission?

Mr. Rajiv Gupta: All of the information belongs to them. If it's their information, that belongs to them under whatever authority: the FAA, for example, for the rest of the departments.

● (1200)

Mr. Garnett Genuis: Yes, that's why I asked you about caveats, though.

Mr. Rajiv Gupta: That would be in our reporting, in our explicit report. Like I said, we didn't even have the emails, so we would share the key to go find them. They would find them, and then they'd have free rein to go and share that information.

Mr. Garnett Genuis: If you shared.... I think it's important that you come back specifically with what those caveats are, because—

Mr. Rajiv Gupta: The caveats restrict the system owner from sharing anything with their people.

Mr. Garnett Genuis: We're talking about information you shared with them, though. The government has said that it had information about members of Parliament facing threats, including the source of those threats. You've just acknowledged that in the process of sharing that information with the House of Commons, you likely included an expectation that they wouldn't share that information with others without your consent.

Mr. Rajiv Gupta: I would reject the premise of that statement.

Mr. Garnett Genuis: I just said what you said.

Ms. Caroline Xavier: Just to be clear, what my colleague was saying is that—

Mr. Garnett Genuis: I don't know. I'd like to hear what he was saying from him, actually.

What were you saying, sir? Was there a caveat attached, or was there likely a caveat attached, as you said a minute ago, that information couldn't be shared without CSE's agreement?

Mr. Rajiv Gupta: They could always ask us if they wanted to share something specific from the report. Outside of the report, they have access to all of their IT systems and all of the information that they can share that they own.

Mr. Garnett Genuis: Okay, so did they ask you if they could share any information?

Mr. Rajiv Gupta: No, but if they had...and we have done this many times. We've done this many times in the past with HOC—

Mr. Garnett Genuis: Here's the problem, though—

[*Translation*]

Ms. Marie-Hélène Gaudreau: Mr. Chair, I raise a point of order: How can the interpreters do their work when there are two conversations at the same time?

The Chair: Thank you, Ms. Gaudreau.

[*English*]

Mr. Genuis, can you do your best? I appreciate that you want to direct your questions where you want to direct them.

I'm not going to take time away from anybody. If there's talking over someone and it's taking away from the clarity of an answer, I'm not going to hold that against anybody, but I do think we have to play it smoothly here in terms of how we're conversing, so that the interpreters can do their job.

I have stopped the clock. Two minutes and 20 seconds remain. I hope that all those who are speaking will afford the time for the person asking the question or responding to it to do so properly.

Thank you.

Mr. Garnett Genuis: This is why this situation is bizarre. I'm here with my colleagues, Blaine and Eric, and I have information that's highly relevant to Eric's life that I should probably share with him, and I say that I'm going to tell Blaine, but I'm going to tell Blaine not to tell anyone else, including Eric, without asking me first. Then, two years later, I come back and say it's not my fault I didn't tell Eric, because I thought Blaine was going to tell him. The simplest thing would have been for me to just tell the person affected, rather than put it through a circuitous game of telephone with, potentially, caveats attached that limit the sharing of that information anyway, and potentially without all the information involved.

Fundamentally, the question is: Why was all of this nonsense interposed in between the people who had the information, which is the Government of Canada, and the people who needed the information, who were members of Parliament under threat who could have taken further preventative action to protect themselves? Why was it so difficult for the government to just tell us directly?

Ms. Caroline Xavier: As I've mentioned, we take our role very seriously, and we take the privacy of Canadians very seriously. We take the role that we play with service providers like the House of Commons very seriously. We recognize that everybody has a role to play in the process.

Having said that, I recognize that we're going to learn from this incident and hopefully get a better understanding, especially from the study that you'll do, on how we might do something differently.

Mr. Garnett Genuis: Did you clearly tell the House of Commons that APT31 was the source of the threat? When did you tell them that?

Ms. Caroline Xavier: As per the chronology, since January 2021 we were aware of some activities going on. As was explained by my colleague Rajiv, we progressively started to better understand the threat—

Mr. Garnett Genuis: I asked a specific question that's not answered by the chronology.

Did you tell the House of Commons that APT31 was the source of the threat and, if so, when?

Ms. Caroline Xavier: I believe we've answered the question that we did tell the House of Commons, through the various interactions that we had with them, that we believed at that time that the threat was APT31.

Having said that, the member asked me what specific time that was, and I'm not able to tell you exactly on which date that happened—

● (1205)

Mr. Garnett Genuis: Can you tell us the month?

The Chair: Thanks very much.

Mr. Garnett Genuis: The year?

The Chair: I'm sorry, Mr. Genuis. We're already over time here.

We're over to you, Mr. Collins, for five minutes.

Mr. Chad Collins: Thanks, Mr. Chair.

Ms. Xavier, I think you've painted a picture today that you provide a service to clients, and those clients could be within the government or elsewhere. When you're made aware of information, you provide that information to organizations or departments.

I could probably pose the question, you know, that this is something that could happen to the defence department. We can look at our support for Ukraine and all of the efforts that Russia is doing to those people around this table who still support Ukraine.... Russia has taken many approaches to try to undermine our support on that file.

If this happened in defence, you would provide that information to defence as your client. Would you consider them a client in that instance? You'd provide them with information, and then it would be up to defence to determine internally, with their own security people that they have and their own IT people, what they do.

Is that a fair comparison in terms of how, if this happened somewhere else in the organization, you'd take the same approach?

Ms. Caroline Xavier: That is correct. That is exactly how we function.

Mr. Chad Collins: You said earlier...you used the words that you're “respectful of the independence”. I think you were referring to the House of Commons staff. What level of independence do they have in this instance in terms of dealing with this?

They have their own IT security people. They were here at our last meeting, as you know, and they provided us with evidence. They're responsible for their area of the organization. Maybe that's not the right term, but I think you understand what I mean in terms of how they have their own roles and responsibilities as it relates to dealing with parliamentarians in this instance.

Can you talk about what level of independence the areas of government or external stakeholders have? Where do you draw that line in terms of how you're providing a service but you're giving that information to the client?

Ms. Caroline Xavier: We are very much like a service, as you mentioned. When we are made aware of an incident or when we see something through the tools we have, the intent, our goal, is as much as possible to get the information to the right people, to enable them to act and mitigate the threat first. On what happens in a case like a Government of Canada system, deputies, for example, are the ones accountable within each of the departments, and then they have accountability to a minister.

When we pass on that information to an IT department within a government organization, they are the ones who are going to take the necessary steps, with our support as well as, for example, that of Shared Services Canada. It depends on the department.

In an industry as well, it's the same: We'll contact the IT organizations and tell them we've seen something and they are to act on behalf of their organization. Often there will be this back-and-forth that we talked about before in terms of gathering more information for them to act on.

We do this actually quite regularly, because we do this in a pre-notification ransomware initiative that we have put in place with our U.S. partners, for example. Over 500 organizations have been contacted by us at what we call a “CISO level” to be able to thwart an attack before it happens, saving them millions of dollars.

Mr. Chad Collins: This one is a little unusual, isn't it? There's lots of drama, as you've heard with some of the questions here this morning. We're not a normal client, I would say. I want to go back to the MOU in terms of how all areas of the organization have looked back at what we could have done better and how we improve things moving forward.

Does the MOU deal with the communication aspect? You've heard some questions today about who should have been notified by whom and when. What did that new MOU determine as it relates to your relationship with House of Commons staff?

Ms. Caroline Xavier: I don't want to mislead the committee, so I'll have to go back and reconfirm the contents of the MOU. I can't say that I read it before coming before this committee this morning—

Mr. Chad Collins: I think the question would be, going forward, who's to contact parliamentarians if this happens tomorrow?

Ms. Caroline Xavier: Again, we expect to learn from this incident and to work in collaboration with the House of Commons to identify the best way forward so this incident is not repeated.

● (1210)

Mr. Chad Collins: I'll cede my time, Mr. Chair. I'll pass it on.

The Chair: That's great. Thanks very much, Mr. Collins.

Colleagues, that brings us to the end.

Do you have a point of order, Mr. Duncan?

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

This is just a note for future meetings. I know we have one already scheduled for Tuesday, with a list of witnesses that has been made public. Going forward, could we get into the habit of having the witnesses provide their opening testimony to us in advance, in both official languages? The witnesses had a lot to say in the opening, and it's difficult for us to follow along. I'm trying to make notes. There's a lot being said.

Could we make that the standard going forward, knowing that this is going to be studied? We know who our witnesses are, so could the expectation be that they give it to us at least a day in advance, please?

The Chair: That's a fair point to raise, Mr. Duncan. I think we'll just suspend. We don't have to deal with this immediately. The point is taken. We're going to suspend. We can chat about how we can be more effective in that process to benefit members, witnesses and interpreters.

Colleagues, we're going to suspend briefly before we head into the second half. Thank you.

[*Proceedings continue in camera*]