HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

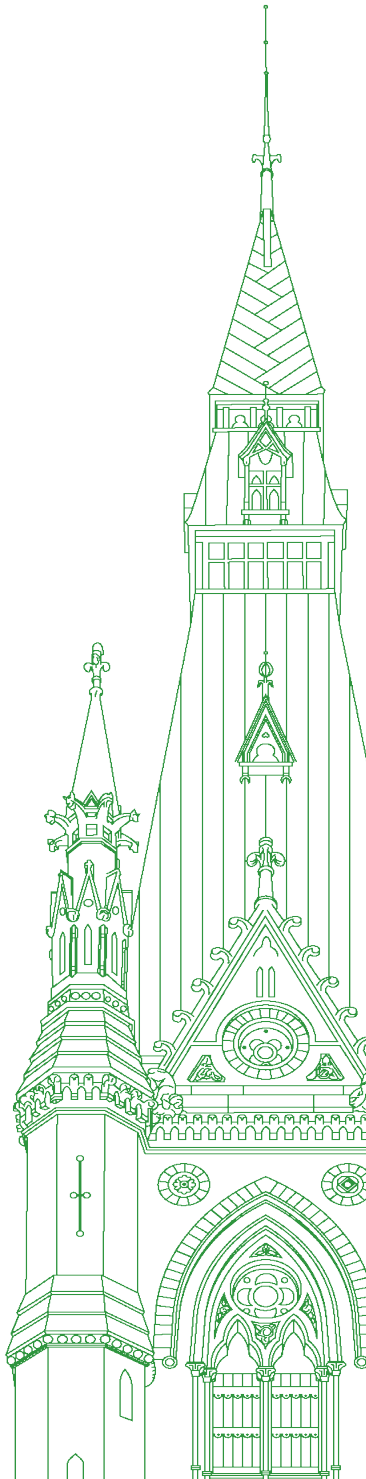
44th PARLIAMENT, 1st SESSION

Standing Committee on Procedure and House Affairs

EVIDENCE

NUMBER 121

Thursday, June 13, 2024



Chair: Mr. Ben Carr

Standing Committee on Procedure and House Affairs

Thursday, June 13, 2024

● (1100)

[*English*]

The Chair (Mr. Ben Carr (Winnipeg South Centre, Lib.)): Good morning, everybody. I hope you have had a good week.

[*Translation*]

Welcome to meeting number 121 of the Standing Committee on Procedure and House Affairs.

[*English*]

Colleagues, we are continuing our study on the question of privilege related to cyber-attacks targeting members of Parliament.

I have just a friendly reminder, as always, as we begin. Please ensure that your audio devices are placed securely on the stickers to either side of you in order to protect the health and well-being of our interpreters, who do such important work for us.

Colleagues, we are joined by a number of our parliamentary colleagues today. The format remains the same.

With us today, we have James Bezan, the member of Parliament for Selkirk—Interlake—Eastman; Garnett Genuis, the member of Parliament for Sherwood Park—Fort Saskatchewan; and the Honourable John McKay, the member of Parliament for Scarborough—Guildwood.

Each witness will be given the opportunity to speak for up to five minutes, and then we will proceed to our regular opening round.

Gentlemen, I'm not sure who wants to begin. I'm not sure if you've had a conversation amongst yourselves, but do we have a volunteer in terms of who would like to go first? It's Mr. Genuis. Okay.

Mr. Genuis, with that, the floor is yours for up to five minutes for your opening remarks.

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

The material facts of this case have already been laid out in the House. I am happy to repeat them in response to questions, but I'll use my opening statement to instead make some specific arguments about what we can learn from this situation.

Generally speaking, we expect a high level of secrecy when it comes to national security. While, in a free democracy, people should generally have access to information about what the government is up to, information pertaining to national security is closely guarded because it could be used against us by adversaries.

On the other hand, it is a well-established principle of national security that information must be shared with citizens if they need that information to defend themselves. For example, if we were at war and a particular area faced imminent bombardment—

The Chair: Mr. Genuis, I'm sorry to interrupt. I'm just hearing from the interpreters that your pace is a little bit quick, so if you could just slow it down.... I'll be generous in terms of making sure that if it costs 30 seconds for the well-being of interpreters to be adhered to, we will offer that to you.

Go ahead, Mrs. Romanado.

Mrs. Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.): On that same note, I understand that Mr. Duncan requested that witnesses provide their speaking points in advance of the meeting. Were they provided to us? I'm not sure if the interpreters have them.

The Chair: I don't know the answer to that, Mrs. Romanado.

Mr. Garnett Genuis: Mine were.

The Chair: They were—okay.

Thank you, Mr. Genuis. I stopped the clock. You have four minutes and 15 seconds remaining.

Mr. Garnett Genuis: Thank you, Chair. I appreciate your indulgence.

On the other hand, it is a well-established principle of national security that information must be shared with citizens if they need that information to defend themselves. For example, if we were at war and a particular area faced imminent bombardment, we would expect the government to warn citizens of the attack so they could shelter themselves. We would not expect government to keep that information secret, obviously. If a terrorist planted a bomb in a building, we would expect the building to be immediately evacuated and not for the government to keep that information secret simply because it involved security.

What is obviously true of physical attacks should, based on an extension of the same principle, also apply in the more benign cases of cyber and other kinds of foreign attacks. The principle remains that the victim or potential victim has a natural right to know, so they can defend themselves.

Moreover, foreign interference is a particular case where exposure is a central part of the solution. The impact of foreign disinformation is significantly reduced when people become aware of the source. In this way, it is exposed as propaganda and loses its persuasive power. The impact of foreign takeovers of institutions can be undone simply through exposure, and politicians identified as foreign collaborators are less likely to be re-elected. When people are aware that the source of something is a hostile foreign state, that awareness may dissolve the impact of the threat.

The current government has used national security as an excuse for keeping secret information related to foreign interference that it would be in the national interest to expose, or where exposing that information would protect victims and reduce the overall impact. Three known examples of this phenomenon are the secrecy that long surrounded the Winnipeg lab documents affair, the failure to inform members of Parliament of threats against them or their families—which resulted in two separate questions of privilege recognized by the Speaker—and the current insistence of the government on keeping secret the names of parliamentarians who have intentionally collaborated with hostile foreign states. It is hard to see how the public interest is served by secrecy in any of these cases.

When it comes to foreign interference, we should be strategically declassifying certain information precisely as a tool to fight against interference. The government's defence of their failure to inform me of threats against me was that they told the House of Commons about these threats, and that they respect the role of the House of Commons as an institution separate from the executive.

In response to this, I will make five observations.

Firstly, as you know, I was targeted at my personal email. House of Commons IT were informed about attacks on parliamentary accounts. I suspect the administration here wasn't even informed of the attack on me, because that had nothing to do with their jobs.

Secondly, we have still not heard clear testimony regarding what information exactly was shared with House IT and when—whether it was merely a few technical details or the full robust picture that was shared with our intelligence services by the FBI. Without the full picture, it would have been hard for us to be briefed.

Thirdly, the government's argument seems to badly misunderstand the nature of the work expected of IT professionals. House of Commons IT are not an intelligence or communications service. They work on IT. It would seem strange, in principle, for those IT professionals to have decided of their own accord to walk around the building and talk to parliamentarians about the threats they face.

Fourthly, CSE acknowledged in their testimony that there were likely caveats associated with the information shared that prevented House of Commons employees from resharing the information without permission. I would suggest that the committee send for further and clearer information about what exactly was shared with House of Commons IT services—when and with what caveats.

Finally, the underlying logic of the government's argument for secrecy is deeply flawed, because the rights and privileges of members of Parliament are vested in them as members of Parliament. Those rights are what enable us to do our jobs for our constituents. Those rights can be given up or modified by the agreement of the House, but they are not held, controlled or modifiable by House administration. The way to respect the rights and independence of members of Parliament is to give them the tools and information they need. The government's argument here implies that the House administration is the holder of our rights, as opposed to members themselves. That is, of course, dead wrong.

Chair, that's my opening statement. I look forward to questions.

● (1105)

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

Is it Mr. Bezan or Mr. McKay?

Mr. Bezan, the floor is yours, sir, for five minutes.

Mr. James Bezan (Selkirk—Interlake—Eastman, CPC): Thank you, Mr. Chair.

Good morning, colleagues.

I am also one of the 18 members of Parliament and senators who are members of the Inter-Parliamentary Alliance on China. APT31 targeted us way back in 2021 and 2022.

Now, what is shocking is that as parliamentarians we were never informed that we were the subject matter of a hack attempt or cyber-attack by the Communist regime in China. By letting us know, we could have then, as parliamentarians, taken protective and corrective actions, but we couldn't because we were never told. We were not informed of this by the House of Commons IT services. We were not informed of it by the RCMP. We were not briefed by CSIS, nor did CSE reach out to us, which ultimately found out through the FBI and informed the House of Commons IT services.

All of us did get briefed on May 9 by the FBI. That, I think, is embarrassing. That was the way we were finally told about how the attack occurred and how we could protect ourselves.

Now, I have to say that the Sergeant-at-Arms in the past has...and was offering a briefing to us this afternoon. It's unclassified, but it's on how we protect ourselves from cybersecurity attacks and what types of measures we take. CSE has briefed me in the past and also others who were targeted on social media by misinformation and disinformation from the PRC.

Also, of course, all of us who have travelled and have been given burner phones by the House of Commons, Global Affairs or the Department of National Defence in our parliamentary activities have received those briefings for travel. I may have a bit better understanding than others of the cybersecurity threats that are out there, but that doesn't make acceptable the actions that were taken by the House of Commons and those in charge, because this isn't an isolated incident. This is happening all the time, and we need to be better informed.

The PRC has been spying on me for a while. I have activities. I'm a patron of Hong Kong Watch. I'm a member of the parliamentary Canada-Taiwan Friendship Group, along with many of you. A number of us at this table travelled to Taiwan as recently as last year.

Iran is also named in the NSICOP report. I'm a co-founder of Canadian Parliamentarians for Human Rights and Democracy in Iran. As you know, I was very big on the charge to get the Quds Force listed as a terrorist organization in 2012. In government, I led the shutdown of the Iranian embassy and consulates here in Canada, and I've been recognized by the Persian community for my advocacy.

Of course, the Russian Federation has been targeting me on social media with trolls, not with bots, for a long time. I was one of the first group of 13 that was banned from Russia back in 2014. I'm vice-president of the Canada-Ukraine Parliamentary Friendship Group. I've been outspoken in my support of Ukraine and, of course, Russia is going to take actions against any of us who are advocates for Ukraine. I brought forward the Sergei Magnitsky Law.

Why does all that matter, all my activities that are beyond what many would say is my scope as a parliamentarian and my day-to-day activities? Modern espionage, intimidation and foreign interference tactics are violating our collective rights and our privileges, but also our privileges as individuals, and this is the new norm.

In Bosc and Gagnon, the Speaker's ruling as referenced on pages 107 and 108 says that we have to make sure that:

> ...Members should be able to go about their parliamentary business undisturbed. Assaulting, threatening, or insulting a Member during a proceeding of Parliament, or while the Member is circulating within the...Precinct, is a violation of the rights of Parliament.

It also says, on page 111:

> A Member may also be obstructed or interfered with in the performance of his or her parliamentary functions by non-physical means.

● (1110)

We have to modernize our efforts to protect our privilege from cyber-attacks. It's no different from a physical obstruction or interference in performing our duties. That particularly is concerning to me. I'm the Conservative shadow minister for national defence. I'm vice-chair of the Standing Committee on National Defence, and John is the chair. We serve on these committees. We talk about information. I provide advice to our leader. We develop policy and platform ideas.

If I'm being targeted by those who try to hack into my emails and my communications, Mr. Chair—and I know I'm getting close on time—then we have to take corrective measures. The laissez-faire and "we don't care" culture coming from the PMO and PCO has infiltrated through the rest of our departments and the way we operate up here. We have to make sure that we are more aggressive in how we protect each and every one of us from these cyber-attacks. That means that we need to know when we have to reclassify how information is shared.

Thank you.

The Chair: Thanks very much, Mr. Bezan.

Mr. McKay, the floor is yours for up to five minutes.

Hon. John McKay (Scarborough—Guildwood, Lib.): Thank you, Mr. Chair.

I'll just pick up where James left off, with the core issue that is in front of this committee, which is when members should be informed of these attacks. These attacks are simply a fact of life. They are massive, and they will increase.

I'm rather hoping this committee will grapple with how, when and where we are to be notified of these attacks, because, frankly, I'm given to understand that there are something like a million attacks a day on this organization, the Parliament of Canada. I don't think every member wants to be informed of every one.

In some respects, we're in a fortunate position in that the evidence at this point shows that we didn't actually suffer any damage. There was no breach and the firewalls held. Having said that, it is—and I adopt my friends' views—kind of embarrassing to learn from a foreign security service that we've had an attack. Frankly, I don't think that's quite acceptable.

The FBI tells the CSE, the CSE tells our security services, our security services are satisfied that the breach does not occur and we're in the dark. We're in the dark for two years, and we only find out about these attacks by virtue of the unsealing of an FBI document.

When we were briefed by the FBI, the FBI representative told us they felt outgunned—I think that's the word he used—50:1. These attacks are massive, and the FBI feels overwhelmed.

This committee needs, in my view, to start wrestling with our protocols. Clearly, the current protocols are not acceptable. For two years, the three of us, plus all of our other colleagues, were quite vulnerable.

● (1115)

I'm rather hoping this committee actually gets to the nub of it. I'm not interested in the blame game. I'm not interested in "we should have done this or done that." Protocols need to be established, because everyone at this table, every one of our colleagues, is vulnerable. I'm rather hoping you take this example of vulnerability—which I don't think has entered into any kind of damage—and give instructions to those whom we ask to protect us.

We are all engaged—and, again, I adopt James's view—in multiple activities that create a vulnerability and are within our privileges as members of Parliament.

I support Garnett's motion, but I want this committee to focus on the protocols that would be appropriate.

Thank you.

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

Colleagues, we will head into the first round of questions.

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

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

Thank you, colleagues.

The committee received a chronology of events from the CSE. The chronology states that CSIS issued a briefing on the Beijing-directed APT31 cyber-attack to 35 Government of Canada clients as early as November 2021.

I asked the director of CSIS who received this briefing, and he has undertaken to provide this committee with a list. However, he did say that, as a general rule, "such a product would indeed be distributed to the Privy Council Office, and that would include the national security and intelligence adviser" to the Prime Minister.

What does it say to you—the fact that, as early as November 2021, 35 Government of Canada clients, likely including the Prime Minister's own department, the PCO, were briefed about this cyber-attack, but you and every other member of Parliament who was a target were kept in the dark?

Whoever wishes to—

Hon. John McKay: I'm happy to respond to that.

Mr. Cooper, I think you've hit the core issue. We were not on the distribution list, shall we say. The protocols at that time—two years ago—are frankly found to be inadequate.

I'm hoping this committee will actually address that issue because it's not acceptable that we were in the dark for the last two years.

Mr. James Bezan: I'll just jump in on this.

You have information shared to government officials. The national security adviser, as we read in the NSICOP report, withheld information from people who should be informed. That information should have been shared with us, as individuals, as to the matter of the attack.

When you look at the culture that exists within the Government of Canada on how they classify information and how they share information, especially when it comes down to foreign intimidation—and APT31 is nothing more than foreign intimidation—we have to be taking on new protocols for how we deal with it. The national security adviser has to be a lot more aggressive in making sure that information percolates through the system and not just to the Prime Minister.

In this situation, where it's involving members of Parliament, that information should be distributed or individuals contacted directly, whether it's through caucus leaders or caucus chairs. We need to make sure we don't repeat these mistakes. I think that is paramount to our ability to do our jobs.

Mr. Michael Cooper: Mr. Genuis.

Mr. Garnett Genuis: I agree with what my colleagues have said.

Thank you for an important question, Mr. Cooper.

I have just one point to add in terms of the dissemination of information.

In the previous hearings with previous witnesses, we have tried to get at what exact information was disseminated, in particular what information was disseminated to House of Commons administration. The government's communication on this has said that "the information"—implying all the information—was given to House of Commons administration.

I pursued this matter with Ms. Xavier, from CSE. I asked her if the House of Commons administration was informed that the source of the threat was APT31.

She chose her words very carefully. I didn't actually notice what she was doing until I read over the testimony afterwards. She said, in response to one of my questions, "As part of the various meetings and the reports we provided, we were able to share with the House of Commons IT security staff what we believed at the time to be the originating source of the threat."

Then I followed up that she had shared with them that it was APT31 and at that point she refused to answer. She said we should go in camera and various other points.

She said she shared what they thought was the source of the threat, but she never actually said they shared that the source of the threat was APT31, so there are big questions. I think there's a little bit of sleight of hand being attempted by officials about what information was actually shared, especially with House of Commons administration.

● (1120)

Mr. Michael Cooper: Thank you for that.

While I completely agree with Mr. McKay that we need to look at solutions to ensure that what happened doesn't happen again, there does have to be some level of accountability. To that end, the government has essentially washed its hands clean insofar as they have tried to place the blame squarely on House of Commons administration.

Then, when we begin to probe House of Commons administration, it seems to have fallen all on House of Commons IT, yet 35 Government of Canada clients, including likely the Prime Minister's department, the PCO, were briefed in November 2021. That's more than a year and a half before you were finally briefed, thanks to the FBI.

Again, the notion that it should be left to IT services, which was dealing with the technical matter of ensuring the integrity of IT systems in the House of Commons, to inform members of Parliament seems to be completely untenable. Wouldn't you agree?

Shouldn't there be some level of responsibility if, in fact, the PCO and the national security and intelligence adviser were informed in November 2021 and said nothing and did nothing for a year and a half, and would not have done anything but for the FBI?

The Chair: Mr. Cooper, unfortunately, that's all the time. Certainly, in the next round, you're welcome to raise that.

Mr. Michael Cooper: If I could get a simple answer—

The Chair: Unfortunately, your preamble—

Mr. Michael Cooper: I think it's very interesting that you're cutting me off on that important point.

The Chair: I'm not cutting you off, sir. I'm simply applying the rules fairly. You will have another opportunity to ask questions of our colleagues.

Ms. Romanado, the floor is yours.

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

I'd like to start my....

Mr. Chair, I have the floor. If Mr. Cooper would like to please stop interrupting me, that would be—

Mr. Michael Cooper: I want an answer to my question.

Mrs. Sherry Romanado: You've had your chance, Mr. Cooper. It is my time. Thank you.

Colleagues, I want to premise this with my firm belief that you should have been made aware at the time, so I want to make sure that you understand. I completely agree that what happened was inappropriate and that you should have been made aware.

We are trying to get to the bottom of what happened and how we can make recommendations to make sure that such a situation does not occur.

I want to just get clarity from each of you on some specifics.

Mr. Genuis, you mentioned that it was your personal email that was attacked. Is that correct?

Mr. Garnett Genuis: That's correct, yes.

Mrs. Sherry Romanado: Was your parliamentary email as well or just your personal?

Mr. Garnett Genuis: I don't believe my parliamentary email was. I think it was only the personal.

Mrs. Sherry Romanado: On what date did you become aware of the fact that you were a victim of the cyber-attack?

Mr. Garnett Genuis: It was earlier this year that I was informed by IPAC. We had a joint briefing and, as I remember the sequence of events, Mr. McKay and I, who are co-chairs of the organization, heard the information first. We had a briefing with members of Parliament later that day. I was let know of the situation very shortly before, in terms of convening those meetings that took place, but it was all within the space of a few days in late April of this year.

● (1125)

Mrs. Sherry Romanado: Thank you.

Mr. Bezan, which email account was used in the cyber-attack in your case?

Mr. James Bezan: Based on the information that we received from IPAC in the IPAC briefing from the FBI, it was our P9s for most of us, and I think that what we were told—although I've never had a conversation with IT services, with the Parliamentary Protective Service or the Sergeant-at-Arms—IT was able to catch it in time, so the firewall worked.

If you look at the case of Mr. Genuis, they were targeting his non-parliamentary account, and that is troubling. In response to what Michael said, I'll just say this—

Mrs. Sherry Romanado: I don't have time—

Mr. James Bezan: —PPS, the Sergeant-at-Arms and House of Commons' IT services all have a role to play in this to make sure that we are informed when these things happen.

Mrs. Sherry Romanado: I agree.

I'm going to go to Mr. McKay.

Mr. McKay, was it your personal email, your parliamentary email or both?

Hon. John McKay: It was my P9, as far as I know.

Mrs. Sherry Romanado: You learned about it at the end of April of this year. Is that correct?

Hon. John McKay: Yes.

Mrs. Sherry Romanado: We've had the CSE, we've had the House of Commons administration, and we've had CSIS come before this committee. It seems to be, as I'm sure you are aware, Mr. Genuis, a sort of “it's not our role to inform MPs”. They all have a little box that they work in, and no one seems to know whose responsibility it is to inform MPs, so part of our study here is to put in place the proper protocols to make sure that, in the event of another situation....

I understand that there was a directive, a ministerial directive, issued to CSIS in May 2023 to inform them that MPs must be made aware.

Would you have any recommendations for this committee in terms of.... I don't want to say a workflow. In the event of a situation such as this occurring again, who would you recommend be the appropriate channel to make sure that MPs are notified immediately?

Hon. John McKay: If I were attempting to write a protocol, I think, first of all, I'd pick up on Mr. Cooper's question that a lot of government authorities all seemed to know, and we didn't. That's unacceptable.

The other point I'd like to make is that we are not the Government of Canada. We are the Parliament of Canada, and we sometimes confuse that. We do interact with government agencies, CSE in this particular instance, so any protocols that should be written should be directed to the House of Commons authorities that look after our security, and I think that's where this committee should focus.

How you arrive at when, if and how I think is extremely difficult. I would hope that the committee focuses its energy on that instead of running around saying that everybody else knew but us.

Mr. James Bezan: Can I follow up on that?

I really believe our physical presence here and our physical protection is through the Parliamentary Protective Service under the auspices of both the Sergeant-at-Arms and the RCMP. Ultimately, they should also be the ones who are responsible for protecting us from cyber-attacks. Whether it's a physical attack or a non-physical attack, somebody has to take the lead here. The Parliamentary Protective Service is first and foremost responsible for making sure we're safe. That includes from online cyber-attacks, deepfakes, AI and all these things that now are going to ramp up and become even more dangerous as we go forward as parliamentarians.

Mrs. Sherry Romanado: Given the fact that in the role we play, we all have personal email accounts—we have them for partisan purposes and so on—would you recommend that some protocol be put in place in terms of also our personal email accounts, given the fact that all of us have those kinds of accounts?

The Chair: One witness can take 10 seconds, please.

Mr. Garnett Genuis: I don't think House of Commons security can be everywhere we are. We're on our personal emails. We're physically in other parts of the country. I think that's where intelligence services have to be taking that macro view. If there's information about a threat to you that may manifest itself on your personal account, in your constituency or when you travel, they need to be informing you, having that broader view of security issues that goes much beyond just what happens in Parliament and with parliamentary devices.

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

● (1130)

[*Translation*]

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

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

Mr. McKay, did you know what APT31 could do to you? What are the mechanics of that?

[*English*]

Hon. John McKay: It was described to us as a pixel attack. I'll give the description I have, because I'm still not quite sure I understand it:

> The emails that you received were all from the domain "nropnews.com". There were various email addresses and names of fake journalists attached to this domain. This kind of attack is known as pixel reconnaissance. It works by embedding a tracking pixel in a photograph or image. When the receiver opens the email, the tracking pixel is able to send back some limited information to whoever has sent the email.

It's kind of like a phishing expedition.

[*Translation*]

Ms. Marie-Hélène Gaudreau: When did you get that information?

[*English*]

Hon. John McKay: It was late April.

Mr. James Bezan: I believe it was April 24 when this was shared through IPAC to us as members of IPAC.

Mr. Garnett Genuis: Perhaps I can add that, aside from the technical pieces, I think the key practical aspect of what Mr. McKay is describing is that this is the early stage of a likely broader attack. It's where an actor is trying to get some information, which they would then use as part of subsequent attacks.

We've now been briefed by the FBI on particular techniques that we can use to protect ourselves in the context of this escalation. This is why informing us is critically important. When you know that you're potentially at the early stage of a reconnaissance attack, you can then put in place those mechanisms to better protect yourself. We weren't told, so we weren't able to protect ourselves.

[*Translation*]

Ms. Marie-Hélène Gaudreau: What astounds and upsets me is that we've been studying this for months, wondering about it and wanting to prevent it. Personally, I'm not in the intelligence service, but on December 15, 2021, I found a document on the web about the APT31 attack campaign.

Honestly, I would have expected the Communications Security Establishment, or CSE, to give us the details and the techniques. The newspaper Le Monde describes how APT31 works. That's why, for me, it's important to know when you knew, but also whether the techniques were clear. You can find out by doing the research yourself.

The CSE could have corrected the situation. Are you satisfied with the service provided at this time, in an emergency situation?

[*English*]

Hon. John McKay: No.

Mr. James Bezan: I would say we wouldn't be here if.... We're all very disappointed.

CSE is a great organization. They are well respected within the Five Eyes. We talk about who's ultimately responsible. PPS is responsible for parliamentary protection, and they have a role to play in this. Definitely, CSIS and CSE are the outward-looking agencies—our intelligence agencies with the ability to handle cyber-attacks. They are the ones that have to make sure those within the House of Commons are in the know. Again, it comes down to the sharing of information and how we classify it, and ensuring proper measures are taken so we can take corrective actions to protect ourselves.

We are our own independent parliamentary offices. At the same time, we have a collective weakness: our emails and online communications.

[*Translation*]

Ms. Marie-Hélène Gaudreau: What I understand is that you agree that we overclassify and that, in our information culture, people say that it's not for us, but that, ultimately, the world is watching us. Today, with all the time we've taken, imagine the new tactics that are in place.

Are you prepared to review both parliamentary privilege and how far to go to protect our privacy at the expense of interference? What do you think? We want to review everything, but do you think we really need to reform and question ourselves?

● (1135)

[*English*]

The Chair: There are about 30 seconds between you.

Hon. John McKay: Let me just say this: You have three members of the defence committee here. They all agree we overclassify everything. That is a settled view on the defence committee.

Having said that, yes, whenever those rules were written, it was way too late. They did not contemplate this kind of issue. This committee would do a wonderful service by updating how we deal with things like phishing attacks.

Mr. Garnett Genuis: In just 10 seconds, I'll say that sharing information is a critical way of fighting foreign interference. Telling people about these attacks is a big part. It's not the only way and it doesn't work for everybody, but it's a critical part of how we fight back against these threats.

[*Translation*]

The Chair: Thank you, Ms. Gaudreau.

[*English*]

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

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

Thank you for appearing today. It's interesting to see us in this different set-up, as opposed to in committee together.

I want to go back to what you said, Mr. McKay, in terms of the when, the if and the how.

It's difficult. As we all know, in the House of Commons, our emails are fairly semi-public at this stage. People crack the code all the time. There are millions of attacks daily upon the House of Commons. This particular APT31 attack was thwarted. Therefore, as it's been told to us, you were not informed.

How, in your opinion, should we go forward in terms of that when, if and how, when there are so many? How do you expect the House of Commons to move forward within such incredible complexity and that sheer number?

Hon. John McKay: If I had an answer to that, I would mail it in. I might even charge you for it.

This is the critical issue in front of this committee. I'm not quite sure about the how, because the volume is immense. The level of threat is variable. The trouble is that the level of threat is not only variable from a national security standpoint but also from an individual parliamentarian standpoint. What I may perceive to be a threat James or Garnett may think of differently.

I wish I could answer your question.

Ms. Lindsay Mathyssen: Would it be more based upon the one doing the phishing?

Hon. John McKay: That would be one of the things. Even if you say, "Well, it's a Chinese threat", okay, that's one level of threat. An Iranian threat is another level of threat. Some guy in his basement in Moose Jaw is another level of threat—no disrespect to Moose Jaw.

Mr. James Bezan: I'm expecting that AI is going to be used to amplify and expand the number of cyber-attacks we all face. I think the one side of this is what's happening collectively. We need to know when it's very targeted. APT31 was very targeted at the 18 of us.

That, I think, is where you need to start saying, okay, you guys need to start watching your personal accounts. You need to be watching what you're doing on your iPhones and in other apps and how your passwords are protected. You know, those types of pieces are what you start sharing with individuals.

If it's just a broad-based attack going after all the P9s, all A1s, all our individual staff or all staff collectively, I think then we just leave it up to IT and CSE to thwart that. When they're targeting us as individuals or going after those of us on the national defence committee, we should know.

Mr. Garnett Genuis: I can add to that.

I don't think it's that complicated at the level of principle to say that, if there are general phishing attempts that are of the sort that target all accounts and come in on a regular basis and are more or less sophisticated, then that's in a different category from your being targeted, Ms. Mathyssen, by a particular foreign state as a result of their not liking a motion you put before the House or a committee. I think in such a case you as an individual would want to know that you were being targeted by a particular actor for something you'd done. That situation might require you to take particular additional steps to protect yourself that are different from what is required by other members of Parliament.

I think that should clearly flip a trigger that says there's a conversation that needs to happen between security agencies and you that's a bit different from what's being done generally with all members of Parliament.

● (1140)

Ms. Lindsay Mathyssen: At some point later in this Parliament, this committee will be studying the "need to know" legislation that's been proposed by Mr. Ruff, Bill C-377. We've had many conversations about this in our defence committee as well in terms of what level of security clearance certain members could have, should have and what have you. How important do you think that is?

As it relates to this conversation, how do members of Parliament navigate that in terms of what they do know and what they have access to in this greater-risk threat environment?

The Chair: There's about one minute remaining, witnesses.

Mr. James Bezan: I support Mr. Ruff's bill completely. I think it's the right way to go to provide classifications to us—whether they're secret, top secret or higher, based upon the rules we have. We definitely have to go through the clearances that are required and background checks. I'm not expecting just a free-for-all, that as soon as you get elected you get a top secret clearance. I do think there is a proper process.

I think this is even a little more different. I agree with Garnett that, as we know more about foreign interference and more about cyber-attacks happening to us on the Hill here, we can share that with the public. We can restore confidence in our democratic institutions.

One of the ways in which we can handle this in a broader way is that Parliament, in general, should be issuing an annual report on the cyber-attacks that we're facing and how we've been able to deal with them. I think it's a way to provide some accountability and also a greater understanding of the evolving cybersecurity threat we're in.

The Chair: Thanks very much, Ms. Mathyssen.

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

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

Members, do you accept the government's contention that this all fell on the House of Commons administration and, as it turns out, House of Commons IT services to brief members of Parliament about a cyber-attack of this nature?

Mr. Garnett Genuis: I'll start, Chair.

No, I don't. I made, I think, five distinct points in my opening comments about why I don't. It was, in my case, a personal account. There are gaps in terms of what we know about what the House was even told. The government misunderstands the nature and expectations of IT professionals, the potential for caveats and the fact that members of Parliament are not creatures of the House. We have rights of our own.

Mr. Cooper, just to follow up on your previous comments, we can talk about systemic failure, systems not doing the things we would expect of them. Then we can talk about individual accountability, people not making the choice to ensure that the information got there.

I think it's important to talk about systems, but also we can't miss the accountability piece that you've pointed out, which is that people had this information and made a choice not to take the steps necessary to get that information to those who were being targeted. I don't think we should use a discussion of systems to detract from the fact that individuals in those systems made choices, and those choices led to members of Parliament being more vulnerable to foreign threats.

Hon. John McKay: I'm not quite so enthusiastic about blaming the government for everything. I think this is more a failure of protocols. Apparently, as the FBI released the information to various governments, some governments had exactly the same protocol Canada had. Other governments' were much more detailed. I tend to think that at this stage, two years on, those protocols need to be changed.

I don't want to take all the time. You want to get James back in there.

● (1145)

Mr. Michael Cooper: Yes.

Mr. James Bezan: I don't buy that argument. It's not just protocol. It's a culture. It starts at the top. It starts in the Prime Minister's Office. This information has to be shared. The way they classify that information, the way they direct traffic, whether it's through CSE, CSIS, RCMP, the Parliamentary Protective Service or the Speaker, and the way they share that information all starts with the yes or no that comes from the top in the PMO.

Mr. Michael Cooper: I guess I would push back a little bit on Mr. McKay insofar as the ministerial directive was issued in May 2023, following the last question of privilege dealing with Mr. Chong. Following that ministerial directive, there was again a briefing to so-called relevant Government of Canada clients about the APT31 cyber-attack. Again, no members of Parliament were briefed.

Does that lend you any confidence in the ministerial directive and this government's approach to making members of Parliament informed?

Hon. John McKay: Let me push back on the push-back and say that the ministerial directives are helpful but late. Are they properly executed? I don't know. I would have hoped that once that ministerial directive was issued in 2023, they might have reviewed their previous decisions, particularly with respect to us, and advised us, even if we were advised late.

Hopefully, this committee will actually indicate that there is a need to change not only the culture here but also the system and the timeliness of the implementation of the change.

Mr. Garnett Genuis: It sounds like Mr. McKay was agreeing instead of pushing back there.

Hon. John McKay: I would like to think that we can spend a little bit more time actually dealing with solutions and analysis of the problem instead of just wasting our time blaming whoever should have been blamed. I'm perfectly prepared to accept that this was an error. We should have been named.

Mr. James Bezan: There's actually a pattern here. It comes back to the national security and intelligence adviser—

The Chair: Mr. Bezan, I am going to let you respond. I'll give you a little bit of leeway if you want to reply.

Mr. James Bezan: I would just say that there is blame to go around here, not only at the PMO but in the PCO with the national security and intelligence adviser. What we saw under NSICOP with not sharing information, what we've seen in reporting, what we saw in Mr. Chong's case, testimony at the Hogue inquiry—it all points to the fact that the NSIA has not been sharing this information or is saying it's not important, especially when it comes to parliamentarians.

The position in the culture has been that we don't need to know. Guess what. We need to know.

The Chair: Thanks.

Hon. John McKay: I don't know whether we're really disagreeing here.

The Chair: Mr. McKay, I'm sorry. I've given some leniency here.

Mr. Duguid, you have five minutes.

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

I want to thank my colleagues for appearing today.

Mr. Chair, I'm not a veteran of this committee. I think I've been on since the session started in October. For about two-thirds of the time we've been focused on motions of privilege related to foreign interference. There are some very common themes. There's the lack of coordination, the lack of communication and, of course, members of Parliament not being informed, which, I think we all agree, has been totally unacceptable.

The other observation I've made is that this has become a very partisan issue. I was struck by one of the things said by Mr. McKay, the longest-serving member of Parliament around this table, who has served with distinction for many years—I'm not buttering you up, don't worry—which was that we really have to get beyond partisanship on this particular issue. This is about our country. This is about the safety of members of Parliament.

Mr. McKay, you may have heard the NSICOP chair, who did a number of interviews yesterday, when he lighted on this very theme. This is about the security of our country, the security of our decision-makers. This is bigger than any MP and bigger than any party. His suggestion was that the leaders of the major parties in our Parliament have to get together in a room. They have to put their heads together. They have to down tools on the partisanship. As we've been talking about today, they have to come up with solutions and protocols, obviously taking advantage of the Hogue inquiry.

I just wonder what your reflections are. I'd be interested in my other colleagues' reflections as well.

● (1150)

Hon. John McKay: Far be it from me to disagree with Mr. McGuinty on anything. I think he makes a valid point. I would add to the point, though.

Don't just defer to the leadership. Apparently, we're all adults here. We need to take care of our own security. I would be pretty upset if the leadership didn't take it seriously, but I'd be even more upset if we didn't take it seriously. This is a serious committee.

Ms. Mathyssen asked a very difficult question. I thought that Mr. Bezan started to disaggregate the answer to that question a little bit better than Garnett or myself, and that is the hard work that needs to be done here because this is going to keep on happening.

I honestly don't know where the protocols need to be drawn. I dare say, you want to put them in pencil or something that disappears because they're going to change about a week after you actually land on them. We need to take responsibility, and Mr. McGuinty's point is absolutely right. We need to take that.

Mr. James Bezan: Mr. Chair, I'd just add to that. To Mr. Duguid's point, there's definitely some of this that can be talked about at the caucus level, whether it's through party leaders, House leaders or whips, on the collective action, but there's still the individual privilege here as well and how we balance that off. It ultimately comes down to how we share information and the classification of that information.

When it comes down to cyber-attacks, we're not talking about intelligence and how that intelligence is collected. We're actually talking about a kinetic cyber-attack that has been documented and is known. Some of it may have been shared through Five Eyes partners, but the other Five Eyes partners—or other NATO allies, for that matter—have often taken action a lot quicker than us.

For the APT31 attack, in particular, Sweden knew about it right away and shared it with those who were targeted almost immediately, and there's one other European country that shared that information very rapidly.

I think that is a key point. We don't have to rest on our laurels and look at what other countries are doing. We need to be aggressive now, and we need to make sure that what we're doing is proactive in making sure that each and every one of us is better prepared and protected.

Mr. Garnett Genuis: Mr. Duguid, just as a brief comment in response to what you said, I agree about the importance of finding solutions.

I do, respectfully, though, sometimes notice that the calls to down tools on partisanship come immediately after a case of significant failure by the government. The government fails to do something they should have done, and then they say, “Well, let's down tools on the partisanship. Be nice to us.” Well, there need to be solutions, but there also needs to be accountability for the choices that were made.

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

[*Translation*]

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

Ms. Marie-Hélène Gaudreau: Mr. Chair, I'm going to pick up on what my colleague said.

Pre-emptively, since the Uyghurs and Taiwan are known, have you been contacted to be on the lookout? Do we have that here? Did you get that?

[*English*]

Hon. John McKay: I haven't been.

Mr. James Bezan: No, I am automatically careful. Domestically, though, I think we get a little more relaxed. When we're at home, we think we're all right. I've had burner phones hacked when I've been in Ukraine. We take extra protocols when we travel to Europe.

Lindsay, John and I were in Estonia last summer. We all had burner phones. We left our other phones and iPads and everything at home. When we were coming up to the Russian border at Narva, I even went as far as shutting off my phone and putting it in my safety bag. I put it in airplane mode before I shut it off. When we went to the border, we were filmed the whole time we were there by Russian border guards. When I got back on the bus and we were a good 30 kilometres away from the border, I opened up the bag, and my phone was on. It was out of airplane mode, and it was hacked.

Those types of attacks happen. I think all of us have stories like that when we're travelling. I had it happen when I was parliamentary secretary of defence back in the day as well, on a good old BlackBerry, but this is different. This is happening right here at home, so we have to be even more careful.

● (1155)

Hon. John McKay: I had a similar experience in Ukraine, where we just shut everything down. That's about the only thing you can do.

[*Translation*]

Ms. Marie-Hélène Gaudreau: I have a few seconds left.

Do you think we are sufficiently equipped, technically, even though we have Five Eyes models? We've heard about Australia, and we're somewhat embarrassed by the fact that the necessary changes haven't been made since 1984. Do you think we're well equipped in Canada?

[*English*]

The Chair: I'll let one witness answer quickly, please.

Hon. John McKay: That's a very difficult question and maybe not entirely relevant to this conversation.

If I looked at the bigger picture, I think Canada is a very sophisticated nation in our participation in the Five Eyes and various other cyber-issues. On this issue, maybe we're not so much.

[*Translation*]

The Chair: Thank you, Ms. Gaudreau.

[*English*]

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

Ms. Lindsay Mathyssen: To continue where we left off in terms of that conversation about the security clearance that we should all be receiving, Mr. Genuis, I think you said that we could talk about the systems and the failures, but there is a personal responsibility and people who make those choices put other members at a greater risk.

I am concerned, of course, about the larger context, the cloud that is now hanging over Parliament. A lot of parliamentarians have said this in relation to the NSICOP report. I'm concerned about how we build those processes and systems in order to deal with this larger cloud that we are all worried about in terms of our privilege.

As you also said, culture starts at the top. How do you apply that to your own leader who will not receive a briefing so that he could potentially be part of the solution?

Mr. Garnett Genuis: I'm happy to answer that. The nature of the requirements that would be associated with receiving that briefing is that he could not use that information in any way to do anything. If a person is briefed, and they are required as a condition of that briefing to tell no one, to action the information in no way, what possible action could be taken?

We have a law that applies to every party, although I'm not sure it is being used. The Reform Act requires every caucus to take a vote at the beginning of Parliament on a mechanism whereby caucus members could be involved in a decision about caucus membership. Let's suppose that a leader becomes aware that there's a concern. They cannot bring that issue to their caucus. They can't bring that issue to the national campaign director. They can't bring it anywhere.

What we need is a process for accountability, not a secret briefing with the condition that you can do nothing with the information. It's not effective.

Ms. Lindsay Mathyssen: It's interesting that you mentioned the Reform Act—

The Chair: You have about 30 seconds.

Ms. Lindsay Mathyssen: One of the former directors of communications for Stephen Harper, Kory Teneycke, said that the Reform Act being used as an excuse is a "false construct". He said that getting the briefing is "an opportunity to demonstrate leadership, and I think that they should welcome it".

Mr. Garnett Genuis: I think Kory is totally and completely wrong about that. Obviously, he can speak for himself in terms of his understanding of the Reform Act.

The Reform Act is very clear about how caucuses make decisions, and I would only say that I wish the Liberal Party had followed the law with respect to the Reform Act and taken those votes at the beginning of Parliament, because it's a concern if that law is not being followed.

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

Colleagues, that brings us to the end of our first panel. I want to thank Mr. McKay, Mr. Genuis and Mr. Bezan for joining us here today.

We appreciate your time, gentlemen.

Hon. John McKay: Thank you.

The Chair: We are going to briefly suspend to set up for the second panel, and we'll get going right away.

● (1155)

_____(Pause)_____

● (1200)

The Chair: Colleagues, we are going to resume our meeting.

We head into the second panel on the same topic.

We'd like to welcome the following members of Parliament, our colleagues who will be joining us for the second panel today. We have Mr. Kmiec of Calgary Shepard, Ms. Stephanie Kusie of Calgary Midnapore and the Honourable Judy Sgro, the member of Parliament for Humber River—Black Creek.

Colleagues, you will each have up to five minutes for an opening statement, and then we will head into a round of questioning no different from any other committee setting.

Witnesses, have you had an opportunity to discuss who may like to go first, or does someone just want to put their hand up?

Mrs. Stephanie Kusie (Calgary Midnapore, CPC): It's going in the order of the notice of meeting, for sure. That's how it should go. It should go in the order that it is in the notice of meeting.

The Chair: It can go in a variety of different ways.

Mrs. Stephanie Kusie: I think it's always good to follow the meeting notice.

The Chair: Mr. Kmiec, go ahead.

Mrs. Stephanie Kusie: That's fine.

Mr. Tom Kmiec (Calgary Shepard, CPC): Thank you, Chair.

I was trying to be a gentleman.

I've had the opportunity, now, to listen to the testimony given this morning in the first panel. I didn't hand speaking notes to the interpreters, so I'll speak slowly and will pause when I switch to French.

I'm going to repeat what I said in the House of Commons. I believe the Government of Canada had a moral and ethical responsibility to tell those 18 parliamentarians that we were targeted by a PRC special unit for a form of digital surveillance, including me. I'm one of them. I'm a member of IPAC. The Government of Canada failed in its moral and ethical responsibility to tell us.

I have six points I want to make based on testimony I heard. I want to refer to these.

The first part was during the CSE's testimony here about when they became aware. They said:

> ...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.

Based on this testimony, I have to assume it was APT31. I had no idea this was going on at the time. I also did not know what APT31 was until I was told on April 24—by my two co-chairs and the executive director of IPAC—that I had been one of the targets of this PRC campaign.

Since then, I have not had any type of contact directly from CSE or CSIS. I have heard, though, from the FBI. I had the same May 9 FBI briefing that other members received, detailing exactly what APT31 is.

Later, in testimony provided before the committee, the CSE's Caroline Xavier said, “I can confirm that when we became aware in 2021 of some anomalies”—it's interesting that she called them “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.”

She went on to detail this, saying:

> ...we did, indeed, share that list of parliamentarians with the House of Commons IT security team. We also shared it with CSIS.

When I became aware that I had been targeted, they responded to me with a citation on April 25. Here it is, as copied and pasted by the Sergeant-at-Arms: “For your records, we have been involved in investigation of this activity while it was ongoing, well before it was publicly disclosed.”

My staff followed up and asked the question, “Are you saying that the Sergeant-at-Arms office was aware and investigated this activity before, or are you referring to the House IT administration?”

The office of the Sergeant-at-Arms, or SAA, was not aware of this investigation. However, the HoC cybersecurity team, information service, IT administration, stated that they were involved in this investigation while it was ongoing.

I want to draw your attention to another piece of testimony in questioning by Mr. Genuis. In that, Ms. Caroline Xavier said, as part of those actions, “We provided 12 reports to the House of Commons.” This would have been since January 2021. Again, I am not aware of the contents of those reports. I don't have the benefit of the in camera sessions that members of this committee received, so I am at a disadvantage.

● (1205)

[*Translation*]

In response to a question asked by Marie-Hélène Gaudreau, Ms. Xavier said:

> 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.

You can't contact the Canadian Centre for Cyber Security at the Communications Security Establishment if you don't know it exists. This is the first time I've realized that there is such a service for parliamentarians. I was elected in 2015, and this is the first time I have heard about this service, which has been in place since 2019.

In addition, it is impossible to ask the government for help from the Canadian Centre for Cyber Security if you do not know that you are being targeted by a foreign agency as a parliamentarian.

[*English*]

In cross-examination and following up on questions asked by Ms. Mathyssen, Mr. Genuis raised the point that the CSE made the following observation in different rounds of questions: that government institutions need to respect the parliamentarians of the House of Commons. However, it's hard to feel respected by CSIS, the CSE or the House of Commons IT cybersecurity administration when they don't bother to tell us we are the targets of foreign campaigns and they don't bother to tell us we're targeted by foreign agencies.

I do a significant amount of work with diaspora communities among Canadians. I have people often tell me that they cannot be seen in a picture of me that will be posted online, so they jump out of the picture.

In my office I also have a Ukrainian flag signed by many of our UCC interns in past years, so I am sure that Russian Federation officials don't like it.

Lastly, I have protest pictures from Hong Kong brought to me by Albertans who were there. Hong Kongers who come and visit me do not take pictures in front of that with me in it.

Thank you, Chair.

● (1210)

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

Mrs. Kusie, you have five minutes.

Mrs. Stephanie Kusie: Good morning, colleagues.

On the morning of Thursday, April 25 of this year, I received an urgent message from my colleague indicating the necessity of a call as soon as possible. I was not alone on the thread, so the call was set for later that afternoon. The contents, once shared, were disturbing. Those present on the call had been the target of a cyber-attack by APT31, which is a hacker group set up by the PRC.

To receive this news is unsettling, to say the least. You immediately think of your most intimate transactions. It's impossible not to. Your thinking regresses backward quickly through all communications.

It's no secret that our electronic communications confer the most precious details of our lives: where we are, who we're with and what we're doing. One comes to Jesus quite quickly in these moments, which is rapidly followed by the crushing resentment of "how did this happen and why?"

I've never taken my stations for granted, as a member of Parliament or a former diplomat for Canada. I've recorded, in thorough detail with the authorities in the past, relationships where I questioned the motivation of those forming a bond with me. My triggers were always lavish gifts, suspicious backgrounds and a forced effort to create a closeness.

In 2021, after changing residences, I requested a sweep of my homes for bugs. I was informed by the authorities that these services were not available for those outside of the executive of government. I had a security assessment done in my home and the recommended security system installed, to the remark of a colleague who indicated that they could see who killed me after I was dead.

Do I desire the 24-hour protection of some of my colleagues? I'm very nervous about reaching that level of notoriety. Yes, I've been stopped in the vitamin aisle and in the deli section by those who recognize me, but this is, of course, another level.

The most disturbing aspect of this is having been informed by not even a second but third hand, so I'm very grateful to have run into Luke de Pulford at the inauguration of the Taiwanese president in Taiwan and to have thanked him personally for his intelligence and for sharing with us.

Despite our differences, I've also always had an affection for the United States, having done my master's degree there and having served as the Canadian consul to Dallas from 2010 to 2013. I'm not surprised that it was actually the Federal Bureau of Investigation that surmised this breach and informed IPAC, which then informed my colleague, who then informed me.

This does, however, not dismiss the pervasive and persistent disappointment I have in not being informed directly by the Canadian government. As a consul, I felt a keen guardianship for all Canadians in my host region. I wish the Canadian authorities reflected the same sentiment in informing me about my violators. I can only deduce that they did not.

My sense of disappointment is overwhelming. The fear that consumes you when you think about the possible effects on you and your family, you try to push it out of your head, like a tooth your dentist says needs to be pulled at a later date. As a legislator, you consider what needs to be done to protect you and those around you, as well as your colleagues. You take this path knowing that a part of your life is not your own, but this validates it in a manner far more vast than you would like to consider.

In closing, I believe in evil and not just in the biblical sense. I believe in malice in the hearts of men—those who wish to intentionally inflict harm upon others. One need only refer to Navalny or the 37 murders in the republic of Mexico in the most recent elections. I'm not talking about someone saying I'm hot or not online—I have thicker skin than that—but about the potential for real harm to me or to my loved ones.

This attack appears on the surface to have been minimal in impact, but it indicates a far greater concern that someone is watching. They want to know what I'm doing, who I'm meeting and where I will be.

Evil, when confronted, will always try to realign, but the tactics are always the same: divide, conquer, intimidate and extort. These micro-acts of aggression are the genesis of the foundation of intelligence-gathering. The reality is that what you don't know can hurt you.

Thank you very much.

The Chair: Thank you very much.

Ms. Sgro, you have five minutes.

● (1215)

Hon. Judy A. Sgro (Humber River—Black Creek, Lib.): I won't take five minutes.

Thank you very much for hosting this study. I'm grateful for your doing it because it's the first time I've talked to anybody about this issue. This is two months later, and that's unacceptable for sure.

Going back, yes, I was furious. I was livid when I got the call from IPAC. We had a joint conversation, as my colleagues have already indicated. The anger left, but then I was left with a huge disappointment, as my colleagues have said. This is not what I would have expected. More importantly, you know, it happened. The firewall held, and because of that, they felt there was no reason to tell us. Well, I want to know.

All of us on this panel do a lot of human rights work, and we take on some pretty hot topics in the House of Commons and outside the House of Commons. I think the intent of a lot of this is to intimidate all of us so that we will stop standing up on behalf of people who don't have a voice. I think that a big, important part of our job is not just to represent our local constituents but also to be a voice for those who are voiceless. It's because of members of Parliament that some of the progress we are seeing in different files is happening, whether it's the Tibet file, the Iran one or the Taiwan one, of course. It's because members of Parliament had the courage to stand up and be counted.

Yes, they did this and we didn't get notified, so let's move on. What did we learn from this? I think I always try to figure out what good comes out of a negative situation. My anger is gone, but my disappointment is still there. My hope is that we are going to use this as an opportunity to put down the when, how and where. My hope is that all of us become much more aware of the threat that we could be under and take more responsibility, ourselves, to make sure that we are protecting our systems. I'm told that turning them off once a week helps to eliminate any viruses or anyone trying to access them. That's a very simple thing. No one's ever told me that in the many years I've been here. However, we need to get serious. We need to, with your help, put a plan in place.

I mean, I didn't even know who to ask about any other damage that might have been.... I had no idea after all the years I've been here. I know the Sergeant-at-Arms is there, but I had no idea where to go, who to ask or how to better protect myself. I think those are things about which we are all or we have been, until now, extremely naive, but based on recent conversation with CSIS and others that I asked for.... There is AI that can clearly reproduce me at another meeting a half an hour from now that I'm not at, but it could look exactly like me with this AI business going on.

I think we are under much more threat now than we've ever been previously, and we need to figure out how to do that. How are we going to protect each other? What's the role and who puts what into place? It needs to be more public. I think our Liaison Committee should also report once a year at minimum, along with all the other reports, on how many cybersecurity issues there have been and that kind of issue. We need to become more knowledgeable, and you have the role of coming up with those suggestions.

I think there needs to be much more emphasis put on parliamentarians being respected, as my colleague mentioned. Thinking that we're dispensable and that, therefore, they won't bother to tell us that there has been something on social media attacking us—that if we don't know ourselves, they're not going to tell us.... Well, their job is to make sure that we are protected. When we talk about trying to get more people to run for public office, if they're going to run for public office, we have the responsibility, at least, to make sure that they have all the tools necessary to be protected so that they and we can do the jobs that we all want to be doing here.

Thank you very much.

The Chair: Thank you, Ms. Sgro.

Colleagues, we will enter our first round of questioning.

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

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

Thank you to our witnesses for being here.

I'll build on what you've said in your intros and the first hour with our other colleagues who were here. Maybe I'll just lay the groundwork here a little bit.

In the aftermath of your becoming aware—and its becoming public knowledge—of the threat and what happened or, frankly, what didn't happen in terms of your being notified, have any of you three on this panel had any conversations or exchanges since this came to light with the PCO, the Prime Minister's Office, the Minister of Public Safety or the department about exactly what happened? Did they ask for your feedback or suggestions on how this situation can be avoided in the future?

I'll ask you to answer if you have been in contact with any of those aforementioned groups or departments.

● (1220)

Hon. Judy A. Sgro: No, I have not.

Mrs. Stephanie Kusie: I have not, but it stems from having formerly been the shadow minister for democratic institutions. From that time, I fundamentally believe the government wasn't acting enough on foreign interference, which I believe is inextricably tied to our protection and cybersecurity as parliamentarians, and that's after at least six interactions with the former minister of democratic institutions as well as speeches that I gave in the House.

As well, the toothless digital charter was another sticking point for me of 2019.

So, no, but I think it's because, if nothing has been done until now, it just felt pointless to me.

Mr. Tom Kmiec: No, I've had no contact whatsoever. The only people who reached out were the FBI in the May 9 briefing.

Mr. Eric Duncan: That is helpful.

Where I want to go with this is that there's a protocol problem, clearly, but I think the bigger issue here is a culture problem. There are protocols in place right now that officials thought would inform parliamentarians, and that hasn't happened. There's a bigger issue here of a culture that comes from the PCO, the PMO and different agencies that just frankly, I felt, were careless in assuming somebody else would look after it, so there was no proper follow-up.

I want to ask each of you for your comments on the culture that's out there of not doing that follow-up and not making sure that people who are actually being threatened are being informed in a timely manner, provided the proper resources and so forth. Then maybe in your response you can talk about what needs to change and who is responsible.

On the disappointment Ms. Sgro mentioned—which you still have—who's that disappointment with in terms of where the responsibility lies?

Mr. Tom Kmiec: Chair, my response to that would be to repeat something Judy said.

I believe that the government sees us as disposable, because we're members of Parliament. We come and go, which is the way our system is supposed to work. Especially for us backbenchers, I think there is this culture in the agencies and government in general that because we're temporary, we're temps—to use a term that I sometimes read in my ATIPs from civil servants. They know we'll leave and think that we're infinitely disposable. I think the government had a moral and ethical responsibility to tell us, to go straight to the top as soon as they knew.

Just tell us—that's the answer. I can take care of myself. I can then go and ask CSE for the cybersecurity centre's help. I can then go and ask the Sergeant-at-Arms for help. I know what I can do, but if I'm not told, I can't do anything if I don't know.

Mrs. Stephanie Kusie: I think it's a coordinated naïveté amongst all authorities. Historically, we've moved into another era, I'd say, even more recently—I'd even say on a weekly or monthly basis. However, I fundamentally feel—and I'm sure I'll be challenged on this—that it's because of an indifference in the current administration, and this leads to incompetence in the rank and file of those who are in charge of our safety. I fundamentally believe this.

Hon. Judy A. Sgro: I think for many years we have all been naive, whether we're parliamentarians or we are people who work in a whole lot of different areas. Canada is just waking up to issues of foreign interference and all the rest of it. This is a new era, and I think everybody's been naive and not realizing. I don't think anybody intentionally held anything back that they thought would hurt us. The firewall held—hallelujah. We're supposed to be really happy. The firewall held when we had this APT31 attack. That's what I was told. We should be glad.

Well, I am glad that it held, and I am glad that we're here, because we're going to find a way to better protect parliamentarians and Canadians as we move forward as a result of this.

Mr. Eric Duncan: Where I'll go with that, the culture of secrecy and I think disrespect of parliamentarians, is that since other questions of privilege and other issues started to come to light, multiple directives were issued to actually improve the process and say that parliamentarians must be informed. Even after those directives were issued, parliamentarians still weren't informed.

My point about the culture is that the protocol, that directive, was given to improve the process, and it was literally ignored with every excuse in the book as to why.

I'll just talk about the culture, Ms. Sgro. It's new and maybe we've been naive, but to me, it's the culture of taking any protocol or directive seriously and improving that. We've seen examples of that said, but not followed through on.

I'd appreciate hearing from anyone who has comments on that.

● (1225)

The Chair: We'll have one witness very quickly, please.

Hon. Judy A. Sgro: I would just add that when we had our discussion with the FBI and with IPAC and we challenged why were we not told, we were told that the way the system is the FBI had to report to one particular person within the Government of Canada. They could not come directly to us. Several weeks after that, the FBI actually had a briefing with all of us. They said there was a system in place that the FBI could not directly inform us. It had to go through a bit of protocol that was in place that nobody seemed to follow.

The Chair: Thanks very much, Mr. Duncan.

Mrs. Romanado, you have six minutes.

Mrs. Sherry Romanado: Thank you very much, Mr. Chair. Through you, I'd like to thank my colleagues for being here.

I'll premise this the way I did with the last panel. I firmly believe that all of you should have been told. It's very unfortunate that you weren't.

Just to pick up on that, Mr. Kmiec, you mentioned that you had a meeting with the FBI, I think on May 9, but you mentioned that you have not met with CSIS or CSE. Have you met with anyone since this has come out? Has anyone, whether they be from CSE, House of Commons IT or CSIS, sat down with you?

Mr. Tom Kmiec: No.

Mrs. Sherry Romanado: Mrs. Kusie, in your case, has anyone met with you?

Mrs. Stephanie Kusie: No. I'll just leave it there, Mrs. Romanado.

Mrs. Sherry Romanado: Ms. Sgro?

Hon. Judy A. Sgro: CSIS...at my request.

Mrs. Sherry Romanado: You actually had to request the meeting.

Hon. Judy A. Sgro: Yes.

Mrs. Sherry Romanado: Obviously, the protocol is not working. The fact that you had to proactively reach out yourself is an issue.

When CSIS and CSE were here, I think there was a fundamental misunderstanding about what MPs actually do. I'm not an intelligence officer. I would not know what they do, but there really is a disconnect, I think. They don't realize, as Ms. Sgro said, that the work we do puts us more at risk in terms of interest from others, whether they be state actors or non-state actors. We never want MPs to change what they're doing. We want them to continue to do what they're doing, because it is important work, whether it be here in Canada or abroad or standing up for human rights.

What would you recommend that this committee put forward in terms of making sure that intelligence agencies and those who are asked to protect us, whether physically or in the virtual world, understand what we do and how we do it? What would you recommend that we recommend to them?

That's for any of the witnesses.

Mr. Tom Kmiec: Chair, I'll go ahead and give that a shot.

The first thing is that these agencies need to have a positive requirement on them to inform parliamentarians. What I don't want to see is what I've now experienced, where the Sergeant-at-Arms office says that HoC cybersecurity knew but the Sergeant-at-Arms office didn't know. Then they come here and everybody says someone else was told to tell someone. It's unclear to me. Again, you have the in camera discussions that were had. I note that CSE kept saying that they could answer some of those questions in camera.

I need to know. I need to know whether I'm a target. It will change the way I do my work, because it's already had an impact on my work. When I have people reach out to me who want to meet with me, if you Google my name, this is one of the things that will come up, so some people, some dissidents and journalists in exile, will self-censor. They will not reach out to us. If I email him, if I contact him on his social media, that might be tapped. That might already be compromised by a foreign agency.

There is public information showing that these foreign agencies have an interest in me for the work that we all do here. Because of that, it's already had an impact on the work I can do.

Thank you, Chair.

● (1230)

Mrs. Sherry Romanado: Thank you. That's a really good point. What we're looking at is not only the question of privilege but also the question of who's responsible for making sure MPs know. Throughout this study, we have not had a clear indication. Everyone, as you said, says, "Oh, it's their responsibility, or it's their responsibility." We want to correct that, obviously.

You also mentioned something about how it's changed the way you do the work that you do. That is very concerning to me. The reality is that every single one of us has different roles that we play and backgrounds and so on. In certain ways, we're all targets for different state and non-state actors.

In terms of the protocol, we have a ministerial directive that, as I understand from the last meeting, has only been directed to CSIS, not to CSE and not to the House of Commons IT. Would you recommend that the ministerial directive be elaborated?

Ms. Sgro.

Hon. Judy A. Sgro: Absolutely, if that's what's necessary. You would think it wouldn't have to be necessary, but it appears that it needs to be a ministerial directive, so start with that. They have to have that directive. They have to share the information with parliamentarians.

I think it's hard to believe that all of the folks involved in protecting us don't know, to Mr. Kmiec's issue, what we're really doing and that we are dealing with a lot of foreign issues and all these other things. Is it possible that they don't know the extent to which many of us are venturing into areas that seem to be areas that upset China, Iran and so on and so forth?

I can't believe that they're not aware of it. Maybe they should spend some time with parliamentarians or watch what goes on in the House of Commons a little bit. Maybe it would change things.

Mrs. Sherry Romanado: I have only 15 seconds. Again, I want to thank you for coming forward today and giving us the feedback you have, because we do have to fix this.

[*Translation*]

The Chair: Thank you.

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

Ms. Marie-Hélène Gaudreau: Mr. Chair, I can honestly see that this is a very relevant meeting today. I don't sense much of the usual partisanship. We're really talking about the problem.

I would like to go back over what happened. I heard what you said about the need to take charge of this and get ahead of it.

I asked this question. One day, there will be another government. Is it normal that trust is no longer there? When we met with the representatives of the Communications Security Establishment, I raised my hand and said that, since I'm not currently their client and they do business with the government, I want to be their client.

I would like to hear your comments on that. What do you think about getting this out? It's part of our lives, being an MP, it's 24 hours a day, seven days a week. What do you think about that?

Mrs. Stephanie Kusie: I think it's necessary to assess the system as a whole. We have to think about the threats. In my opinion, it's important to better inform parliamentarians and members of Parliament, because right now, it seems that there's a lack of a system for analyzing threats. You have to look at the whole system, but you also have to look at the threats against individual members. I think threats against members are different, depending on the activities of the member.

As I also said, it's really important to have transparency and training. I think training is really important for members of Parliament. Personally, I want to see a complete review of the system so that there are more threat assessments, more transparency and more training.

Ms. Marie-Hélène Gaudreau: I just want to make sure, because I may have missed the beginning of your opening remarks. Were the attacks on your personal accounts? Yes or no.

Mr. Tom Kmiec: I was going to say that, in my case, it was on my public account that I use. I have the three emails with me today. I printed them off, because they're still in my account. I can open those emails at any time.

However, in the cybersecurity system, no one told me whether or not I could open emails. So I opened them and printed them off, all three of them. They're still in my account. No one told me I couldn't do it. As far as I know, the digital surveillance technique for these attacks works with pixel spies. Since this is a new topic for me, I did a Google search to find out, with the help of my staff. It's all described perfectly.

In my case, it affected my public email account. My staff in my constituency office and my staff in my Hill office have access to these accounts to assist me in my work. Every single one of those computers could have been affected by these attacks because of a lack of training, which should have been given to me.

● (1235)

Ms. Marie-Hélène Gaudreau: Was that your personal account, Ms. Sgro?

[*English*]

Hon. Judy A. Sgro: It was my House of Commons account altogether.

Can I just take it somewhere else, following on the earlier question of what we can do?

You know, this is June, and we're learning a whole lot. I would hope that, when the House comes back in September, there is a very significant presentation on security issues to all parliamentarians, and one so that we would start the session with—

[*Translation*]

Ms. Marie-Hélène Gaudreau: I'm going to stop you there, because my time is limited.

In fact, I don't know about you, but our caucus was briefed by the Canadian Security Intelligence Service. It is becoming a necessity, but yes, I'm very concerned about parliamentary prevention.

Were you in the same situation?

Mrs. Stephanie Kusie: More or less, I'd say. I have three accounts. The first is stephaniekusie.mp; the second is my MP personal account, my .p9 address; and the third is a Gmail address. In my case, it was the account with the least sensitive information, but it was a window to accessing the other accounts. That's what bothers me the most.

Ms. Marie-Hélène Gaudreau: That's correct.

I have another question. Earlier, I was explaining my annoyance with the fact that I, someone with no qualifications in espionage, found an article on the web on December 15, 2021, explaining the APT31 attack campaign. There are newspaper articles, including the one from May 12, describing what was requested during the visit from representatives of the Communications Security Establishment, who gave us nothing in the way of information. We've learned nothing.

That being said, and I'll close with this, there's an MP—it's in Le Monde—who said she intended to file a legal complaint, because she's experienced exactly what you have. On that, in your situation, where do you stand on this? Are you angry enough to get things moving?

Mr. Tom Kmiec: Personally, I wasn't angry when I found out that I was the target of this type of attack by a foreign agency. I was disappointed that my government didn't think it was worth telling me or protecting me.

[*English*]

The Chair: Okay.

[*Translation*]

Thank you very much.

[*English*]

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

Ms. Lindsay Mathyssen: Thank you, Chair.

Thank you to all three of you as well for joining us today and sharing this experience with us.

In the last round, I was talking about the fact that this institution and parliamentarians overall would get millions of hits. I'm a little concerned and I worry about how, when CSIS and CSE were here, they talked about the fact that—and I think House of Commons administration said—they regularly provide parliamentarians with general warnings and that they thought that was enough in terms of understanding what foreign interference or a cyber-attack would be. We also talked about personal responsibility and what that means to the individual MP. We just talked about the fact that we were briefed by CSIS this week at caucuses.

Ms. Sgro, you were talking about the need for those briefings. What do you want to see far beyond that in general? I know it would probably be overwhelming for members of Parliament if they were briefed on every single attack that was put forward, but what do you see those briefings looking like? Would they be quarterly, because that information changes so quickly?

Just give me an idea of what you're thinking on that.

Hon. Judy A. Sgro: I think we have to stop not talking about it, and we have to start learning more about it and how many threats there are. Again, it depends on the category of threat that is there as well.

More knowledge needs to be shared. Things are moving so quickly that, even if we had a briefing a year ago or six months ago, by the fall, things will have moved again very quickly. We have to make sure we are staying on top of it. We're all busy. I don't even look at the social media. I don't go on it. I don't care what they say. Let them do what they want, because I'm going to do what I need to do.

However, when the category of threat reaches a certain point, I rely on somebody getting in touch with me and saying, “You know, what you said last week has generated this particular threat.” Just let me know. I will handle it accordingly. I think it needs to be frequent. With the way things are moving so quickly, I don't think doing this once a year or once every three years at the beginning of a new Parliament is enough.

● (1240)

Mrs. Stephanie Kusie: I've had the pleasure of visiting the majority of threatened democracies in the world, except Ukraine. That's the one that stands out. When I was in South Korea, they had a digital map of cyber-threats in real time. In this day and age, I don't see why we can't be informed about this in a daily report or even an attack report. The technology is there, in my opinion, and we are able to intercept or to view and intercept the attacks. I believe we should be receiving far more information because the technology is there. I think we have a right to know.

As I said, those of us who are more involved in pro-democratic, pro-human rights activities will certainly have more. I think the government has a responsibility to protect us when we are doing that work.

Mr. Tom Kmiec: Thank you for the question.

My view is that these generic briefings or emails we receive that tell us not to open an obvious phishing scam by email, and there's that “phishing” button.... I have never used that button in 20 years of using Outlook, so I can't tell you what it does. I just know not to open the email. It's obvious to me.

I know my colleagues here. I know that Mrs. Kusie is very involved with Cuban exiles who are fighting for freedom in Cuba. I know that Ms. Sgro shares my interest in a free Iran and she leads one of the different parliamentary groups. When there are specific attacks on us by foreign governments or foreign groups, we should be told in the moment, instead of getting these generic quarterly briefs or as they happen when there's a phishing attack on Parliament Hill on our emails. That's not useful.

I will praise one group: the ParlVoyage people, who give us the burner phones and inform us on what to do and on the security-level threats. When I travelled to Iraq last year with a parliamentary delegation, they were excellent. They told us exactly what was reasonable, what was unreasonable and how to be digitally secure as you're travelling through different airports.

Outside of that, like I said, nobody from CSIS, CSE or any of the other alphabet soup agencies has come to talk to me, except for the FBI, to tell me and to explain to me what I could do to be safer and to provide actual, technical, usable things.

Ms. Lindsay Mathyssen: Thank you.

The Chair: You have one minute.

Ms. Lindsay Mathyssen: Ms. Sgro, I wanted to focus on you and thank you for being a chair for the Canada-Taiwan Friendship Group and all your work on that. I travelled to Taiwan as well. We heard their perspective in terms of how they deal with millions of hits by China every day as well.

They have put forward a specific minister of digital affairs. Is that something that Canada should replicate? Do you have other ideas from your many trips and learning from them where we could go?

Hon. Judy A. Sgro: I found it fascinating to see the thousands and thousands of hits they get on disinformation every single day. They have four people whose job, 24 hours a day, is to monitor the system—that's all they do—and put out corrections to the disinformation that is being fed into the networks that are out there. I think we have a lot to learn from them in that particular area where they're dispelling disinformation.

I think cybersecurity—the whole thing—needs to be taken much more seriously as we move forward.

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

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

Mr. Blaine Calkins (Red Deer—Lacombe, CPC): Thank you, Chair.

I want to differentiate because I think there have been attempts to conflate so many attacks with the incident that happened in this particular case. We're dealing with phishing here. This is a different thing altogether. This is not a denial-of-service attack. This is not a cyber-attack. A phishing attack is a personal attack, because the vulnerability is at the human level.

I'm fully convinced that our technical experts.... I actually did IT work in a previous life. I'm so outdated now that I wouldn't know some of the new things they're doing.

The difference here is that it involves a human being making an error. That's how they do it. We can actually thwart most of the cyber-stuff. We can thwart denial-of-service attacks. We can thwart all of these things that attack the technology. However, this is an attack whereby the vulnerability is one of us clicking on something that we ought not be clicking on.

The difference in this particular case is that it was serious enough.... It was not just somebody looking to try to scam us out of some money. It's not the Nigerian prince type of question. This was serious enough because it was from a hostile foreign state actor, or considered to be a potentially hostile foreign state actor, directly targeting a group of us—18 of our colleagues—with this attack.

The frustrating part for me is that our job and our primary responsibility.... We're not in the sausage grinding of government. We're actually very nimble people. We're much more nimble than Monday to Friday, nine to five. If we're going to be able to do our jobs, we need to know what's going on. If we're not informed....

I think it's absolutely embarrassing for a country that 18 parliamentarians basically found out because the FBI released this. It is different from a cyber-attack. It's different from all the other random stuff that our emails might get hit with. This is hostile activity meant to do something subversive or damaging to individual members of Parliament and, thereby, the entire institution and our democracy at the root level.

If we're not told about something this specific.... The FBI thought it was important enough. It seems to be able to sort out cyber-attacks, denial-of-service attacks, other infrastructure attacks and other random phishing or malware attacks. Why can't Canada do this?

How are we supposed to hold our government to account if we don't even know that something is happening?

I'm looking to you three to say something that would give this committee some direction about this. What do you think would have been, to the best of your knowledge, a more appropriate way for you to find out? What would have been a more appropriate timeline for you to find out in?

The only reason we're talking about this is because somebody else tipped us off.

● (1245)

The Chair: Mr. Calkins, you have about 90 seconds left for the witnesses.

Mr. Blaine Calkins: I'll leave it at that. I know it's a very open-ended, general question, but....

Hon. Judy A. Sgro: If IPAC hadn't told us, we wouldn't know today. It took that organization, which has nothing to do with Canada, to reach out to us and let us know, or we wouldn't have known.

I go back to the disappointment. We, parliamentarians, need to know when there's been a threat levelled against us. We need to know. That doesn't mean six months from now. If I got a threat today, based on what I said yesterday, I wouldn't even know where to go. I know I'm going to go to the Sergeant-at-Arms, but then what?

We need to know what to do when we receive something that we think is a serious threat, what not to do and where to go.

Mr. Tom Kmiec: Thank you for the question.

I'll add that the Government of Canada needs to treat our digital security like the House of Commons treats our physical security. I feel safe around the parliamentary precinct because I know there are enough PPS officers around, who are actively managing the security of the area.

On digital security, I'm sure they can shut down our emails and keep our files safe, whatever device that they're on, but when the CSE found out that this was APT31.... These aren't basement goons. These are men and women for whom there is a $10-million reward by the U.S. State Department for information leading to their arrests. This is an active foreign intelligence unit that was used.

As soon as that was found out, there should have been a positive responsibility on the part of CSIS, the CSE and all of the alphabet soup agencies. Don't send me an email. Call my office. Contact me directly. Tell me I'm a target. Tell me why I'm a target, if they know, because I would like to know.

On the phishing stuff, I entirely agree with you. People go through that in their private life and businesses, but being targeted by a foreign intelligence service is new.

● (1250)

The Chair: Thanks very much.

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

Mr. Ken Hardie (Fleetwood—Port Kells, Lib.): Thank you, Mr. Chair.

Thank you for the information that we've had this morning.

NSICOP, of course, came down with a report. Evidently, as we've learned, some people are named in that report. It is based on intelligence that surfaced during a variety of work done by our agencies.

I want to pull it back to the issue of privilege. There's been a lot said about whether we should divulge the names of those people to the world. Should we perhaps think about ways of divulging the names of those people to those people? Is that a question of privilege?

I'm just asking for an opinion here. You don't have to be encyclopedic or well read on the whole issue, but what do you think?

We'll start with you, Mrs. Kusie.

Mrs. Stephanie Kusie: Absolutely, I think that's the first step. I think that they should be divulged to the world, as the position of my party and my leader as well. It absolutely should be divulged to them. I know I constantly do an inventory—

Mr. Ken Hardie: We'll ask for a fairly short answer to that one, because I have a lot of questions.

Mrs. Stephanie Kusie: Yes.

Mr. Ken Hardie: What do you think, Ms. Sgro?

Hon. Judy A. Sgro: I think that they should know that they are named in a report of concern, but certainly they should not be publicly released.

How could you throw out anybody's name?

There's a lot of innuendo in that report and so on and so forth, but there's no proof. There's lots of possible intelligence and all of that. You could not turn around and throw out Ken Hardie's name as being in that report as a person who's possibly working contrary to Canada.

Mr. Ken Hardie: I'll have something to say on that one in a second.

Go ahead, Mr. Kmiec.

Mr. Tom Kmiec: Chair from the Canada-China committee, I'm glad to see you here.

I'm going to draw your attention to page 66 of the NSICOP report, “Engagement with Parliamentarians”. To answer your question in brief, I just want to quote this part and say, yes, those names should be released. It says here in paragraph 162:

> It did so because Parliamentarians are often at the center of interference activities by foreign states. While the Committee recognizes that CSIS has provided briefings to some members of Parliament, a comprehensive briefing strategy covering all Parliamentarians was not implemented despite PCO seeking the Prime Minister's approval on two occasions.

It goes straight to the top.

Mr. Ken Hardie: Right.

There's some character running around Surrey right now who's identified as a proxy for India. He's telling everybody, including the reporter that I spoke to last weekend, that he and I are just like this. That's not the case. I wouldn't doubt that my name is in that report just based on that. I would deserve to know, even if it's just private, because I think it's a matter of privilege.

Mr. Kmiec, I have to compliment you on the work that you have done on the Canada-China committee. You've been in the thick of a lot of very interesting testimony and commentary.

We know that China is very persistent. They play the long game. APT31 is one thing, but I'm concerned about the cumulative effect of APT31 on top of what the United Front does on top of all of these other things.

Do you care to sort of gather all of that and comment on what we should be looking at here?

Mr. Tom Kmiec: I'll try to keep it as brief as possible.

I agree in general. There are many different APTs out there, as I've discovered with my staff. When you do a search of it, there are multiple units. This is the thin wedge of the sword that the PRC wields. As you know, Chair, we expect that a lot more of these types of activities in the future, entire campaigns that will be led against western democracies and against legislators. In many cases, legislators are seen as the weak point in the government because you typically don't have the help of the agencies.

I'll draw your attention to the statement made by Belgian legislators, who said that they equally were not told by their government that they had been targets of APT31. In their case, they said there was a direct attack on their democracy and on their Parliament for their government not having told them, and they expect other attacks by PRC entities and agencies.

I will say that, since 2012 when Xi Jinping took over, the United Front Work Department has basically become a state security apparatus that operates in all western democracies, and we should be paying serious attention to all of their subentities like these APT31-type groups.

● (1255)

The Chair: That's about it, Mr. Hardie.

Thank you.

[*Translation*]

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

Ms. Marie-Hélène Gaudreau: I'll just go back, Mr. Chair. I note that what I've found, which is from the Agence nationale de la sécurité des systèmes d'information de la Republic française, is our Communications Security Establishment. When we met, we were expecting some details.

I'm telling you: go get it. Inside, there's the entire chain of infection—it dates back to 2021—intrusion vectors, invasion methods, victimization, infrastructure, targeted equipment and the back door, for example. It's all there; it's been available since 2021. I invite you to read it. We will be vigilant.

I have just one question. Is your privacy affected? If so, are your families worried?

[*English*]

Hon. Judy A. Sgro: They are, but that's as far as it goes. I said to not worry; I'm well protected. I said don't worry; that's just the way it is.

[*Translation*]

Ms. Marie-Hélène Gaudreau: It's unacceptable.

Mrs. Stephanie Kusie: My husband and I basically accept the situation because, given the life we live, we have no privacy. That's more or less the truth. It's a little more complicated for my son because he's young. He's afraid, he thinks about things like nuclear war. He's worried about us and whether it's dangerous for us. Obviously, we have to continue to live, knowing that the threats exist.

Mr. Tom Kmiec: On a daily basis, the answer is no. My three children know that I travel and take pictures. Those of my children who are allowed to have an account follow me on social media. I don't actually take my children to many public events.

However, I worry about the fact that my children are part Chinese and part Jewish. When I see street protests and anti-Asian racism, I have concerns about our country's culture and the harmful effects that these kinds of campaigns, led by foreign agencies against us, will have on our culture and our society.

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

The Chair: Thank you, Ms. Gaudreau.

[*English*]

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

Ms. Lindsay Mathyssen: One of the reasons we were given at this committee that MPs within the IPAC group were not informed was that there was an active investigation under way and there was a belief that it might become public, which would interfere with any further investigation.

Do you accept that as a reason?

Hon. Judy A. Sgro: No.

They know how to run their part of this operation. We're parliamentarians, so we don't necessarily understand their rationale, but it doesn't make any sense to me. Don't try to protect me. I can protect myself, but I have to know if there's a serious threat out there. I want to know. It's probably not going to change much, but I want to know if it's serious.

I can't see the rationale for not sharing that information.

Ms. Lindsay Mathyssen: In terms of what Mr. Hardie was asking, I do worry in terms of.... I'm not on one side or the other about whether we release the names or not. I see the harm in terms of that court of public opinion. We work in very public jobs, as we've just said.

What does that do to a parliamentarian? In my estimation, intelligence isn't always evidence. For that investigation, how do we allow that to happen, if I can merge both questions?

● (1300)

Mrs. Stephanie Kusie: We have to fix the system. That's a real, serious problem, if intelligence isn't evidence.

This goes back to my initial point of what I perceive to be a naïveté and the necessity to revamp the entire system. As I said, I believe it's a result of naïveté. I believe it's a result of indifference, inaction and incompetence.

It shouldn't be that way. We should be able to trust what's in the report. That's a huge problem. I really hope—whether it's this government or another government—that it can be addressed so that, when something is published, we can have confidence in it.

If not, what does that say about us as a nation, that we can't even have faith in the information within what is supposed to be the most sound and most sensitive report? I think that's a pretty sad statement. I hope one day to live in a state where we can trust a report such as that and the information within it.

Thank you.

The Chair: That's about it, Ms. Mathyssen.

Mr. Kmiec, if you have a quick response, you're welcome to go ahead.

Mr. Tom Kmiec: Thank you, Chair.

My only response would be to go back to the very beginning of my statement and what I said in the House of Commons. The Government of Canada, when dealing with legislators, has a positive responsibility to tell us. We had a need to know. It had a moral and ethical responsibility to tell us, and it failed.

The Chair: Thank you very much.

Mr. Kmiec, Mrs. Kusie and Ms. Sgro, thank you very much for joining us today. We very much appreciate your reflections.

Colleagues, I think we've had another set of very productive and insightful meetings. Thank you for your co-operation today.

The meeting is adjourned.