



Public Inquiry Into Foreign Interference in Federal
Electoral Processes and Democratic Institutions

Enquête publique sur l'ingérence étrangère dans les
processus électoraux et les institutions démocratiques
fédéraux

Public Hearing

Audience publique

**Commissioner / Commissaire
The Honourable / L'honorable
Marie-Josée Hogue**

**VOLUME 21
ENGLISH INTERPRETATION**

Held at:

Library and Archives Canada
Bambrick Room
395 Wellington Street
Ottawa, Ontario
K1A 0N4

Tuesday, September 24, 2024

Tenue à:

Bibliothèque et Archives Canada
Salle Bambrick
395, rue Wellington
Ottawa, Ontario
K1A 0N4

Le mardi 24 septembre 2024

INTERNATIONAL REPORTING INC.

<https://www.transcription.tc/>

(800)899-0006

II

Appearances / Comparutions

Commission Lead Counsel

Shantona Chaudhury

Commission Counsel

Gordon Cameron

Erin Dann

Matthew Ferguson

Hubert Forget

Leila Ghahhary

Benjamin Herrera

Howard Krongold

Hannah Lazare

Jean-Philippe Mackay

Kate McGrann

Emily McBain-Ashfield

Hamza Mohamadhossen

Lynda Morgan

Siobhan Morris

Annie-Claude Poirier

Gabriel Poliquin

Natalia Rodriguez

Guillaume Rondeau

Nicolas Saint-Amour

Daniel Sheppard

Maia Tsurumi

Commission Research Council

Geneviève Cartier

Nomi Claire Lazar

Lori Turnbull

Leah West

Commission Senior Policy Advisors

Paul Cavalluzzo

Danielle Côté

III

Appearances / Comparutions

Commission Staff	Annie Desgagné Casper Donovan Hélène Laurendeau Michael Tansey
Ukrainian Canadian Congress	Donald Bayne Jon Doody
Government of Canada	Gregory Tzemenakis Barney Brucker
Office of the Commissioner of Canada Elections	Christina Maheux Luc Boucher Sébastien Lafrance Nancy Miles Sujit Nirman
Human Rights Coalition	David Matas Sarah Teich
Russian Canadian Democratic Alliance	Mark Power Guillaume Sirois
Michael Chan	John Chapman Andy Chan
Han Dong	Mark Polley Emily Young Jeffrey Wang
Michael Chong	Gib van Ert Fraser Harland

IV

Appearances / Comparutions

Jenny Kwan

Sujit Choudhry

Mani Kakkar

Churchill Society

Malliha Wilson

The Pillar Society

Daniel Stanton

Democracy Watch

Wade Poziomka

Nick Papageorge

Canada's NDP

Lucy Watson

Conservative Party of Canada

Nando De Luca

Chinese Canadian Concern Group on
The Chinese Communist Party's
Human Rights Violations

Neil Chantler

David Wheaton

Erin O'Toole

Thomas W. Jarmyn

Preston Lim

Senator Yuen Pau Woo

Yuen Pau Woo

Sikh Coalition

Balpreet Singh

Prabjot Singh

Bloc Québécois

Mathieu Desquilbet

Iranian Canadian Congress

Dimitri Lascaris

V

Table of Contents / Table des matières

	PAGE
M. DAVID VATCHER, Affirmed/Sous affirmation solennelle	1
Mme JULIE LACROIX, Affirmed/Sous affirmation solennelle	1
Examination in-Chief by/Interrogatoire en-chef par Mr. Gabriel Poliquin	2
Cross-Examination by/Contre-interrogatoire par Mr. Sujit Choudhry	29
Cross-Examination by/Contre-interrogatoire par Mr. Fraser Harland	35
Cross-Examination by/Contre-interrogatoire par Ms. Sara Teich	37
Cross-Examination by/Contre-interrogatoire par Mr. Guillaume Sirois	40
Cross-Examination by/Contre-interrogatoire par Mr. Neil Chantler	43
Cross-Examination by/Contre-interrogatoire par Ms. Ryann Atkins	47
 M. PATRICK EWEN McDONELL, Affirmed/Sous affirmation solennelle	 54
M. BENOÎT EUGÈNE DICAIRE, Affirmed/Sous affirmation solennelle	54
Examination in-Chief by/Interrogatoire en-chef par Mr. Hamza Mohamadhossen	54
Examination in-Chief by/Interrogatoire en-chef par Mr. Gabriel Poliquin	73
Cross-Examination by/Contre-interrogatoire par Mr. Fraser Harland	115
Cross-Examination by/Contre-interrogatoire par Mr. Thomas Jarmyn	118
Cross-Examination by/Contre-interrogatoire par Mr. Sujit Choudhry	122
Cross-Examination by/Contre-interrogatoire par Ms. Sarah Teich	129
Cross-Examination by/Contre-interrogatoire par Mr. Gregory Tzemenakis	131
 M. STÉPHANE PERRAULT, Affirmed/Sous affirmation solennelle	 142
Examination in-Chief by/Interrogatoire en-chef par Mr. Jean-Philippe MacKay	142
Examination in-Chief by/Interrogatoire en-chef par Mr. Daniel Sheppard	167
Cross-Examination by/Contre-interrogatoire par Mr. Neil Chantler	197
Cross-Examination by/Contre-interrogatoire par Mr. Guillaume Sirois	204

VI

Table of Content / Table des matières

	PAGE
Cross-Examination by/Contre-interrogatoire par Ms. Sarah Teich	209
Cross-Examination by/Contre-interrogatoire par Mr. Thomas Jarmyn	210
Cross-Examination by/Contre-interrogatoire par Ms. Mani Kakkar	218
Cross-Examination by/Contre-interrogatoire par Mr. Fraser Harland	225
Cross-Examination by/Contre-interrogatoire par Mr. Barney Brucker	227

VII

Exhibit List / Liste des pièces

No.	DESCRIPTION	PAGE
SEN0000001.EN	Senate of Canada Institutional Report	2
SEN0000001.FR	Rapport institutionnel - Le parlement et le processus législatif	2
WIT0000126.FR	Résumé d'entrevue : Administration du Sénat (David Vatcher, Julie Lacroix et Shaila Anwar)	3
WIT0000126.EN	Interview Summary: Senate Administration (David Vatcher, Julie Lacroix and Shaila Anwar)	3
JKW0000169	Senate Procedure - Chapter 11 Privileges and Immunities	34
WIT0000128.EN	Interview Summary: House of Commons Administration (Patrick McDonell and Benoît Dicaire)	56
WIT0000128.BIL	Interview Summary: House of Commons Administration (Patrick McDonell and Benoît Dicaire)	56
WIT0000128.FR	Résumé d'entrevue : Administration de la Chambre des communes (Patrick McDonell et Benoît Dicaire)	57
WIT0000129.EN	Appendix to Interview Summary: House of Commons Administration (Hedi Touati and Benoît Dicaire)	58
WIT0000129.FR	Complément au résumé d'entrevue: Administration de la Chambre des communes (Hedi Touati and Benoît Dicaire)	58
HOC0000001.EN	Institutional Report of the House of Commons Administration	59
HOC0000001.FR	Rapport institutionnel de l'administration de la Chambre des Communes	59
CAN.SUM.000027	PRC Email Operations Against parliamentarians	96
CAN.SUM.000027.001	Tab A - Chronology of Events: Email Tracking Link Campaign Targeting Canadian parliamentarians	96
COM0000363	Special Report on Foreign Interference in Canada's Democratic Processes and Institutions	116
WIT0000074.EN	Interview Summary - Elections Canada (Stage 2)	142

VIII Exhibit List

No.	DESCRIPTION	PAGE
WIT0000074.FR	Résumé d'entrevue: Élections Canada (Stéphane Perrault, Serge Caron, Josée Villeneuve et Susan Torosian)	143
WIT0000074.001	Affidavit of Jose Villeneuve	143
WIT0000074.002	Affidavit of Serge Caron	143
WIT0000074.003	Affidavit of Susan Torosian	143
ELC.IR.0000002.EN	Elections Canada's Supplementary Institutional Report August 2024	144
ELC.IR.0000002.FR	Rapport institutionnel supplémentaire d'élections Canada	144
CAN004599	Site Status Update and Summary of Foreign Interference Threats to Canadian Democratic Institutions-2023	159
ELC0000054	Meeting New Challenges - Recommendations from the Chief Electoral Officer of Canada following the 43rd and 44th General Elections	180
WIT0000015.EN	Interview Summary: Leona Alleslev	210
CAN011293	China: Domination of Chinese-Language Media in Canada Poses National Security Threats - IM 30/2023	213
CEF0000302_R	Memo for CCE_Summary 2022-0925	221

Ottawa, Ontario

--- The hearing begins Tuesday, September 24, 2024 at 9:32 a.m.

THE REGISTRAR: Order, please

This sitting of the Foreign Interference Commission is now in session. Commissioner Hogue is presiding.

The time is 9:32 a.m.

COMMISSIONER HOGUE: I hope that you had a great weekend.

Maître Poliquin, you will be leading the procedure this morning?

MR. GABRIEL POLIQUIN: So we could we swear in the witnesses, please?

THE REGISTRAR: Mr. Vatcher, could you tell us your full name and spell your last name for the record?

MR. DAVID VATCHER: Good morning. David Vatcher, V-a-t-c-h-e-r.

THE REGISTRAR: And now for the swearing in.

--- MR. DAVID VATCHER, Affirmed:

THE REGISTRAR: And now for Mrs. Lacroix. Could you tell us your full name and spell your last name for the record?

MS. JULIE LACROIX: Julie Lacroix, L-a-c-r-o-i-x.

THE REGISTRAR: Thank you very much. And now for the official swearing in.

--- MS. JULIE LACROIX, Affirmed:

1 **THE REGISTRAR:** Thank you.

2 You can proceed.

3 **--- EXAMINATION IN-CHIEF BY MR. GABRIEL POLIQUIN:**

4 **MR. GABRIEL POLIQUIN:** I would ask to post
5 the official report from the Senate of Canada, SEN.FR,
6 please.

7 Thank you very much.

8 So the Canadian Senate prepared an
9 institutional report following a request by the
10 Commissioner's -- by the Commission's counsel.

11 **MS. JULIE LACROIX:** Yes.

12 **MR. GABRIEL POLIQUIN:** And you had an
13 opportunity to review this document?

14 **MR. DAVID VATCHER:** Yes.

15 **MS. JULIE LACROIX:** Yes.

16 **MR. GABRIEL POLIQUIN:** And you had an
17 opportunity to review this document?

18 **MS. JULIE LACROIX:** Yes.

19 **MR. GABRIEL POLIQUIN:** So you agree for this
20 to be tabled?

21 **MS. JULIE LACROIX:** Yes.

22 **MR. GABRIEL POLIQUIN:** So the report is part
23 of the evidence. The English version is SEN -- and you don't
24 have to post it on the screen, but I just wanted to mention
25 it for the proceedings. It is also tabled as evidence.

26 **--- EXHIBIT No. SEN0000001.EN:**

27 Senate of Canada Institutional Report

28 **--- EXHIBIT No. SEN0000001.FR:**

1 Rapport institutionnel - Le parlement
2 et le processus législatif

3 **MR. GABRIEL POLIQUIN:** So now, I would ask to
4 post the summary of the witnesses' interrogation with the
5 counsel of the Commission.

6 So you remember, both of you, that you were
7 interviewed by the Commission lawyers on Thursday, September
8 12th, 2024? It is exact?

9 **MR. DAVID VATCHER:** Yes.

10 **MS. JULIE LACROIX:** Yes.

11 **MR. GABRIEL POLIQUIN:** And then a summary of
12 the interview were prepared as well as a registry of the
13 Senate information. So you had an opportunity to check the
14 information?

15 **MS. JULIE LACROIX:** Yes.

16 **MR. GABRIEL POLIQUIN:** You agree that it is
17 the exact summary of your answers during the interview?

18 **MR. DAVID VATCHER:** Yes.

19 **MS. JULIE LACROIX:** Yes.

20 **MR. GABRIEL POLIQUIN:** So the summary is
21 tabled as evidence. You don't have to post the English
22 version, WIT. So this also will be tabled as evidence.

23 **--- EXHIBIT No. WIT0000126.FR:**

24 Résumé d'entrevue : Administration du
25 Sénat (David Vatcher, Julie Lacroix
26 et Shaila Anwar)

27 **--- EXHIBIT No. WIT0000126.EN:**

28 Interview Summary: Senate

1 Administration (David Vatcher, Julie
2 Lacroix and Shaila Anwar)

3 **MR. GABRIEL POLIQUIN:** So my questions will
4 be mostly in French, but you can answer in either official
5 language, of course.

6 First of all, I would like to talk about your
7 responsibilities and functions for the Senate.

8 Mrs. Lacroix, what are your present duties?

9 **MS. JULIE LACROIX:** I'm the Director of
10 Institutional Security and Safety for the Senate and I'm in
11 charge of any issue that has to do with Senate security
12 except the physical issues that have to be dealt with by the
13 parliamentary security service.

14 **MR. GABRIEL POLIQUIN:** And what are your
15 duties? Do you deal with other subjects?

16 **MS. JULIE LACROIX:** Yes. I'm also the main
17 advisor in terms of security with the president, the Chair of
18 the Senate and the Clerk of the Senate. I'm in charge of
19 several divisions in my branch, the security accreditation,
20 the management of investigations, anything that has to do
21 with foreign travelling or travelling across the country,
22 fire control, parking, security project management, technical
23 operations that have to do with safety and awareness
24 campaigns. And these are just a few of the various
25 divisions.

26 **MR. GABRIEL POLIQUIN:** We'll deal with the
27 awareness issue later on.

28 But since when are you in that position?

1 **MS. JULIE LACROIX:** Since 2018.

2 **MR. GABRIEL POLIQUIN:** And how many people in
3 your service?

4 **MS. JULIE LACROIX:** Forty-two (42).

5 **MR. GABRIEL POLIQUIN:** And in that bench, who
6 has a security clearance?

7 **MS. JULIE LACROIX:** Forty-two (42).

8 **MR. GABRIEL POLIQUIN:** At what level?

9 **MS. JULIE LACROIX:** Top secret.

10 **MR. GABRIEL POLIQUIN:** And within your unit,
11 within your branch, is there someone who deals with the
12 foreign intervention in particular or is it something that is
13 shared by many people?

14 **MS. JULIE LACROIX:** It is a responsibility
15 that is shared by many people.

16 **MR. GABRIEL POLIQUIN:** We will deal with that
17 later.

18 Mr. Vatcher, now a few similar questions.
19 What are your present functions?

20 **MR. DAVID VATCHER:** Good morning. I'm
21 Director of Information Services for the Senate and our
22 branch, well, about 50 employees, we are responsible for
23 managing information so we deal with archives also,
24 parliamentary archives, and we are also responsible with the
25 client services in terms of technological services, the
26 management of the infrastructure, and we are also responsible
27 for system integration and so on.

28 **MR. GABRIEL POLIQUIN:** Could you give us more

1 details about what you mean by that?

2 MR. DAVID VATCHER: Well, as you know, Senate
3 is a unique institution in Canada and we have apps that are

4 MR. GABRIEL POLIQUIN: You mean software and
5 so on.

6 MR. DAVID VATCHER: Yes.

7 MR. GABRIEL POLIQUIN: Since when are you in
8 this position?

9 MR. DAVID VATCHER: Since February 2018.

10 MR. GABRIEL POLIQUIN: Do you have security
11 clearance in your section?

12 MR. DAVID VATCHER: We have secret clearance
13 in my branch.

14 MR. GABRIEL POLIQUIN: And is there one
15 person who's in charge of foreign interference or is it a
16 shared responsibility?

17 MR. DAVID VATCHER: No. There's nobody who's
18 in charge of those issues that have to do with foreign
19 intervention.

20 MR. GABRIEL POLIQUIN: Now, with respect to
21 relations with external partners with anything that has to do
22 with foreign intervention -- so I'll start with you, Mrs.
23 Lacroix.

24 Could you describe what are your relations
25 with external partners? And I mean for the police services
26 and intelligence services and the other law services.

27 MS. JULIE LACROIX: Well, we have great
28 relationships with information intelligence services, with

1 local police, with the RCMP and various other partners
2 through the federal machine and on Parliament Hill.

3 **MR. GABRIEL POLIQUIN:** You're talking about
4 what; you exchange information?

5 **MS. JULIE LACROIX:** Yes, there are daily
6 meetings, exchanges of information, advice in terms of
7 various preparations or briefing documents.

8 **MR. GABRIEL POLIQUIN:** With respect to
9 briefing documents, do you have other things that have to do
10 with these issues?

11 **MS. JULIE LACROIX:** Well, I think that we all
12 have a common goal, that is, to make sure that everybody is
13 safe, all our clients are in a safe environment.

14 **MR. GABRIEL POLIQUIN:** With respect to
15 various exchange forums, in paragraph 38 in the summary of
16 the interview, you talked about Intersec. What does it mean?

17 **MS. JULIE LACROIX:** It is an exchange forum,
18 various partners that have to do with safety and security and
19 the Senate, of course, participate in this forum.

20 **MR. GABRIEL POLIQUIN:** And for any other
21 exchange forum, could you describe these exchanges as being
22 proactive in terms of prevention or is it a reaction?

23 **MS. JULIE LACROIX:** Well, both, in fact.

24 **MR. GABRIEL POLIQUIN:** And in terms of
25 proaction, is foreign interference an issue that is often in
26 the agenda?

27 **MS. JULIE LACROIX:** Well, it could happen.

28 **MR. GABRIEL POLIQUIN:** Is it frequent? Is it

1 frequent?

2 MS. JULIE LACROIX: Could you repeat?

3 MR. GABRIEL POLIQUIN: Is it frequent?

4 MS. JULIE LACROIX: Well, it depends on the
5 context and the exchanges, but sometimes it is debated.

6 MR. GABRIEL POLIQUIN: And what about formal
7 agreements with these agencies in terms of physical safety?

8 MS. JULIE LACROIX: Well, the Senate and
9 House of Commons, in fact, both chairs, have a formal
10 agreement with Public Safety and the RCMP with respect to the
11 Parliamentary Protection Service.

12 MR. GABRIEL POLIQUIN: The Parliamentary
13 Protection Service is not under your direction.

14 MS. JULIE LACROIX: No, they report to the
15 two chairs.

16 MR. GABRIEL POLIQUIN: You talked about
17 accreditation. What do you mean by that?

18 MS. JULIE LACROIX: Well, what it means is
19 that we are checking in terms of safety background check for
20 any employees. So it is an operation that has to do about
21 the loyalty and the previous career of these people.

22 MR. GABRIEL POLIQUIN: Do you deal with
23 foreign intervention in these circumstances? Did it happen?
24 Without getting into details.

25 MS. JULIE LACROIX: Yes.

26 MR. GABRIEL POLIQUIN: [No interpretation]

27 COMMISSIONER HOGUE: Just one question, Mr.
28 Poliquin.

1 You said that about these checking, are
2 Senators excluded from these operations?

3 **MS. JULIE LACROIX:** Yes. This policy does
4 not apply to Senators, but to employees.

5 **MR. GABRIEL POLIQUIN:** And once you are given
6 your accreditation, what are you entitled to?

7 **MS. JULIE LACROIX:** Well, they can access the
8 information they need, they can access to the location that
9 is a condition of employment.

10 **MR. GABRIEL POLIQUIN:** So once a Senator is
11 appointed, as the Commissioner asked, do they have access to
12 all these services, software, et cetera?

13 **MS. JULIE LACROIX:** You're talking about a
14 Senator?

15 **MR. GABRIEL POLIQUIN:** Yes.

16 **MS. JULIE LACROIX:** Well, as soon as a
17 Senator is appointed, he has -- he or she has access to
18 parliamentary operations and he can take care of duties.

19 **MR. GABRIEL POLIQUIN:** So if there's a
20 question of checking the background of a Senator before his
21 or her appointment, it has nothing to do with you.

22 **MS. JULIE LACROIX:** No. It's a question that
23 has to be dealt with by Privy Council.

24 **MR. GABRIEL POLIQUIN:** Mr. Vatcher, in terms
25 of information safety, what are your relationships with
26 external partners?

27 **MR. DAVID VATCHER:** I would say that we have
28 a very good relationship in terms of various teams, my team

1 and other government teams and various departments, so when
2 something is of interest, let's say that a Senator or a
3 Senate employee could be a specific target for a cyber
4 attack, we are warned and we take action if need be.

5 **MR. GABRIEL POLIQUIN:** We'll have more
6 questions on that topic, but since there's a specific rule,
7 you are informed, but do you also take charge of some issues
8 by your own capacities?

9 **MR. DAVID VATCHER:** Yes, on a daily basis.

10 **MR. GABRIEL POLIQUIN:** And in what
11 circumstances would you get a warning from an external
12 partner?

13 **MR. DAVID VATCHER:** Well, if you're talking
14 about a cyber attack or an attack that is reported by one of
15 their means that could have an impact on a parliamentarian or
16 an employee, we would be told about it, simply.

17 **MR. GABRIEL POLIQUIN:** Well, we'll go back to
18 that later in terms of one particular incident.

19 And how frequently do you deal with external
20 partners?

21 **MR. DAVID VATCHER:** Well, we have regular
22 exchanges, but it's on a needs basis. We don't have a
23 monthly forum. There are meetings to discuss various
24 subjects, but my team is always, of course, aware of any
25 potential problem. They are in contact with these agencies.

26 **MR. GABRIEL POLIQUIN:** Potential issues, but
27 also in terms of exchanges that have to do with best
28 practices and in terms of education for the administration of

1 the Senate, is there something?

2 **MR. DAVID VATCHER:** Well, in this case we
3 have some best practices and the Senate, in fact, has a cyber
4 safety program and, through this program, we were able to
5 implement the best practices to be found in the industry and
6 as represented for any government institution.

7 So we do cooperate with all these agencies.
8 If we have questions, of course, we can ask them, but we
9 implement the best practices in the industry.

10 **MR. GABRIEL POLIQUIN:** So it is up to you to
11 look for these best practices that are provided by various
12 agencies?

13 **MR. DAVID VATCHER:** Yes.

14 **MR. GABRIEL POLIQUIN:** So there's no
15 particular forum or regular meetings to exchange information.

16 **MR. DAVID VATCHER:** You're right.

17 **MR. GABRIEL POLIQUIN:** In these exchanges,
18 you mention that it is on the needs basis. So let's say that
19 -- is there something about foreign intervention --
20 interference?

21 **MR. DAVID VATCHER:** Well, we're talking about
22 cyber threat, cyber safety, and in some cases, there's no
23 direct link with a foreign entity, but anything of that
24 nature is taken very seriously. And sometimes, later on, we
25 do discover that a foreign actor was involved.

26 **MR. GABRIEL POLIQUIN:** So in such
27 circumstances, does it mean that there's a difference in your
28 practices in terms of prevention or reaction following a

1 cyber attack?

2 **MR. DAVID VATCHER:** No. I would say that in
3 terms of global threats, we are facing these issues in order
4 to eliminate them as soon as possible. And since we don't
5 know if a foreign state is involved, is threatening us, it is
6 not the optic in which we are trying to solve the issue. We,
7 rather, want to prevent any potential damage, so we want to
8 control damages.

9 **MR. GABRIEL POLIQUIN:** Well, I'll have more
10 questions on this topic later on.

11 Now, let's talk about training for Senators
12 and staff members. And here I mean staff of your
13 administration, of Senate administration, and those that are
14 employed by Senators. I know that there are differences in
15 terms of training. Well, I'm not sure, but if there's a
16 difference, please tell me so.

17 Mrs. Lacroix, could you tell me, what about
18 training in your unit for Senators and staff members?

19 **MS. JULIE LACROIX:** Well, as soon as an
20 appointment is confirmed for a given Senator, there's an
21 onboarding session and this training is to make people aware
22 of safety issues. And we do the same thing with the staff,
23 with the administration staff, and also the Senators' staff.

24 **MR. GABRIEL POLIQUIN:** Is it the same
25 training for Senators as well as for the personnel?

26 **MS. JULIE LACROIX:** No. For Senators, there
27 may be some different elements with respect to personal
28 security and physical security for the Senators when they're

1 travelling, for example.

2 **MR. GABRIEL POLIQUIN:** And of course, what
3 we're interested here is foreign interference.

4 Is there any difference with that in the
5 training? Do the Senators have a different training with
6 respect to foreign interference than the staff?

7 **MS. JULIE LACROIX:** Yes, absolutely,
8 especially in the context of foreign travel when they are
9 also having delegations or foreign delegations who are their
10 guests. So yes, there are elements in the training that are
11 different for the Senators with respect to the staff.

12 However, we do touch on those issues with the
13 staff also.

14 **MR. GABRIEL POLIQUIN:** So the foreign
15 interference, that's part of the onboard or training since
16 when?

17 **MS. JULIE LACROIX:** Since before my arrival.

18 **MR. GABRIEL POLIQUIN:** Okay. And can you say
19 in more detail with respect to the training for foreign
20 interference, whether it's for Senators or for staff, what
21 type of training does it comprise?

22 **MS. JULIE LACROIX:** I can't go into too much
23 detail because that might be a problem for questions of
24 security.

25 **MR. GABRIEL POLIQUIN:** And your branch, do
26 you collaborate with other agencies for the development of
27 this training?

28 **MS. JULIE LACROIX:** Yes, we collaborate with

1 other partners. And sometimes in our exchanges with
2 intelligence agencies, they give us material and we -- that
3 we will use during the trainings.

4 **MR. GABRIEL POLIQUIN:** Fine. And do -- the
5 security agencies, do they give any kind of particular
6 training for the staff?

7 **MS. JULIE LACROIX:** This is something that
8 they do offer if it's requested.

9 **MR. GABRIEL POLIQUIN:** This is something they
10 offer to the Senators if it's requested?

11 **MS. JULIE LACROIX:** Yes.

12 **MR. GABRIEL POLIQUIN:** So generally speaking
13 with respect to security, and we don't need to go into the
14 details, but what type of resources are available? What can
15 -- who can the Senators contact if they have a threat, a
16 security threat?

17 **MS. JULIE LACROIX:** They can contact us and
18 they can contact the local police in their region or here.
19 And we can facilitate meetings with the intelligence services
20 or with the RCMP. It really depends on the subject.

21 **MR. GABRIEL POLIQUIN:** Thank you.

22 And what is -- what happens if they're
23 abroad, if they're outside of Canada?

24 **MS. JULIE LACROIX:** If they're outside of
25 Canada, if they're travelling, we do have a security
26 framework that will accompany them, that there may be staff
27 resources on location or we will give them the resources and
28 points of contact, for example.

1 **MR. GABRIEL POLIQUIN:** Mr. Vatcher, for the
2 question of travel, maybe we could start there. If Senators
3 or a member of staff of the Senate is travelling abroad, what
4 type of preparation do you do to be able to equip them,
5 whether it's the Senator or the staff?

6 **MR. DAVID VATCHER:** Before travel, we ask
7 Senators that are travelling to let us know where that they
8 will be travelling to and the reasons for their travel
9 without necessarily going into too much detail to be able to
10 determine the amount of risk that's associated with this
11 travel. And then provisions will be made to be able to give
12 more security as needed with respect to the equipment of the
13 Senator that is travelling.

14 **MR. GABRIEL POLIQUIN:** When you're talking
15 about equipment, you're talking about computers?

16 **MR. DAVID VATCHER:** We're talking about
17 computers and cell phones.

18 **MR. GABRIEL POLIQUIN:** And what type of
19 training is given to Senators or staff with respect to
20 protecting intelligence information and IT?

21 **MR. DAVID VATCHER:** There are two mandatory
22 trainings that are for both Senators and staff. The first is
23 on the management of information where we explain very
24 clearly the processing the information has to have, and that
25 from the cradle to the end of its useful life and then,
26 within our program, for the protection and cyber security,
27 there is a training, and that is mandatory training that --
28 for awareness of cyber security. And we use this for

1 everyone. Both all new staff and new Senators have to
2 complete that training within the two weeks of their arrival
3 at the Senate.

4 The Senators can also -- I do meet each, or
5 one of my managers if I'm not there that day, meet with the
6 Senators -- new Senators to speak to them about risks with
7 respect to cyber security and cyber threats that they may be
8 -- have as Senators.

9 **MR. GABRIEL POLIQUIN:** With respect to the
10 onboarding, are there meetings that are done regularly after
11 that?

12 **MR. DAVID VATCHER:** Some training can be done
13 following. There may be a simulation -- simulation exercises
14 that we would do and they may have to do a follow-up training
15 to be able to be reminded of dangers and also to be able to
16 manage the risk.

17 **MR. GABRIEL POLIQUIN:** So this is a type of
18 test that you give Senators and staff, a simulation for -- a
19 phishing simulation.

20 **MR. DAVID VATCHER:** Yes.

21 **MR. GABRIEL POLIQUIN:** If they don't pass the
22 test, then further training is given?

23 **MR. DAVID VATCHER:** Yes.

24 **MR. GABRIEL POLIQUIN:** What is the -- how are
25 those trainings done? Are they included as security and
26 intelligence agencies?

27 **MR. DAVID VATCHER:** They're not included.
28 It's our internal experts that have developed the training

1 and we have recourse to a specialized external company that
2 help us set up the training for cyber security.

3 **MR. GABRIEL POLIQUIN:** Thank you.

4 Before going to the next, there's a question
5 I had for you, Madam Lacroix, and it's to follow up on what
6 Mr. Vatcher has said.

7 The training that you give for security in
8 your case, is this training that is mandatory?

9 **MS. JULIE LACROIX:** No.

10 **MR. GABRIEL POLIQUIN:** So the onboarding
11 process, that's not mandatory either?

12 **MS. JULIE LACROIX:** No.

13 **MR. GABRIEL POLIQUIN:** It's not mandatory,
14 either, for the Senators or for the staff?

15 **MS. JULIE LACROIX:** No.

16 **MR. GABRIEL POLIQUIN:** Fine. Let's move to
17 the question of cyber attacks. So Mr. Vatcher, I'm going to
18 be questioning you especially.

19 And it's mentioned at paragraph 57 of the
20 interview summary. You don't have to go to the document, but
21 simply I'm making reference to that.

22 So for cyber attacks, generally speaking,
23 without going into the detail, can you describe the nature of
24 cyber attacks the Senate might face?

25 **MR. DAVID VATCHER:** Our institution is faced
26 with all types of cyber threats that exist, and this on a
27 continual basis. We know through -- with our tools, we know
28 that in part because sometimes there may be phishing emails

1 that come in we might not be aware of because they'll be
2 immediately deleted, so I can't give you a number precise,
3 but we do face all types of attacks that are possible since
4 we respond to the four type of -- four types of malicious
5 actors.

6 The first is an opportunist that discovers
7 some kind of loophole and they try to exploit that. The
8 second is an activist, and they may have a cause. And the
9 third type -- category, it would be more of a financial
10 nature, so those groups will be wanting to obtain money. And
11 so this would be ransom type of attack. And then you have a
12 fourth category, which would be the states, state actors that
13 would be trying to information or else to create chaos within
14 the institution. And so these actors have money and time to
15 invest.

16 **MR. GABRIEL POLIQUIN:** So depending on the
17 category, does it change how you operate, how you respond?

18 **MR. DAVID VATCHER:** The response to an attack
19 will be based, of course, on the type of attack, but all
20 attacks are taken seriously and processed as quickly as
21 possible.

22 **MR. GABRIEL POLIQUIN:** Can you clarify
23 something for me? Earlier, it was said that the information
24 as to whether it's a state actor that is behind an attack, if
25 I understood your response, it's -- it can't be determined.

26 **MR. DAVID VATCHER:** First of all, we try to
27 ensure that the attack is not successful, and then we go
28 through a verification exercise to see where the attack is --

1 what's the source, where's it coming from. And we would work
2 with our colleagues with the different security and
3 intelligence agencies in Canada to be able to find the source
4 and to do a forensic investigation.

5 **MR. GABRIEL POLIQUIN:** Paragraph 58 of your
6 interview summary, you're talking about one of the risks.
7 And I don't know if it's a vulnerability or a risk that the
8 Senate is facing and other institutions also are faced with
9 the same thing. It would be a secondary attack.

10 What is that? If you want to put it into
11 context, we could put it up.

12 **MR. DAVID VATCHER:** That wouldn't be
13 necessary.

14 A secondary attack, this is an attack that is
15 -- goes through some company that we work with, so there's an
16 infiltration and then the -- they use that link through that
17 company. So if I were to receive an email from a company
18 that I'm aware of that has an invoice that I have to be
19 careful and look at it and to make sure that we ensure that
20 the people that we're dealing with are really the people that
21 they say they are.

22 **COMMISSIONER HOGUE:** So the Senate, if they
23 may have, say, an accounting firm that has accounting
24 services for them, so a secondary attack would mean that any
25 type of actor would first attempt to infiltrate the
26 accounting firm and, through that accounting firm, because
27 they have links with the Senate, they would use that link to
28 infiltrate your system.

1 **MR. DAVID VATCHER:** Yes, or almost. What
2 they would do is to try and usurp the identity of the firm to
3 become -- to be able to enter into account with us and to
4 trick us, and so we have to confirm with the company so we
5 ask them, the firm we work with, if they have a problem --
6 that if they think they've been attacked, that they let us
7 know or at least to inform us of what's happening.

8 **COMMISSIONER HOGUE:** So there's not
9 necessarily an intrusion through a third system. It's simply
10 a means of access.

11 **MR. DAVID VATCHER:** Yes, exactly.

12 **COMMISSIONER HOGUE:** Thank you.

13 **MR. GABRIEL POLIQUIN:** With respect to state
14 actors, foreign state actors and their cyber attacks, if you
15 know internally, say, that there is a foreign state actor,
16 what type of collaboration do you have with other -- with the
17 intelligence and security agencies? Is this increased work
18 at that collaboration at that time?

19 **MR. DAVID VATCHER:** Yes, absolutely. When we
20 have phishing campaigns, anti-phishing campaigns would happen
21 pretty much every day. And some of these campaigns come from
22 states and they may be more sophisticated, depending on the
23 funds they have access to, and it may be more targeted.

24 So we -- when we detect that there is, in
25 fact, a foreign power who wants to get information or to
26 infiltrate, we will communicate with our colleagues on the
27 Hill as well as other agencies.

28 **MR. GABRIEL POLIQUIN:** So you would be able

1 to get information from the different agencies to be able to
2 go ahead with your work in cyber security.

3 **MR. DAVID VATCHER:** Absolutely. These
4 agencies really have our well-being in mind, of course, so
5 they will give information to us to help us out.

6 **MR. GABRIEL POLIQUIN:** Thank you.

7 If we look at a specific incident that maybe
8 would be a study, if you want, for a cyber attack, we're
9 talking about the incident APT31 in January 2021. I think
10 you were in your position at that time.

11 So at paragraph 27 and 28 in your interview
12 summary, and let's bring that up. And this would be simply
13 to situate what we're talking about here.

14 So you can describe it yourself. So can you
15 tell us what happened?

16 **MR. DAVID VATCHER:** So at the end of January
17 2021, our colleagues from the House of Commons let us know
18 that there had been a phishing attempt that was under way.
19 And as we said earlier for the phishing, we see that every
20 day, but it's less frequent.

21 **MR. GABRIEL POLIQUIN:** Can you tell us what's
22 the difference between phishing and the -- and the other
23 phishing term?

24 **MR. DAVID VATCHER:** So phishing, you send
25 many lines into the water and you hope a fish will -- and so
26 the other type of attack, harpooning, is much more targeted,
27 and so -- and that is done especially when an entity will be
28 taken if you have somebody who is -- if you have a package

1 that is later sent.

2 But spear phishing, this is somebody in
3 particular that is targeting, and so that person will be --
4 will have information that they have obtained elsewhere to be
5 able to attempt to get more information or to put malicious
6 software in. But it will be sent to targeted people, several
7 people, but targeted people.

8 **MR. GABRIEL POLIQUIN:** So APT, what type?
9 Was it a spear phishing type?

10 **MR. DAVID VATCHER:** Yes, it was spear
11 phishing and it was more targeted.

12 **MR. GABRIEL POLIQUIN:** In January, what were
13 you aware of with respect to that attack?

14 **MR. DAVID VATCHER:** All that we knew at the
15 time, that there were strange emails coming in and that some
16 of our parliamentarians may be -- may be being targeted
17 through spear phishing.

18 **MR. GABRIEL POLIQUIN:** So this was something
19 that had already been detected or was it the Cyber Security
20 Centre that alerted you?

21 **MR. DAVID VATCHER:** It was the colleagues
22 from the House of Commons that alerted us to this.

23 And our tools had already detected some of
24 the emails of the campaign and they had set them aside, and
25 what we did is that we immediately entered in contact with
26 the Senators who had been targeted to ensure that all of the
27 messages be deleted.

28 **COMMISSIONER HOGUE:** I have a question.

1 When you put them aside, set them aside, so
2 that's kind of in a quarantine. When we're told that an
3 email is in quarantine, there's a certain delay to be able to
4 access it. So that doesn't necessarily go into the inbox
5 once there's -- if they're set aside.

6 **MR. DAVID VATCHER:** Yes. Sometimes the tool
7 will take care of that itself. It will detect, because of
8 the different qualities of the -- they'll know either that
9 it's spam or it will be more serious if it were potentially
10 dangerous, and so they will set it aside.

11 Our own internal policy means that we will
12 not destroy any email that goes -- that is addressed to a
13 Senator. We'll put it -- set it aside and we will let the
14 Senator know that there is an email that has been set aside
15 for you. We want to let you know that, potentially, it may
16 be an attack. And so we would like to delete it with your
17 position.

18 **MR. GABRIEL POLIQUIN:** And with respect to
19 that question, you mentioned earlier that phishing and spear
20 phishing, this is something that happens every day, so for
21 each of the mails of that nature, you will notify the
22 Senator?

23 **MR. DAVID VATCHER:** The phishing is almost a
24 day. The spear phishing is more rare. It has more effort.

25 **MR. GABRIEL POLIQUIN:** So the same question
26 on phishing. You get emails with such contents, you warn
27 Senators?

28 **MR. DAVID VATCHER:** We will warn the Senator.

1 If it is flagged, we'll warn the Senators that are targeted
2 for this phishing campaign.

3 **COMMISSIONER HOGUE:** And when it's phishing,
4 you can sent out a general notice to all Senators saying,
5 "This type of email is going around, don't open it", et
6 cetera, whereas when it's the other kind, you will
7 communicate with the Senators directly because they are
8 specifically targeted?

9 **MR. DAVID VATCHER:** [No interpretation]

10 **MR. GABRIEL POLIQUIN:** So to come back to
11 APT31, if I understand your interview summary, some messages
12 would have and did end up in the inboxes. Is that correct?

13 **MR. DAVID VATCHER:** Yes.

14 **MR. GABRIEL POLIQUIN:** And others would not
15 have reached them. They would have been blocked by the
16 firewalls?

17 **MR. DAVID VATCHER:** By some tools.

18 **MR. GABRIEL POLIQUIN:** It's not the right
19 word, but it's okay.

20 Protection tools. Generalized protection
21 tools.

22 **MR. DAVID VATCHER:** Correct.

23 **MR. GABRIEL POLIQUIN:** And were any messages
24 sent to Senators whether the email was blocked by the
25 protection tools or did you only contact the Senators who did
26 receive the email?

27 **MR. DAVID VATCHER:** We contacted all the
28 Senators who had been targeted because a targeted attack can

1 come in two or three ways. So the awareness raising of our
2 clients is our best protection in the Senate, so when a
3 Senator knows that they are the target of an attack, they
4 will be even more cautious, obviously. And it's really the
5 best tool.

6 **MR. GABRIEL POLIQUIN:** And you knew at that
7 time, in January 2021, that Senators had received those
8 emails?

9 **MR. DAVID VATCHER:** We knew that some
10 Senators had been the target of a spear phishing campaign.

11 **MR. GABRIEL POLIQUIN:** And did you know in
12 January 2021 that -- who was behind this campaign?

13 **MR. DAVID VATCHER:** No.

14 **MR. GABRIEL POLIQUIN:** When did you discover
15 that?

16 **MR. DAVID VATCHER:** I would say it was April
17 or May of this year when it was published in the newspapers.

18 **MR. GABRIEL POLIQUIN:** You discovered that in
19 the press?

20 **MR. DAVID VATCHER:** Yes.

21 **MR. GABRIEL POLIQUIN:** Would this information
22 have been good to have in January or February 2021?

23 **MR. DAVID VATCHER:** Not really because, as I
24 explained earlier, the threat -- whoever it comes from, the
25 threat will be dealt with directly and immediately once we
26 are made aware of it, obviously. Whether it comes from a
27 criminal group trying to get money or from a foreign state,
28 we just want to eliminate the threat.

1 **COMISSAIRE HOGUE:** So your reaction would be
2 the same? There's no distinction depending on the identity
3 of the actor behind the attack?

4 **MR. DAVID VATCHER:** None. What we do is
5 there's a threat, we take care of the threat. Then after
6 that, maybe we'll have follow-up with our security colleagues
7 to see where it came from. We'll give them the information
8 that they need to help them identify this because we want the
9 protection of the Senate and the House of Commons and all the
10 Canadian government, so we are good collaborators in that
11 sense.

12 **COMMISSIONER HOGUE:** Did those exchanges take
13 place? Because we see that the attack happened in January
14 2021, and you say that it's this year in, I think you said,
15 April or May 2024, that you learned who is behind this
16 attack.

17 Between 2021 and '24, were there this kind of
18 exchanges to try and understand where this type of attack had
19 come from, or was it just one of so many?

20 **MR. DAVID VATCHER:** It was one amongst many,
21 and we didn't follow up as to the specific attack on the
22 Senate. We didn't have a follow-up with our colleagues from
23 the House or another government body. It's really in April-
24 May of this year that the case became more broadly public and
25 the link with APT31 was established.

26 **COMMISSIONER HOGUE:** And even if it was
27 targeted phishing rather than general phishes because you say
28 less often this targeted phishing. It doesn't change the

1 fact that it was one attempt amongst many.

2 **MR. DAVID VATCHER:** Just like for others.

3 Quite often, targeted phishing is not a state, but a well-
4 organized group who wants to attempt to get money out of us,
5 often in a very awkward way.

6 **COMMISSIONER HOGUE:** Those who get the names
7 wrong in the emails and stuff like that?

8 **MR. DAVID VATCHER:** That's right. Some things
9 are pretty obvious, but the attacks are more and more
10 sophisticated and good quality, I would say, so the awareness
11 raising and the training of our parliamentarians, but also of
12 our employees in the Senate, is our first line of defence.

13 **MR. GABRIEL POLIQUIN:** And since the APT31
14 attack, now you know that it's a state actor, are there any
15 additional measures or different measures that would have
16 been taken to face this kind of attack in the future?

17 **MR. DAVID VATCHER:** No. For sure we have
18 communications, as I said, with external partners. And given
19 that we all want the same thing, we want to make sure that
20 we're following that if there's any other threat.

21 **COMMISSIONER HOGUE:** Once you knew that it
22 was APT31 that was behind this attack, did you communicate
23 with Senators who were the target of that phishing to inform
24 them of that? Probably they knew that in the newspaper, but
25 did you contact them to discuss it?

26 **MR. DAVID VATCHER:** I did not communicate
27 with them, but I answered a question from one of the Senators
28 on how it had been dealt with.

1 I answered that we had eliminated the risk
2 and there had been no breach of information. There had been
3 no success in this attack. And that was the end of that
4 attack, as far as we were concerned.

5 **MR. GABRIEL POLIQUIN:** I'm running out of
6 time, but was there anything else that you would like to
7 inform the Commission about foreign interference in your
8 particular duties at the Senate?

9 **MS. JULIE LACROIX:** No.

10 **COMMISSIONER HOGUE:** [No interpretation] and
11 if you cannot answer, I invite to tell me right away. Don't
12 worry because I'm asking the question.

13 On the basis of what you can see as
14 information, would you say that the attacks that the Senate
15 is facing come frequently from foreign actors -- and I'm
16 thinking, you know, states or agents acting in their name --
17 or is that something that remains marginal and not that
18 frequent?

19 Essentially, amongst all the attacks -- I
20 understand that you get a great many daily cyber attacks.
21 What's the share of those that's coming from foreign states?
22 Are they an important part of it?

23 **MR. DAVID VATCHER:** Thank you for your
24 question.

25 In terms of quantity, the attacks from
26 foreign states or people who represent or supporting a
27 foreign state are increasing, but represent a minority of
28 attacks that we're facing because it's often ransomware that

1 we receive because there's money to be made and people are
2 trying that more. There's some companies that exist in other
3 countries that do only that.

4 However, we are in a geopolitical climate --
5 I don't want to go too far in this, but the geopolitical
6 climate is very tense and it would be crazy to think that
7 these attacks are not going to continue increasing in number
8 and in level of sophistication.

9 **COMMISSIONER HOGUE:** So could we say that,
10 currently, for you, just the Senate, there is no immediate
11 peril in the sense that it remains something that is
12 relatively modest and controlled but you are seeing an
13 increase of those attacks from foreign state actors? You are
14 observing an increase?

15 **MR. DAVID VATCHER:** I'm not sure I want to
16 answer that.

17 **COMMISSIONER HOGUE:** That's fine.

18 Nothing to add, Mrs. Lacroix?

19 **MS. JULIE LACROIX:** No.

20 **MR. GABRIEL POLIQUIN:** Thank you. That's it
21 for my questions.

22 **COMMISSIONER HOGUE:** So we'll have cross-
23 examination. Let me just find my paper.

24 So first of all, we will have Mr. Choudhry
25 representing Jenny Kwan.

26 **--- CROSS-EXAMINATION BY MR. SUJIT CHOUDHRY:**

27 **MR. SUJIT CHOUDHRY:** Good morning. I'll be
28 posing my questions in English. I hope that's ---

1 **MS. JULIE LACROIX:** Not a problem.

2 **MR. SUJIT CHOUDHRY:** Not a problem. Okay.

3 Great. Thanks. So I'd like to just ask you -- for the
4 record, I'm -- my name is Sujit Choudhry and I represent
5 Jenny Kwan, member of Parliament.

6 So I just want to take you back to the
7 interview summary, if we could, and we'll use the French
8 version, because that's what Commission counsel referred to.

9 So if we could go to paragraph 30, please?

10 And so this is the APT31 incident, and I just
11 want to dig into this a bit. And so I'd like to take you to
12 the second sentence of paragraph 30, which says:

13 "The fact of knowing the source of
14 the attack earlier would not have
15 changed the quick response from the
16 information services..." (As read)

17 And so that's your evidence; correct?

18 **MR. DAVID VATCHER:** I maintain that.

19 **MR. SUJIT CHOUDHRY:** Okay, good. And so --
20 and just for the record, the corresponding paragraph in the
21 English witness summary of his paragraph 29, and I'll just
22 state it for the record, it says, "Knowing the source of the
23 attack earlier would not have changed the Senate's prompt
24 response." And that's the same statement. So I want to ask
25 you to imagine a different scenario.

26 **MR. DAVID VATCHER:** Right.

27 **MR. SUJIT CHOUDHRY:** So suppose when you
28 became aware of the attack back in January 2021, at that

1 time, you had also become aware that the attack was from
2 APT31. I know you didn't learn that until June 2024, but
3 let's imagine you learned at that time or soon thereafter.
4 And so the question I have is this, in addition to informing
5 the offices of the relevant senators that there had been an
6 attack, would you also have informed them that the attack had
7 come from APT31?

8 **MR. DAVID VATCHER:** The way I answered that
9 question in French -- let me give you a preamble first --

10 **MR. SUJIT CHOUDHRY:** Sure.

11 **MR. DAVID VATCHER:** --- is because -- and as
12 I've said -- as I've already mentioned more than once this
13 morning, we treat all these threats seriously ---

14 **MR. SUJIT CHOUDHRY:** Sure, sure.

15 **MR. DAVID VATCHER:** --- and we act quickly.
16 And in our actions, that would not have changed -- I mean,
17 our actions would not have changed in that we'd have taken
18 steps immediately to thwart the attack.

19 **MR. SUJIT CHOUDHRY:** M'hm.

20 **MR. DAVID VATCHER:** Your question as to would
21 we have mentioned to senators at that time if APT31 was
22 behind it?

23 **MR. SUJIT CHOUDHRY:** M'hm. If you had been
24 aware, which you weren't, but if you had been aware.

25 **MR. DAVID VATCHER:** I think I would first
26 have raised it to my superiors, and, ultimately, that
27 decision to warn senators, or to mention it to senators would
28 have been taken by our CIBA steering members.

1 So to make that clear to you, sir, I report
2 to my boss, and she reports to what we call the Committee on
3 Internal Budgets and Economy ---

4 **MR. SUJIT CHOUDHRY:** M'hm.

5 **MR. DAVID VATCHER:** --- and Administration.
6 So we report to that committee, and when different decisions
7 need to be taken, we will defer to their judgment on whether
8 that should have happened or not.

9 **MR. SUJIT CHOUDHRY:** Okay. So if I could
10 summarize, the information would have ultimately been brought
11 through the, you know, through your reporting chain to a
12 group of senators?

13 **MR. DAVID VATCHER:** Correct.

14 **MR. SUJIT CHOUDHRY:** Who then would have ben
15 able to decide whether to disclose. Ms. Lacroix, did you
16 want to -- you're nodding. Did you want to add something to
17 that?

18 **MS. JULIE LACROIX:** I think I would just add
19 for context and clarification, in the administration we are
20 agents of the senate and the senators, and, therefore, we
21 take our direction from senators. So we would bring it to
22 our board and then we would take direction on the way
23 forward.

24 **MR. SUJIT CHOUDHRY:** So that's helpful. So
25 maybe I'll just want to -- Madam Commissioner, how much more
26 time do I have?

27 **COMMISSIONER HOGUE:** You have another five
28 minutes.

1 **MR. SUJIT CHOUDHRY:** Okay. So I just want to
2 pursue a point with you on this if I could because this is
3 helpful. So last week we had -- sorry ---

4 **COMMISSIONER HOGUE:** Thanks.

5 **MR. SUJIT CHOUDHRY:** Yes, I'll learn.
6 Anyway, so last week we had testimony from two members of
7 Parliament, so from the other place, misters -- Messieurs
8 McKay and Genius, who had also been targeted by the same
9 attack. And their evidence was the following, that this was
10 obviously, this attack was an interference with their
11 parliamentary privilege, which I don't think is in dispute.
12 But they also agreed with the following two points, that they
13 felt that the government had violated their parliamentary
14 privilege by not warning them of the attack and also by not
15 adequately protecting them of the attack. And so what I want
16 to do is link those answers to what you just said about
17 bringing this to the Board of Internal Economy and how you
18 take your direction from the senators, which is a helpful
19 framing. Is it fair to say that the -- your kind of
20 reporting or accountability mechanisms within the senate are
21 rooted in the idea that, ultimately, your administration is
22 there to protect and implement the privileges of the senate
23 as a body collectively but also its members individually?

24 **MS. JULIE LACROIX:** Correct. Our job is to
25 ensure the safety and security of the senate and senators as
26 a whole, and to balance any mitigation measures we have with
27 their requirements and need to -- needs in order to execute
28 their parliamentary functions.

1 MR. DAVID VATCHER: I ---

2 MR. SUJIT CHOUDHRY: Mr. Vatcher? Yes?

3 MR. DAVID VATCHER: --- I would add that I am
4 not an expert on ---

5 MR. SUJIT CHOUDHRY: Sure

6 MR. DAVID VATCHER: --- parliamentary
7 privilege. I really am not. I'm the IT guy and, you know,
8 so my response would be that I want to make sure that
9 senators can do their job to the fullest. And I want to take
10 any things that hampers their ability to do their job to the
11 fullest out of the way. So I'm not going to speak to
12 parliamentary privilege on that end.

13 MR. SUJIT CHOUDHRY: Sure. And I thought
14 about that when I was posing the question, but you can
15 understand why we're interested in the legal basis for all
16 these responsibilities you have. And so for the record, I'll
17 just wrap up here, we've put into -- I'd like to just mark as
18 an exhibit to your cross-examination JKW169. That's the
19 relevant chapter from Senate Procedure and Practice, Chapter
20 11. That actually sets out the privileges of the senate, and
21 it's those ideas that I was referring to.

22 --- EXHIBIT No. JKW0000169:

23 Senate Procedure - Chapter 11

24 Privileges and Immunities

25 MR. SUJIT CHOUDHRY: Anyway, thank you for
26 your time. Have a good day.

27 COMMISSIONER HOGUE: Thank you.

28 Mr. Harland for Michael Chong.

1 **--- CROSS-EXAMINATION BY MR. FRASER HARLAND:**

2 **MR. FRASER HARLAND:** Good morning,
3 Commissioner. I'm going to pick up a little bit where my
4 friend, Mr. Choudhry, left off because I also have some
5 questions about the APT31 cyber attack. So if I could ask
6 the Court Operator to pull up WIT126, please? Either
7 language is fine. If we can go to paragraph 29. So it
8 indicates here, Mr. Vatcher, that:

9 "The information service and we knew
10 that the malware had been sent by
11 email." (As read)

12 No, paragraph 30, sorry.

13 "That they learned in June 2024 that
14 the security -- IT security team of
15 the House of Commons had been led by
16 APT31." (As read)

17 So it was the House of Commons that informed
18 you of this, correct, at the time?

19 **MR. DAVID VATCHER:** Correct.

20 **MR. FRASER HARLAND:** And were you informed by
21 CSIS or by any other government department that APT31 was
22 responsible for ---

23 **MR. DAVID VATCHER:** I was not.

24 **MR. FRASER HARLAND:** Thank you. And I think
25 you said in a response to the Commissioner's question that
26 you did not inform senators of that at the time, unless they
27 came to you and asked for any clarity on the attack; is that
28 right?

1 **MR. DAVID VATCHER:** Correct. So in May or
2 June of this year, I did not reach out to the senators who
3 were targeted by the attack in January 2021; however, I did
4 respond to questions from one of the senators to their
5 satisfaction.

6 **MR. FRASER HARLAND:** Okay. And Mr. Choudhry
7 mentioned MP McKay and MP Genius, who were very clear that
8 they want to be informed of incidents like this. Would it be
9 fair to say that that would also be true for senators?

10 **MR. DAVID VATCHER:** I can't speak on the part
11 of senators, of course.

12 **MR. FRASER HARLAND:** Fair enough. Have any
13 senators made you aware that they would want to be informed
14 of attacks like this in the future?

15 **MR. DAVID VATCHER:** I think that senators
16 always want to be informed, and at the same times, I think
17 that senators receive a lot of information, and there's -- I
18 mean, I'm completely transparent, and when asked by senators
19 to provide more information, I always do. And if that -- if
20 there was a ruling by CIBA steering to that effect, I would,
21 of course, comply. I'm not trying to hide anything from
22 anybody. I'm just -- this was -- this attack happened two-
23 and-a-half years ago. It was thwarted. There was no damage.
24 So I would leave it to senators to ask me if they wish to
25 have any more information. I mean, I have no issue with
26 that.

27 **MR. FRASER HARLAND:** Understood. That's very
28 helpful. So do I understand that there's not a policy or

1 directive in place from that steering committee to inform
2 senators of attacks like the APT31 incident?

3 **MR. DAVID VATCHER:** For a spear phishing
4 attack like that, I do not have -- that only attacked a small
5 minority of senators. I do not have that requirement.
6 However, that attack was made available in our quarterly
7 reports on cyber security, which are internal documents.

8 **MR. FRASER HARLAND:** But in that -- so what
9 we and the Commission are most interested in is that this was
10 an attack from a foreign state. So that's the part -- was
11 that known in that -- made known in that document? Or just
12 that it was a spear phishing attack?

13 **MR. DAVID VATCHER:** In 2021 it was made known
14 that it was a spear phishing attack. And recently, we
15 updated, of course, accordingly with the knowledge that we
16 gained.

17 **MR. FRASER HARLAND:** Okay. So without a
18 policy like that in place, it remains possible that a future
19 attack from a foreign state like this could happen and
20 senators would not be informed? Is that fair?

21 **MR. DAVID VATCHER:** What I will say is that
22 should the events occur once more, the result would be the
23 same.

24 **MR. FRASER HARLAND:** Okay. Those are my
25 questions. Thank you, Commissioner.

26 **COMMISSIONER HOGUE:** Thank you.

27 Ms. Teich for the Human Rights Coalition.

28 **--- CROSS-EXAMINATION BY MS. SARAH TEICH:**

1 **MS. SARAH TEICH:** Good morning. I'll be
2 directing all my questions to Mr. Vatcher as well.

3 Mr. Vatcher, are you aware, generally
4 speaking, that foreign state actors may also be interested in
5 targeting particular human rights defenders and activists,
6 including members of vulnerable diaspora communities?

7 **MR. DAVID VATCHER:** They may. I really -- my
8 main concern is to protect the Senate, senators, and I'm
9 sorry, but I don't have much time to dedicate to other
10 protections or other worries, but I do understand that
11 they'll hit whatever they don't like; right?

12 **MS. SARAH TEICH:** Okay. If a senator's
13 device or email is targeted by -- particularly by a foreign
14 state actor, and then that senator is using that device or
15 email to communicate with members of diaspora communities, do
16 you see it as a risk that those diaspora community members
17 might have their devices compromised as a result?

18 **MR. DAVID VATCHER:** There are a lot of ifs in
19 your question.

20 **MS. SARAH TEICH:** I know.

21 **MR. DAVID VATCHER:** I'm not sure what to
22 reply to your question because in fact, it was an
23 unsuccessful attack against a handful of senators. We made
24 sure that all of their devices were not compromised as part
25 of our routine verifications. And so your question is --
26 calls for me to speculate, and I don't think I should.

27 **MS. SARAH TEICH:** Okay. I appreciate that.
28 I'm not asking particularly about the APT31 attack. I'm

1 speaking generally, just, you know, using your expertise.
2 But I appreciate that your focus is on senators.

3 When you conduct your forensic investigations
4 after the fact, and you mentioned in examination in-chief,
5 and I hope I'm getting this right, that you communicate, you
6 collaborate with members of the security intelligence
7 agencies as well. If there's a scenario where there may be
8 the sort of downstream impacts on contacts of a senator
9 targeted, do you think, would it fall to the security and
10 intelligence agency then and not the Senate administration to
11 potentially offer protection to those community members?

12 MR. DAVID VATCHER: No.

13 MS. SARAH TEICH: Why not?

14 MR. DAVID VATCHER: The Senate is an
15 independent institution and I do not believe that external
16 government entities should manage security for our devices.

17 MS. SARAH TEICH: Okay. If not the Senate
18 administration, would it be valuable for another agency to
19 offer that kind of support?

20 MR. DAVID VATCHER: I don't see why. Why
21 would it be -- I'm sorry.

22 MS. SARAH TEICH: Sorry, maybe I'm not being
23 clear. Not to senators, but to potentially the contacts of
24 senators, who may have their devices compromised as a result
25 of the attack on senators?

26 MR. DAVID VATCHER: I'm -- I don't know what
27 to answer to that.

28 MS. SARAH TEICH: Okay. Those are my

1 questions. Thank you.

2 COMMISSIONER HOGUE: Thank you.

3 Next one is Maitre Sirois for the RCDA.

4 --- CROSS-EXAMINATION BY MR. GUILLAUME SIROIS:

5 MR. GUILLAUME SIROIS: Guillaume Sirois from
6 the Russian-Canadian Democratic Alliance.

7 126 French version, please. Paragraph 24.

8 Just a few words about the service denial
9 attack that took place, and it was thought that Russian
10 actors were involved. When were you told that this cyber
11 attack had been performed by Russian actors?

12 MR. DAVID VATCHER: Well, there were several
13 instances of this service denial incident on our external
14 website. In each case, of course, we have tools in order to
15 monitor the number of external connections on our site. And
16 when something happens, I am informed if it is abnormal and
17 the required action is taken in order to counter the attack.
18 So it is almost immediately that I'm informed, but it is
19 quite regular sometimes.

20 MR. GUILLAUME SIROIS: Do you know when, in
21 which month?

22 MR. DAVID VATCHER: Sorry. I don't have this
23 information.

24 MR. GUILLAUME SIROIS: But as soon as you
25 were informed, when were you told that Russian sympathizers
26 were involved?

27 MR. DAVID VATCHER: Well, the way these cyber
28 attacks are performed, there are some technological

1 components, some specificity that allow us to identify the
2 source of the cyber attack. And in the case of some groups,
3 they are quite vocal about how they want to use social media
4 to say that they are responsible for these cyber attacks.

5 **MR. GUILLAUME SIROIS:** According to the
6 summary of your interview, in terms of delay, how long does
7 it take before the moment you know that an attack took place
8 and then through technological information or social media
9 when you learn that Russian actors were involved? What's the
10 timeline?

11 **MR. DAVID VATCHER:** Well, not much time. We
12 know that a cyber attack is taking place. We know that it's
13 very similar to a previous attack. There are
14 characteristics. And I won't deal into various details, but
15 these elements allow us to conclude that this or that group
16 is involved. And it's almost an immediate conclusion.

17 **MR. GUILLAUME SIROIS:** And in that context,
18 it's the same reaction for the Senate, so whether we deal
19 with Russian or other foreign actors, the answer is the same,
20 whatever the source?

21 **MR. DAVID VATCHER:** Yes, absolutely.

22 **MR. GUILLAUME SIROIS:** Now, I understand that
23 getting in touch with partners in terms of safety issues is
24 not useful for the Senate, but seeing that you are aware of
25 this kind of cyber attacks, don't you think that it might be
26 useful for these entities?

27 **MR. DAVID VATCHER:** They know. They know
28 about it.

1 **MR. GUILLAUME SIROIS:** How can you say that
2 they know if you are not in touch with them?

3 **MR. DAVID VATCHER:** Well, when there are
4 cyber attacks against Canadian government entities,
5 organizations, we are talking about public events in the
6 sense that these people are making it public and they are not
7 hiding anything, and we are not hiding anything. We know
8 that something happened. I don't have evidence that they are
9 aware, you are right about that, but I think that they are
10 aware that other government entities are aware.

11 **MR. GUILLAUME SIROIS:** But don't you think,
12 you are the target of an attack, and maybe some information
13 might be useful for these agencies to pursue their
14 investigations or for reprisals and so on?

15 **MR. DAVID VATCHER:** Yes, absolutely. But I
16 don't want to say that we are not discussing with these
17 agencies about these cyber attacks. Members of my team are
18 working with external entities and I wouldn't be surprised
19 that these attacks were discussed, but it's not -- during the
20 attack as such, I don't think that we are telling them "Be
21 careful" because we think that we are the target of an attack
22 by this or that group.

23 **COMMISSIONER HOGUE:** When you say that these
24 groups are gloating about it, are there claims about an
25 attack as such?

26 **MR. DAVID VATCHER:** Absolutely.

27 **COMMISSIONER HOGUE:** So they are gloating and
28 saying yes, we are responsible for this or that attack?

1 **MR. DAVID VATCHER:** Yes.

2 **COMMISSIONER HOGUE:** And now the Concern
3 Group. Mr. Chantler.

4 **--- CROSS-EXAMINATION BY MR. NEIL CHANTLER:**

5 **MR. NEIL CHANTLER:** Good morning. My name is
6 Neil Chantler. I'm counsel for the Chinese Canadian Concern
7 Group. I'm going to ask you both questions about sponsored
8 travel, insofar as it relates to your mandates.

9 Could the Court Reporter please call up
10 WIT.126, the English version, page 11, paragraph 66?

11 In your interview summary tendered earlier
12 today, you describe, at paragraph 66, a Senate motion
13 advanced by Senator Raymonde Saint-Germaine. And as you
14 described the motion, the motion is passed, but authorized
15 the Standing Committee on Ethics and Conflicts of Interest to
16 study changes to regulations around sponsored travel. This
17 motion is undergoing the adoption process in the Senate.

18 And you're aware, and you describe at
19 paragraph 67 of your interview summary, that this motion was
20 introduced last spring following the release of the Special
21 Report on Foreign Interference released by the National
22 Security and Intelligence Committee of parliamentarians,
23 NSICOP. You're aware of that and you've stated it in your
24 interview summaries; correct?

25 **MR. DAVID VATCHER:** I'm sorry, ---

26 **MS. JULIE LACROIX:** We're aware in general
27 terms. Correct.

28 **MR. DAVID VATCHER:** Yes.

1 **MR. NEIL CHANTLER:** Okay. And that report
2 reported on intelligence that suggests there are
3 parliamentarians who are witting participants in efforts of
4 foreign states to interfere with our democracy. You're aware
5 of that general finding? Either of you.

6 **COMMISSIONER HOGUE:** Are you?

7 **MS. JULIE LACROIX:** No, I think for specifics
8 on this motion, you would need to direct the questions to
9 either the Standing Committee on Ethics and Conflicts of
10 Interest or Senator Sainte-Germain.

11 **MR. NEIL CHANTLER:** I'm asking about the
12 NSICOP report and your general awareness of that finding.

13 **MR. DAVID VATCHER:** I'm ---

14 **MS. JULIE LACROIX:** I'm not aware.

15 **MR. DAVID VATCHER:** I'm sorry. I'm not
16 aware.

17 **MR. NEIL CHANTLER:** You're not aware that
18 that committee found there are witting participants among
19 parliamentarians in assisting foreign states?

20 **MS. JULIE LACROIX:** I've not read the report.

21 **MR. NEIL CHANTLER:** And you're not aware of
22 news reports that have reported on these very significant
23 allegations?

24 **MR. DAVID VATCHER:** Of course I listen to the
25 news, but I mean I have not read the report myself.

26 **MR. NEIL CHANTLER:** Are you aware that the
27 NSICOP report identified sponsored foreign travel as a
28 particular vulnerability for parliamentarians?

1 **MR. DAVID VATCHER:** Once again, mostly
2 through the news, but yes, I understand that.

3 **MR. NEIL CHANTLER:** And do you accept or
4 understand that that's had a negative impact on the trust
5 Canadians may have and the work that Senators may undergo on
6 sponsored trips to places like China where the country has a
7 demonstrated interest in interfering with Canadian political
8 affairs?

9 **MR. DAVID VATCHER:** I understand these
10 things, sir, but frankly my concern is in protecting senators
11 from outside attacks and I really can't speak to senators and
12 the way they're acting or behaving. My job is to protect
13 their ability to do their work and I can't speak to them
14 being -- whatever.

15 **MR. NEIL CHANTLER:** If I understand correctly
16 though, the issue of security around senators' sponsored
17 travel is within both of your mandates; correct?

18 **MR. DAVID VATCHER:** We ---

19 **MS. JULIE LACROIX:** Correct. We share ---

20 **MR. DAVID VATCHER:** Yeah.

21 **MS. JULIE LACROIX:** --- responsibilities for
22 David with respect to the IT component.

23 **MR. NEIL CHANTLER:** Well you both undergo --
24 or I apologize, the CSD undergoes a process of risk
25 assessment, ---

26 **MS. JULIE LACROIX:** Yes.

27 **MR. NEIL CHANTLER:** --- you help to educate a
28 senator prior to travel on the risks of that foreign country,

1 you provide information about how to be safe in the foreign
2 country, you give advice on best practices, on how to use
3 electronic devices, and so on. And you'd both agree that
4 those are critically important -- that's critically important
5 information for a senator to have before ---

6 **MS. JULIE LACROIX:** Yes.

7 **MR. NEIL CHANTLER:** --- undergoing a trip
8 like that?

9 **MS. JULIE LACROIX:** Yeah.

10 **MR. NEIL CHANTLER:** And when a senator
11 accepts sponsored foreign travel, often it's the foreign
12 state or a foreign interest group that is paying for that
13 travel and making the arrangements for the senator? Is that
14 correct?

15 **MS. JULIE LACROIX:** I can't comment on that.

16 **MR. NEIL CHANTLER:** I mean, by its very
17 nature, the sponsored travel is being paid for by a foreign
18 entity?

19 **MR. DAVID VATCHER:** That would be the
20 definition of a sponsored trip.

21 **MR. NEIL CHANTLER:** Right. And in
22 circumstances like that, would you agree that there's a
23 heightened risk to the safety and security of the travelling
24 senator, perhaps heightened risks of espionage, entrapment,
25 and other forms of foreign interference?

26 **MS. JULIE LACROIX:** I would agree in general
27 terms that throughout the assessment, those are all
28 considerations that will form part of the assessment and

1 mitigation measures put in place.

2 **MR. NEIL CHANTLER:** So there's a heightened
3 element of risk to sponsored foreign travel is what I'm
4 getting at?

5 **Ms. JULIE LACROIX:** I would say there's an
6 element of risk that's considered.

7 **MR. NEIL CHANTLER:** So in light of that
8 recognition and the findings of the NSICOP report, do you
9 think there's a case to be made to restrict sponsored travel
10 by senators, at the very least, at the very least, for
11 reasons of security?

12 **MS. JULIE LACROIX:** That would be a decision
13 for senators. I take my direction from senators.

14 **MR. NEIL CHANTLER:** Would it make your job of
15 keeping senators safe easier?

16 **MS. JULIE LACROIX:** I ---

17 **MR. DAVID VATCHER:** It would not, ---

18 **MS. JULIE LACROIX:** No.

19 **MR. DAVID VATCHER:** --- but like my colleague
20 mentioned, that's a decision for senators.

21 **MS. JULIE LACROIX:** M'hm.

22 **MR. DAVID VATCHER:** Very well. Thank you.

23 **COMMISSIONER HOGUE:** Thank you.

24 AG.

25 **--- CROSS-EXAMINATION BY MS. RYANN ATKINS:**

26 **MS. RYANN ATKINS:** Good morning. My name is
27 Ryann Atkins for the Attorney General of Canada.

28 You note in your witness statement that the

1 senate administration collaborates quite closely with the
2 sergeant-at-arms of the House of Commons. Is that right?

3 **MS. JULIE LACROIX:** Correct.

4 **MS. RYANN ATKINS:** Does that extend also to
5 cyber security and IT matters?

6 **MR. DAVID VATCHER:** It does.

7 **MS. RYANN ATKINS:** And I might get the
8 terminology wrong because I'm not an IT guy, so maybe you
9 could help me out, but am I correct that the Senate IT
10 systems reside on a system that is owned and managed by the
11 House of Commons?

12 **MR. DAVID VATCHER:** That is incorrect.

13 **MS. RYANN ATKINS:** No? Okay. But in any
14 event, the Senate IT and House of Commons IT have a
15 collaborative relationship?

16 **MR. DAVID VATCHER:** We do.

17 **MS. RYANN ATKINS:** And you share information
18 about cyber attacks?

19 **MR. DAVID VATCHER:** We do.

20 **MS. RYANN ATKINS:** And you're aware, I take
21 it, that the House of Commons has a memorandum of
22 understanding with the CSE?

23 **MR. DAVID VATCHER:** I am.

24 **MS. RYANN ATKINS:** The Senate does not have a
25 similar MOU; correct?

26 **MR. DAVID VATCHER:** Correct.

27 **MS. RYANN ATKINS:** And the relationship
28 between the Senate and the House of Commons is such that you

1 would expect that if the House of Commons received
2 information that was relevant to your IT systems or the
3 protection of senators, that they would share that
4 information with you?

5 **MR. DAVID VATCHER:** Absolutely.

6 **MS. RYANN ATKINS:** And ---

7 **MR. DAVID VATCHER:** And they have.

8 **MS. RYANN ATKINS:** Sorry, go ahead?

9 **MR. DAVID VATCHER:** And they have.

10 **MS. RYANN ATKINS:** And they have. Yes. I
11 anticipate there will be evidence based on the Appendix to
12 the House of Commons Summary, that I anticipate will be
13 entered into evidence at some point today, that the House of
14 Commons digital services cannot share MPs' information
15 without prior consent. Is that the same for the Senate
16 administration with respect to senators' information?

17 **MS. JULIE LACROIX:** Correct.

18 **MS. RYANN ATKINS:** Okay. I want to talk to
19 you about the cyber incident in January 2021 by the threat
20 actor known as APT31. And you noted in your testimony that
21 this incident was not successful, the attack was thwarted.
22 Correct?

23 **MR. DAVID VATCHER:** Correct.

24 **MS. RYANN ATKINS:** And you were informed of
25 this incident by the House of Commons?

26 **MR. DAVID VATCHER:** Yes.

27 **MS. RYANN ATKINS:** And am I correct that your
28 team would have been responsible for linking the IP addresses

1 of the systems that were attacked to the specific Senators
2 that were being targeted?

3 MR. DAVID VATCHER: Yes.

4 MS. RYANN ATKINS: Okay. And so to put it
5 another way, the security agencies may have had the IP
6 addresses, but it was your team who would have identified the
7 specific Senators.

8 MR. DAVID VATCHER: Correct.

9 MS. RYANN ATKINS: And did you receive
10 consent from the Senators to share their names with CSE or
11 any other government agency?

12 MR. DAVID VATCHER: At that point, we were
13 informed that -- we were informed which parliamentarians were
14 already targeted, so we didn't share that information; that
15 information was given to us.

16 MS. RYANN ATKINS: By the House of Commons?

17 MR. DAVID VATCHER: Correct.

18 MS. RYANN ATKINS: Okay. But in any event,
19 you weren't -- you didn't obtain consent to share it with the
20 CSE or CSIS, for example?

21 MR. DAVID VATCHER: No, but once again, it
22 was shared with us. We didn't share it; it was shared with
23 us.

24 MS. RYANN ATKINS: Okay. But sitting here
25 today you don't know if the House of Commons shared that
26 information with government agencies?

27 MR. DAVID VATCHER: I do not.

28 MS. RYANN ATKINS: Okay. And the Cyber

1 Centre -- you note in your summary that the Cyber Centre
2 didn't provide any information to the Senate Administration
3 about who might have been behind the attacks. Did the House
4 of Commons relay that information to you?

5 **MR. DAVID VATCHER:** Correct, the House of
6 Commons relayed that information to us.

7 **MS. RYANN ATKINS:** The House of Commons
8 relayed to you that the attack was perpetrated by APT31?

9 **MR. DAVID VATCHER:** In May or June of this
10 year, the House -- I believe the House of Commons did.

11 **MS. RYANN ATKINS:** Okay. I anticipate we're
12 going to hear evidence of a meeting on February 17th, 2021,
13 between security agencies and House of Commons Administration
14 at which the identity of the threat actor was shared with the
15 House of Commons, as well as country-specific tactics and
16 targets. Did anyone from the Senate Administration attend
17 that meeting?

18 **MR. DAVID VATCHER:** No.

19 **MS. RYANN ATKINS:** And did the House of
20 Commons share the information that was relayed to them at
21 that meeting with the Senate?

22 **MR. DAVID VATCHER:** Please let me rephrase;
23 nobody from my Directorate attended that meeting. I don't
24 know, I can't speak for other Directorates.

25 **MS. RYANN ATKINS:** Ms. Lacroix, are you aware
26 of anyone from the Senate attending that meeting?

27 **MS. LACROIX:** I'm not at this time.

28 **MS. RYANN ATKINS:** Okay. And following that

1 meeting, did anyone from the House of Commons share with you
2 the information that was relayed at that meeting?

3 **MR. DAVID VATCHER:** Not to my recollection.

4 **MS. RYANN ATKINS:** Okay. The House of
5 Commons -- I anticipate we're going to hear that the House of
6 Commons relayed to the security agencies that some of its
7 members, members of Parliament, may have received similar
8 messages on their personal email addresses. Did the House of
9 Commons deliver that same message to the Senate?

10 **MR. DAVID VATCHER:** I don't remember that
11 they did.

12 **MS. RYANN ATKINS:** Okay. And when the Senate
13 reached out to the specific Senators who were targeted, were
14 they told to check their personal email addresses or devices
15 with similar emails?

16 **MR. DAVID VATCHER:** I would not be surprised.

17 **MS. RYANN ATKINS:** Okay.

18 **MR. DAVID VATCHER:** But I can't -- I don't
19 know the details of those conversations, what exactly was
20 said.

21 **MS. RYANN ATKINS:** Is that part of the
22 general advice and training on cyber security that Senators
23 receive?

24 **MR. DAVID VATCHER:** Yes.

25 **MS. RYANN ATKINS:** Thank you. Those are my
26 questions.

27 **COMMISSIONER HOGUE:** Thank you.

28 For the Senate it's Maître Roy and Maître

1 Clair.

2 MR. MARC-ANDRÉ ROY: No, no questions.

3 COMMISSIONER HOGUE: We'll resume -- [No
4 interpretation]?

5 MR. GABRIEL POLIQUIN: I don't have any
6 questions for re-direct, but I would like to say that Me
7 Choudhry said that there's paragraphs the English form in 26
8 doesn't have its number, so that may have created an offset
9 in terms of the numbering.

10 COMMISSIONER HOGUE: But all of the
11 information is there.

12 MR. GABRIEL POLIQUIN: That's right.

13 COMMISSIONER HOGUE: Well, thank you very
14 much.

15 Have a good day. You're free to go.

16 MR. GABRIEL POLIQUIN: Thank you.

17 COMMISSIONER HOGUE: So we're going to take a
18 break now. We'll take a 20-minute break. We'll resume at
19 11:15.

20 THE REGISTRAR: Order, please.

21 The sitting of the Commission is now in
22 recess until 11:15 a.m.

23 --- Upon recessing at 10:55 a.m.

24 --- Upon resuming at 11:18 a.m.

25 THE REGISTRAR: Order, please.

26 This sitting of the Foreign Interference
27 Commission is now back in session.

28 The time is 11:18 a.m.

1 **COMMISSIONER HOGUE:** [No interpretation]

2 **MR. HAMZA MOHAMADHOSSEN:** Commissioner.

3 For the record, it's Hamza Mohamadhossen for
4 the Commission.

5 Commissioner, the witnesses before you are
6 representatives from the House of Commons, Mr. Patrick
7 McDonell and Me Benoît Dicaire.

8 Mr. Registrar, I would ask that both
9 witnesses please be sworn.

10 **THE REGISTRAR:** We'll start with Mr.
11 McDonell. Could you please state your full name and then
12 please spell your last name for the record?

13 **MR. PATRICK McDONELL:** My full name is
14 Patrick Ewen McDonell. McDonell is spelled M-C-D-O-N-E-L-L.

15 **--- MR. PATRICK EWEN McDONELL, Affirmed:**

16 **THE REGISTRAR:** Thank you.

17 Now, I'll proceed with Mr. Dicaire. Could
18 you please state your full name and spell your last name for
19 the record?

20 **MR. BENOÎT DICAIRE:** My full name is Benoît
21 Eugène Dicaire. And my last name is spelled D-I-C-A-I-R-E.

22 **--- MR. BENOÎT EUGÈNE DICAIRE, Affirmed:**

23 **THE REGISTRAR:** Thank you, Mr. Dicaire.

24 Counsel, you may proceed.

25 **--- EXAMINATION IN-CHIEF BY MR. HAMZA MOHAMADHOSSEN:**

26 **MR. HAMZA MOHAMADHOSSEN:** Mr. McDonell, do
27 you recall attending an interview with Commission counsel on
28 September 3rd, 2024?

1 **MR. PATRICK McDONELL:** I do.

2 **MR. HAMZA MOHAMADHOSSEN:** And a summary was
3 generated following that interview?

4 **MR. PATRICK McDONELL:** Yes.

5 **MR. HAMZA MOHAMADHOSSEN:** Court Operator,
6 could we please pull up document WIT128.BIL, please? And the
7 document on screen is the summary that was generated from
8 your interview?

9 **MR. PATRICK McDONELL:** Yes, it appears so.

10 **MR. HAMZA MOHAMADHOSSEN:** And you've had a
11 chance to review that summary for accuracy?

12 **MR. PATRICK McDONELL:** I had that opportunity
13 to review it, yes.

14 **MR. HAMZA MOHAMADHOSSEN:** And do you have any
15 corrections, additions, or any other modifications to make
16 today?

17 **MR. PATRICK McDONELL:** I do not.

18 **MR. HAMZA MOHAMADHOSSEN:** And do you adopt
19 the contents of the witness summary as part of your evidence
20 today before the Commission?

21 **MR. PATRICK McDONELL:** I do.

22 **MR. HAMZA MOHAMADHOSSEN:** Thank you.

23 Me Dicaire, I'll ask you the same questions.
24 Do you recall attending an interview with Commission counsel
25 on September 3rd, 2018 -- sorry, 2014 -- sorry, 2024?

26 **MR. BENOÎT DICAIRE:** Twenty twenty-four
27 (2024)?

28 **MR. HAMZA MOHAMADHOSSEN:** Twenty Twenty-four

1 (2024).

2 MR. BENOÎT DICAIRE: Yes, I do.

3 MR. HAMZA MOHAMADHOSSEN: And the document on
4 screen is the summary that was generated from your interview
5 with Commission counsel?

6 MR. BENOÎT DICAIRE: Yeah.

7 MR. HAMZA MOHAMADHOSSEN: And you've reviewed
8 the summary for accuracy?

9 MR. BENOÎT DICAIRE: I did.

10 MR. HAMZA MOHAMADHOSSEN: Do you have any
11 corrections, additions, or deletions to make today?

12 MR. BENOÎT DICAIRE: I don't.

13 MR. HAMZA MOHAMADHOSSEN: And do you adopt
14 the contents of the witness summary as part of your evidence
15 before the Commission?

16 MR. BENOÎT DICAIRE: I do.

17 MR. HAMZA MOHAMADHOSSEN: Thank you.

18 So we will have this bilingual summary
19 entered into evidence as the next exhibit for the record.
20 The full English version of the summary can be found at
21 WIT128.EN, and the full French version is at WIT128.FR.
22 These two documents will also go into the record as the next
23 exhibits.

24 **--- EXHIBIT No. WIT0000128.EN:**

25 Interview Summary: House of Commons
26 Administration (Patrick McDonell and
27 Benoît Dicaire)

28 **--- EXHIBIT No. WIT0000128.BIL:**

1 Interview Summary: House of Commons
2 Administration (Patrick McDonell and
3 Benoît Dicaire)

4 **--- EXHIBIT No. WIT0000128.FR:**

5 Résumé d'entrevue : Administration de
6 la Chambre des communes (Patrick
7 McDonell et Benoît Dicaire)

8 **MR. HAMZA MOHAMADHOSSEN:** Mr. Dicaire, you
9 were also interviewed in a secured setting on September 17th,
10 along with your colleague, Mr. Hedi Touati. Correct?

11 **MR. BENOÎT DICAIRE:** Correct.

12 **MR. HAMZA MOHAMADHOSSEN:** And an interview
13 summary was generated following this secured interview?

14 **MR. BENOÎT DICAIRE:** Correct.

15 **MR. HAMZA MOHAMADHOSSEN:** Court Operator,
16 could we please pull up WIT129.EN? And have you had a chance
17 to review the summary that's on screen?

18 **MR. BENOÎT DICAIRE:** I did.

19 **MR. HAMZA MOHAMADHOSSEN:** And do you have any
20 corrections, additions, or modifications to make today to
21 that summary?

22 **MR. BENOÎT DICAIRE:** No.

23 **MR. HAMZA MOHAMADHOSSEN:** And do you adopt
24 the contents of this summary as part of your evidence before
25 the Commission today?

26 **MR. BENOÎT DICAIRE:** Yes.

27 **MR. HAMZA MOHAMADHOSSEN:** Thank you.

28 For the record, the French version of this

1 summary is at WIT129.FR, and both versions will be entered
2 into evidence as the next two exhibits.

3 **--- EXHIBIT No. WIT0000129.EN:**

4 Appendix to Interview Summary: House
5 of Commons Administration (Hedi
6 Touati and Benoît Dicaire)

7 **--- EXHIBIT No. WIT0000129.FR:**

8 Complément au résumé d'entrevue:
9 Administration de la Chambre des
10 communes (Hedi Touati and Benoît
11 Dicaire)

12 **MR. HAMZA MOHAMADHOSSEN:** Finally, I
13 understand that the House of Commons prepared an
14 institutional report at the request of the Commission.
15 Correct?

16 **MR. BENOÎT DICAIRE:** Correct.

17 **MR. HAMZA MOHAMADHOSSEN:** And I would ask
18 that HOC1.EN please be brought up to the screen. And is this
19 the institutional report that was prepared by the House of
20 Commons?

21 **MR. BENOÎT DICAIRE:** Correct.

22 **MR. HAMZA MOHAMADHOSSEN:** And you have had an
23 opportunity to review the IR?

24 **MR. BENOÎT DICAIRE:** Yes.

25 **MR. HAMZA MOHAMADHOSSEN:** And do you adopt
26 the institutional report as part of the evidence of the House
27 of Commons for the purposes of this Commission?

28 **MR. BENOÎT DICAIRE:** We do.

1 **MR. HAMZA MOHAMADHOSSEN:** Great. For the
2 record the French language version is at HOC1.FR, and we will
3 have both versions of the institutional report be entered
4 into evidence as the next two exhibits.

5 **--- EXHIBIT No. HOC0000001.EN:**

6 Institutional Report of the House of
7 Commons Administration

8 **--- EXHIBIT No. HOC0000001.FR:**

9 Rapport institutionnel de
10 l'administration de la Chambre des
11 Communes

12 **MR. HAMZA MOHAMADHOSSEN:** So this morning I
13 will be focussing mainly on physical security, and my
14 colleague Me Poliquin will be covering relationships with
15 government, IT matters, as well as briefings to MPs. And for
16 all other topics, including the structure of the House of
17 Commons administration, we refer the Commission and
18 participants to the IR and the witness summaries that were
19 just entered into the record.

20 So Mr. McDonell, what is your current role at
21 the House of Commons?

22 **MR. PATRICK McDONELL:** I'm the Sergeant-at-
23 Arms at the House of Commons, and also oversee corporate
24 security.

25 **MR. HAMZA MOHAMADHOSSEN:** Can you please
26 describe the responsibilities associated with those two
27 roles?

28 **MR. PATRICK McDONELL:** Sergeant-at-Arms role

1 is for the most part ceremonial. And the Corporate Security,
2 we oversee the safety and security of members of Parliament
3 off the hill.

4 **MR. HAMZA MOHAMADHOSSEN:** Okay. Before you
5 joined the House of Commons, can you provide us with a brief
6 overview of your professional experiences?

7 **MR. PATRICK McDONELL:** I spent 30 and a half
8 years with the Royal Canadian Mounted Police, both in
9 contract and federal policing, and international policing. I
10 retired and moved on to Parliament Hill with the Senate,
11 became Director of their security services. After three
12 years I moved over to the House of Commons, did several
13 months as their Director of Security Services and then became
14 the Acting Sergeant-at-Arms in January of 2015, was appointed
15 the Sergeant-at-Arms in 2019, and was reappointed in July of
16 this year as Sergeant-at-Arms.

17 **MR. HAMZA MOHAMADHOSSEN:** Right. In your
18 interview summary you referenced the Parliamentary Protective
19 Services. Can you explain how the responsibilities of the
20 Parliamentary Protective Service differs from your
21 responsibilities when it comes to ensuring the safety of MPs?

22 **MR. PATRICK McDONELL:** Parliamentary
23 Protective Service is responsible for the security of MPs,
24 staff, employees, contractors, volunteers, anyone who comes
25 into the Parliamentary precinct, they are responsible for
26 their physical security.

27 **MR. HAMZA MOHAMADHOSSEN:** Okay. And what is
28 the geographical scope of your responsibility then?

1 **MR. PATRICK McDONELL:** Basically, beyond the
2 Wellington Wall and out in the communities. So I provide
3 residential security, constituency security, mobile duress
4 alarms, open source -- we do open-source intelligence,
5 technical surveillance countermeasures.

6 **MR. HAMZA MOHAMADHOSSEN:** Right, okay. We'll
7 get into all of that shortly. The Director of the PPS is not
8 a house official?

9 **MR. PATRICK McDONELL:** The Director of the
10 PPC is a Chief Superintendent in the Royal Canadian Mounted
11 Police.

12 **MR. HAMZA MOHAMADHOSSEN:** Perfect. Thank
13 you.

14 Mr. Dicaire, what is your current role at the
15 House of Commons?

16 **MR. BENOÎT DICAIRE:** My current role is Chief
17 Information Officer in the House of Commons.

18 **MR. HAMZA MOHAMADHOSSEN:** And can you please
19 describe the responsibilities associated with that role?

20 **MR. BENOÎT DICAIRE:** So I oversee a team
21 that's responsible for the IT infrastructure, the
22 applications, the broadcasts, webcast infrastructure, and
23 also our real property group and facilities group.

24 **MR. HAMZA MOHAMADHOSSEN:** Okay. And can you
25 please provide us with a brief overview of your professional
26 background prior to becoming CIO?

27 **MR. BENOÎT DICAIRE:** I've been an employee of
28 the House of Commons since October 2000, so 24 years. And

1 I've been responsible for various roles throughout this
2 tenure, namely as a DG of applications and also as a Director
3 of IT Infrastructure before.

4 **MR. HAMZA MOHAMADHOSSEN:** Okay. Thank you.

5 I'd like to focus in a bit on physical
6 security. So most of these questions will be directed to
7 you, Mr. McDonell.

8 Are there any teams under your supervision
9 that are either dedicated or engage with foreign interference
10 issues?

11 **MR. PATRICK McDONELL:** Yes. There would be
12 the RMI, Risk Management Investigators. They work hand in
13 hand with CSIS and the RCMP. There is my Technical
14 Surveillance Countermeasures team.

15 **MR. HAMZA MOHAMADHOSSEN:** M'hm.

16 **MR. PATRICK McDONELL:** And also, the open-
17 source work on foreign intelligence.

18 **MR. HAMZA MOHAMADHOSSEN:** Right. Can you
19 describe a little bit about the open-source monitoring
20 program?

21 **MR. PATRICK McDONELL:** The open-source
22 monitoring program is a team of analysts that scan the
23 internet using various software for threats against --
24 threats and harassment of members of Parliament.

25 **MR. HAMZA MOHAMADHOSSEN:** Right. Do they
26 receive support or information from other teams internal to
27 the House of Commons?

28 **MR. PATRICK McDONELL:** Yes, they do. From

1 the Risk Management Investigators.

2 **MR. HAMZA MOHAMADHOSSEN:** What about teams
3 external to the House of Commons?

4 **MR. PATRICK McDONELL:** The Risk Management
5 Investigative team works hand in hand with CSIS. They
6 regularly meet once a month.

7 **MR. HAMZA MOHAMADHOSSEN:** Okay. And in the
8 event that the open-source team detects a threat, what would
9 they do next?

10 **MR. PATRICK McDONELL:** If it's a physical
11 threat to a member of parliament they'll bring it to the
12 attention, or if they believe it's a physical threat, they'll
13 bring it to the attention of the risk management team who
14 work on a daily basis with the RCMP POC, Protective
15 Operations, ---

16 **MR. HAMZA MOHAMADHOSSEN:** M'hm.

17 **MR. PATRICK McDONELL:** --- and bring it to
18 their attention, and also the POJ, the police force of
19 jurisdiction. It's always the RCMP and the POJ who determine
20 if it is indeed a criminal offence.

21 If it's the harassment of an MP or a website
22 portraying an MP, for example, to -- in another light, like
23 an immigration centre or agent, which we receive often, or
24 see often on the web, they use the likeness of MPs on these
25 fraudulent sites, we bring it to the attention of the
26 platform provider.

27 **MR. HAMZA MOHAMADHOSSEN:** Okay. And would
28 you ever communicate those threats directly to the MP?

1 **MR. PATRICK McDONELL:** Yes. And the MP often
2 finds it before we do, ---

3 **MR. HAMZA MOHAMADHOSSEN:** Okay.

4 **MR. PATRICK McDONELL:** --- through an email
5 or Facebook, people using their image fraudulently. But we
6 converse with the MP in question ---

7 **MR. HAMZA MOHAMADHOSSEN:** Right.

8 **MR. PATRICK McDONELL:** --- and the Whip's
9 Office also.

10 **MR. HAMZA MOHAMADHOSSEN:** Okay. So you would
11 also notify the Whip's Office, I think I heard you say?

12 **MR. PATRICK McDONELL:** In most cases, yes.

13 **MR. HAMZA MOHAMADHOSSEN:** Okay. And does
14 that also include the House Leader? The MP's House Leader?

15 **MR. PATRICK McDONELL:** No, we'll go to the
16 respective Whips.

17 **MR. HAMZA MOHAMADHOSSEN:** Okay.

18 **MR. PATRICK McDONELL:** Yeah.

19 **MR. HAMZA MOHAMADHOSSEN:** At a high level,
20 and without getting into details, how often are there threats
21 to the physical security and safety of MPs?

22 **MR. PATRICK McDONELL:** Daily.

23 **MR. HAMZA MOHAMADHOSSEN:** Daily. Okay. And
24 to the extent that you're able to discuss in a public forum
25 here, can you describe the ways that your office ensures the
26 security of MPs off of Parliament Hill?

27 **MR. PATRICK McDONELL:** Okay. As I mentioned
28 earlier, we have a residential security program, both for

1 their primary and secondary residence.

2 **MR. HAMZA MOHAMADHOSSEN:** By secondary
3 residence, you're referring to what, exactly?

4 **MR. PATRICK McDONELL:** Their secondary
5 residence would be here in Ottawa. It doesn't cover a
6 cottage or anything. It's -- when they travel to Ottawa,
7 many stay in apartments. Some stay in hotels.

8 **MR. HAMZA MOHAMADHOSSEN:** M'hm.

9 **MR. PATRICK McDONELL:** I don't know if any
10 own a house in Ottawa, ---

11 **MR. HAMZA MOHAMADHOSSEN:** Right.

12 **MR. PATRICK McDONELL:** --- but the secondary
13 residence refers to the geographical area of Ottawa and
14 Gatineau.

15 **MR. HAMZA MOHAMADHOSSEN:** Great.

16 **MR. PATRICK McDONELL:** Constituency office
17 security. Some MPs have more than one constituency office.

18 **MR. HAMZA MOHAMADHOSSEN:** M'hm.

19 **MR. PATRICK McDONELL:** We provide members of
20 Parliament with mobile duress alarms, ---

21 **MR. HAMZA MOHAMADHOSSEN:** M'hm.

22 **MR. PATRICK McDONELL:** --- which are
23 geofenced, geofence meaning that when they press the "come
24 help me" button, we know whether -- exactly where they are
25 and which POJ, police force of jurisdiction, should respond,
26 or if they're on the Hill, that Parliamentary Protective
27 Service should be responding. We provide the mobile duress
28 alarm also to their partner if they request it.

1 Recently PPS is providing an escort when
2 requested, off and on -- onto and off the hill.

3 **MR. HAMZA MOHAMADHOSSEN:** M'hm.

4 **MR. PATRICK McDONELL:** If the MP wants to be
5 escorted to their place of residence in the Ottawa area.

6 **MR. HAMZA MOHAMADHOSSEN:** M'hm.

7 **MR. PATRICK McDONELL:** --- PPS will provide
8 that.

9 **MR. HAMZA MOHAMADHOSSEN:** And are you
10 involved at all with that process? Or is that entirely PPS?

11 **MR. PATRICK McDONELL:** No, that's entirely
12 PPS.

13 **MR. HAMZA MOHAMADHOSSEN:** Okay. I'd like to
14 shift to the next area of questioning, which is ---

15 **MR. PATRICK McDONELL:** Oh, if I may?

16 **MR. HAMZA MOHAMADHOSSEN:** I'm sorry.

17 **MR. PATRICK McDONELL:** And we also provide
18 event security if an MP is attending an event and requests
19 security at an event in relation to their parliamentary
20 duties, we'll provide security at that event and their
21 constituency.

22 **MR. HAMZA MOHAMADHOSSEN:** And that would
23 happen if they approach you first to request that security?

24 **MR. PATRICK McDONELL:** Yeah, we have a travel
25 and events section ---

26 **MR. HAMZA MOHAMADHOSSEN:** Okay.

27 **MR. PATRICK McDONELL:** --- who also do the
28 threat assessments on MPs' travel.

1 **MR. HAMZA MOHAMADHOSSEN:** Okay. I'd like to
2 shift to security screening for House of Commons personnel.

3 You indicate at paragraph 49 of your summary,
4 and I'm not going to bring it up, but if it's helpful, let me
5 know and I will call it. You indicate that your office is
6 responsible for conducting security screening of House of
7 Commons personnel and staff. When you're referring to House
8 of Commons personnel and staff, can you describe who would be
9 captured by that security screening?

10 **MR. PATRICK McDONELL:** Okay. So when I refer
11 to House of Commons personnel, that's an employee of the
12 administration. When I refer to staff, I'm referring to
13 political staff, commonly known as staffers.

14 **MR. HAMZA MOHAMADHOSSEN:** So those working in
15 the offices of MPs? Is that what you mean by political
16 staff?

17 **MR. PATRICK McDONELL:** Exactly. Yes.

18 **MR. HAMZA MOHAMADHOSSEN:** Okay. And so they
19 are nonetheless House of Commons employees, even though they
20 are hired by the MPs themselves?

21 **MR. PATRICK McDONELL:** They're -- no, they're
22 MP employees.

23 **MR. HAMZA MOHAMADHOSSEN:** They're MP
24 employees.

25 **MR. PATRICK McDONELL:** They're hired by the
26 MP.

27 **MR. HAMZA MOHAMADHOSSEN:** But they're
28 required to follow House of Commons policies?

1 **MR. PATRICK McDONELL:** Yes, the Board of
2 Internal Economy decided some time ago that all political
3 staffers must undergo a security screening.

4 **MR. HAMZA MOHAMADHOSSEN:** Okay. Can you
5 describe what this security screening looks like?

6 **MR. PATRICK McDONELL:** Security screening
7 looks like a criminal background check ---

8 **MR. HAMZA MOHAMADHOSSEN:** M'hm.

9 **MR. PATRICK McDONELL:** --- and loyalty to
10 Canada check.

11 **MR. HAMZA MOHAMADHOSSEN:** M'hm.

12 **MR. PATRICK McDONELL:** So the criminal
13 background check is done through the Royal Canadian Mounted
14 Police ---

15 **MR. HAMZA MOHAMADHOSSEN:** M'hm.

16 **MR. PATRICK McDONELL:** --- and the loyalty to
17 Canada check is done by CSIS.

18 **MR. HAMZA MOHAMADHOSSEN:** Okay. At a high
19 level, are you able to explain what a loyalty of Canada check
20 entails?

21 **MR. PATRICK McDONELL:** Loyalty to Canada
22 check infers exactly that. Are there any doubts about their
23 loyalty to Canada, is Canada -- do they put Canada first, do
24 they have another country that comes before Canada? That's a
25 question we ask.

26 **MR. HAMZA MOHAMADHOSSEN:** And that's handled
27 entirely by CSIS?

28 **MR. PATRICK McDONELL:** CSIS handles it.

1 Sometimes -- yeah, it's handled by CSIS and then there's --
2 it goes into CSIS often because the person has spent some
3 period of time within the last five years outside of Canada,
4 ---

5 MR. HAMZA MOHAMADHOSSEN: M'hm.

6 MR. PATRICK McDONELL: --- it could be
7 someone new to Canada, or a Canadian citizen, so CSIS will
8 investigate that period of time.

9 MR. HAMZA MOHAMADHOSSEN: M'hm.

10 MR. PATRICK McDONELL: CSIS may interview the
11 individual. CSIS may come back to us and say it's -- they
12 haven't reached a conclusion and they recommend that we
13 interview the person on a resolution of doubt interview.

14 MR. HAMZA MOHAMADHOSSEN: Okay. And can you
15 explain a little bit what that resolution of doubt interview
16 ---

17 MR. PATRICK McDONELL: Yeah, so the
18 resolution of doubt interview is my personnel, trained
19 investigators for the most part, well experienced in police
20 work and security, and they will interview the applicant to
21 determine if there's any concerns for the House if they were
22 to have access to our buildings and our network.

23 MR. HAMZA MOHAMADHOSSEN: Okay. I think you
24 mentioned that you were originally appointed sergeant-at-arms
25 back in 2019?

26 MR. PATRICK McDONELL: Yes.

27 MR. HAMZA MOHAMADHOSSEN: How has the use of
28 resolution of doubt interviews changed over time?

1 **MR. PATRICK McDONELL:** I'm sorry?

2 **MR. HAMZA MOHAMADHOSSEN:** How has the use of
3 resolution of doubt interviews evolved ---

4 **MR. PATRICK McDONELL:** Oh, it's increased.

5 **MR. HAMZA MOHAMADHOSSEN:** --- over time?

6 **MR. PATRICK McDONELL:** Yeah, thank you. It's
7 increased significantly. I believe in 2019 we did --
8 conducted 10 resolution of doubt interviews. And in 2023,
9 128, ---

10 **MR. HAMZA MOHAMADHOSSEN:** Okay.

11 **MR. PATRICK McDONELL:** --- approximately.

12 **MR. HAMZA MOHAMADHOSSEN:** Yeah. And these
13 interviews, is there a threshold for conducting the
14 interviews, or is it only when CSIS indicates there's a need
15 for an interview?

16 **MR. PATRICK McDONELL:** It's not only CSIS.
17 If the person has a criminal record, they will most likely
18 undergo a resolution of doubt interview. A criminal record
19 will not bar you from employment at the House of Commons. It
20 depends on the circumstances. So those resolution of doubt
21 interviews, we just want to learn more about the
22 circumstances of the charge and record.

23 **MR. HAMZA MOHAMADHOSSEN:** Okay. And at the
24 end of this process, what is the output -- what is the
25 outcome?

26 **MR. PATRICK McDONELL:** There's a
27 recommendation provided to me by the interviewer ---

28 **MR. HAMZA MOHAMADHOSSEN:** M'hm.

1 MR. PATRICK McDONELL: --- whether to move
2 forward and give the applicant access and accreditation, ---

3 MR. HAMZA MOHAMADHOSSEN: M'hm.

4 MR. PATRICK McDONELL: --- or to refuse.

5 MR. HAMZA MOHAMADHOSSEN: And when you say
6 access, that's access to what exactly?

7 MR. PATRICK McDONELL: That would be access
8 to our buildings and our network.

9 MR. HAMZA MOHAMADHOSSEN: Okay. Let's say
10 there's -- let's say that you decide not to grant
11 accreditation.

12 MR. PATRICK McDONELL: M'hm.

13 MR. HAMZA MOHAMADHOSSEN: Is there an appeal
14 mechanism available to anyone involved in the process?

15 MR. PATRICK McDONELL: Yes, they can appeal
16 their decision -- or my decision, and I meet with them.

17 MR. HAMZA MOHAMADHOSSEN: By they, you are
18 referring to who?

19 MR. PATRICK McDONELL: The applicant.

20 MR. HAMZA MOHAMADHOSSEN: The applicant.

21 Okay.

22 MR. PATRICK McDONELL: Yeah. If I refuse.

23 Yeah.

24 MR. HAMZA MOHAMADHOSSEN: And you said, I
25 think, that you meet with them?

26 MR. PATRICK McDONELL: I meet with them, yes,

27 ---

28 MR. HAMZA MOHAMADHOSSEN: Okay.

1 **MR. PATRICK McDONELL:** --- and discuss it.

2 **MR. HAMZA MOHAMADHOSSEN:** Okay. Referring
3 generally to the screening process, where does your team
4 obtain the information required to conduct the screenings?

5 **MR. PATRICK McDONELL:** Overall, if we're
6 going into a resolution of doubt interview, we'll take the
7 information either received from the Royal Canadian Mounted
8 Police and/or CSIS ---

9 **MR. HAMZA MOHAMADHOSSEN:** M'hm.

10 **MR. PATRICK McDONELL:** --- and we'll also do
11 open-source analysis prior to the interview.

12 **MR. HAMZA MOHAMADHOSSEN:** Okay. And does the
13 process of security screening, including the loyalty to
14 Canada investigation, the resolution interview, does that
15 entire process capture foreign interference concerns?

16 **MR. PATRICK McDONELL:** Yes, I would say so.

17 **MR. HAMZA MOHAMADHOSSEN:** Okay. And without
18 going into detail, have you, in fact, denied accreditation
19 over foreign interference concerns?

20 **MR. PATRICK McDONELL:** Yes, I've denied let's
21 say a handful in the last 10 years, 2 of them being in the
22 last 6 months.

23 **MR. HAMZA MOHAMADHOSSEN:** Okay. You
24 indicated earlier that when there are threats to MPs, you
25 contact the MPs directly sometimes, or if they're not the one
26 bringing you the ---

27 **MR. PATRICK McDONELL:** Yes ---

28 **MR. HAMZA MOHAMADHOSSEN:** --- threat

1 themselves.

2 MR. PATRICK McDONELL: --- we'd make them
3 aware.

4 MR. HAMZA MOHAMADHOSSEN: And in some
5 instances the Party whips ---

6 MR. PATRICK McDONELL: Yes.

7 MR. HAMZA MOHAMADHOSSEN: --- also the RCMP.
8 In the event that there are security concerns relating to
9 staffers, to political staffers in an MP's office, who would
10 you notify regarding these concerns?

11 MR. PATRICK McDONELL: Well, the staffer and
12 the MP and the whip. And that has happened, and we've had,
13 you know, meetings, the staffer, the whip, the MP, myself,
14 and discussed the way forward.

15 MR. HAMZA MOHAMADHOSSEN: Okay. And would
16 you ever communicate your concerns to external agencies?

17 MR. PATRICK McDONELL: Only agencies that
18 could assist in the investigation of the possible offence.

19 MR. HAMZA MOHAMADHOSSEN: Thank you. These
20 are my questions. Maître Poliquin will carry on with the
21 rest of the examination.

22 COMMISSIONER HOGUE: Thank you.

23 MR. HAMZA MOHAMADHOSSEN: Thank you.

24 --- EXAMINATION IN-CHIEF BY MR. GABRIEL POLIQUIN:

25 MR. GABRIEL POLIQUIN: Just I'll get set up
26 here. Turns out I had water.

27 Good morning. Just for the record, Gabriel
28 Poliquin for the Commission. So I'll take over from Mr.

1 Mohamadhossen on the relationships with government entities.
2 We've talked a little bit about it already in terms of
3 specific examples when you collaborate with the RCMP or with
4 CSE and so on, but I'd like to take it to a more formal level
5 and talk about formal agreements that the House of Commons
6 has with various security and intelligence agencies. And
7 I'll start with you, Mr. McDonell. I understand from
8 paragraph 24 of the witness summary -- we could actually pull
9 that up, Mr. Court Operator, just so we have it before us,
10 paragraph 24.

11 So it said at paragraph 24 that the House of
12 Commons has an MOU with CSIS and the RCMP. And what is that
13 MOU about? What's it for? What's its purpose?

14 **MR. PATRICK McDONELL:** The MOU with CSIS and
15 the RCMP, the purpose of both of those MOUs is the sharing of
16 information.

17 **MR. GABRIEL POLIQUIN:** Okay. And does that
18 MOU provide for anything about foreign interference
19 specifically?

20 **MR. PATRICK McDONELL:** I don't believe the
21 wording foreign interference is in the MOU. I'd have to
22 refer to it. But when we're dealing with CSIS, we're dealing
23 always with matters of national security, so there's an
24 inference ---

25 **MR. GABRIEL POLIQUIN:** Okay.

26 **MR. PATRICK McDONELL:** --- foreign
27 interference.

28 **MR. GABRIEL POLIQUIN:** Very well. And then

1 at paragraph 24 it's also mentioned that there's an MOU with
2 Privy Council, if you could elaborate on that, please?

3 **MR. PATRICK McDONELL:** Yeah, so I have an MOU
4 with Privy Council and that has to do with technical
5 surveillance countermeasures. We assist them in the
6 provision of those service -- and those services for caucus
7 meetings and possibly other meetings where they require that
8 service.

9 **MR. GABRIEL POLIQUIN:** Okay. So it's not
10 just limited to MP's offices?

11 **MR. PATRICK McDONELL:** No, we do MP's offices
12 where, you know, we'll sweep MP's offices for bugs, and we
13 provide that service to Privy Council also.

14 **MR. GABRIEL POLIQUIN:** Okay.

15 **MR. PATRICK McDONELL:** And the monitoring of
16 signals, cell phones in a room, Bluetooth, watches, whatever
17 may emit a signal.

18 **MR. GABRIEL POLIQUIN:** Right.

19 **MR. PATRICK McDONELL:** We'll monitor the
20 room.

21 **MR. GABRIEL POLIQUIN:** Okay. And I think you
22 mentioned briefly through my colleague's questions that there
23 are regular meetings with the RCMP and other security
24 intelligence agencies. And are those meetings at regular
25 intervals?

26 **MR. PATRICK McDONELL:** CSIS, the RMI section,
27 which I had mentioned earlier, Risk Management Investigators,
28 they meet with CSIS once a month and discuss files of

1 interest, investigative techniques, latest trends, and then
2 operational files as they come forward. The RCMP, pretty
3 well talk to the RCMP every day.

4 **MR. GABRIEL POLIQUIN:** Okay. And this is
5 what you were referring to earlier, the exchanging
6 information about open-source intelligence, is that what
7 you're referring to?

8 **MR. PATRICK McDONELL:** Exchange of
9 information on files, like, if we get -- we make the RCMP
10 aware of any and all our files that have come to light in the
11 last 24 hours. So every day we generate a report of files
12 that came to our attention, or incidents, or concerns that
13 came to our attention. Could range anywhere from the
14 harassment of an MP online, an email, a phone call, a
15 confrontation, a death threat. We make the RCMP aware of
16 all, all our open files. They in turn do the same.

17 **MR. GABRIEL POLIQUIN:** Okay. It was
18 mentioned earlier this morning by senate witnesses that the
19 senate participates in Intersec, and I believe you touch on
20 that in the interview summary as well. Could you just remind
21 us what Intersec is and what's the purpose of the House of
22 Commons participation?

23 **MR. PATRICK McDONELL:** Yeah, so the Intersec
24 is a community of Ottawa-area first responders. So the NCR,
25 Gatineau, they all come together. You'll have fire,
26 paramedics, police, people who, for the most part, will be
27 involved in a major event.

28 **MR. GABRIEL POLIQUIN:** Okay. And you also

1 touch on the Deputy Minister Protection Committee. What's
2 that and what's ---

3 **MR. PATRICK McDONELL:** So the DM Protection
4 Committee is headed up by the NSIA, National Security
5 Intelligence Advisor to the Prime Minister, and it's a
6 community made up of DMs, Deputy Ministers, where the
7 protection of Ministers and parliamentarians is discussed.

8 **MR. GABRIEL POLIQUIN:** Okay. Thank you. Now
9 I had some similar questions for you, Mr. Dicaire, as CIO. I
10 understand from paragraph 25 of the witness summary that the
11 House of Commons has an MOU with CSE that pertain more to
12 your field of expertise. If you could describe why that MOU
13 is in place?

14 **MR. BENOÎT DICAIRE:** That's correct. There's
15 an MOU between us and CSE, specifically the Cyber Centre.
16 It's really tied to three main objectives. One is the
17 exchange of information, similar to that. The second is the
18 protection of IT systems or IT infrastructure at the
19 perimeter. And third is really around the awareness and then
20 also incident handling.

21 **MR. GABRIEL POLIQUIN:** Okay.

22 **MR. BENOÎT DICAIRE:** So if there's an
23 incident.

24 **MR. GABRIEL POLIQUIN:** Very well. And what
25 about Shared Services Canada? That's touched on at paragraph
26 26 at the ---

27 **MR. BENOÎT DICAIRE:** Well, we have
28 independence from, we're not subject to Treasury Boards, so

1 we're not subject to Shared Services Canada, but we do
2 consume some services with them, so as a client, not as a
3 partner department. And I'm invited to some informal or
4 formal forum, communities of practice, CIO sharing, some of
5 their offerings, these types of scenarios.

6 **MR. GABRIEL POLIQUIN:** Okay. And while we're
7 on that topic, I know that it's covered in the institutional
8 report, but if you could describe, you know, the general
9 relationship with the House of Commons with respect to other
10 departments when it comes to IT, you know, are you completely
11 independent, or do you depend on the Government of Canada for
12 ensuring that?

13 **MR. BENOÎT DICAIRE:** No, we're completely
14 independent from -- as part of the -- you know, we are
15 subject to *Parliament Act*, which is completely different than
16 some other departments that would be typically subject to
17 Treasury Board guidelines and the rest.

18 **MR. GABRIEL POLIQUIN:** Okay. And so you have
19 your own IT unit, everything is separate; is that correct?

20 **MR. BENOÎT DICAIRE:** Yeah, we manage our own
21 infrastructure for the -- and we also manage the
22 infrastructure for parliamentary partners.

23 **MR. GABRIEL POLIQUIN:** Okay. And who are
24 those parliamentary partners?

25 **MR. BENOÎT DICAIRE:** Well, the senate, the
26 library, the Ethics Commissioner, the PPS, officers of
27 parliament mostly.

28 **MR. GABRIEL POLIQUIN:** Okay. And if you

1 could explain for us laypersons, when you -- you manage the -
2 - I might not have the right term, but you manage the
3 network, what does that mean exactly?

4 **MR. BENOÎT DICAIRE:** Well, it's a common
5 infrastructure for the parliamentary partners that the House
6 supports. They are all independent. They own -- in the case
7 of the senate, they own their portion, but we manage it. And
8 in case of the rest of the institution, we manage pretty much
9 the perimeter and the network itself.

10 **MR. GABRIEL POLIQUIN:** Okay. And when you
11 say the perimeter, what does that mean?

12 **MR. BENOÎT DICAIRE:** Well, the perimeter edge
13 is really the connection with the outside of our network, and
14 also, the connection with the Government of Canada networks.

15 **MR. GABRIEL POLIQUIN:** I see. Okay. And
16 while we're on that topic with collaboration with the Senate,
17 could you describe your collaboration with your Senate
18 partners in terms of exchange of information? How does that
19 work?

20 **MR. BENOÎT DICAIRE:** It is a longstanding
21 collaboration and it's very efficient, both on the security
22 front and on the IT front.

23 **MR. GABRIEL POLIQUIN:** Okay. And it's been -
24 - we'll explore that question in a little bit more detail
25 later on, but just at a high level while we're on the topic,
26 I understand from those MOUs and those collaborations you
27 have with security and intelligence agencies, that you
28 receive information from them from time to time, is that

1 right?

2 **MR. BENOÎT DICAIRE:** That's correct.

3 **MR. GABRIEL POLIQUIN:** Okay. And then to
4 what extent do you share that information that you receive
5 with Parliamentary partners? Does it happen at all?

6 **MR. BENOÎT DICAIRE:** Yes, if for some reason
7 it's mostly technical information and if there's risk that
8 will extend, potentially, to their institution, we would
9 collaborate with them.

10 **MR. GABRIEL POLIQUIN:** Okay. And so you
11 would relay that information received to the Senate, for
12 instance?

13 **MR. BENOÎT DICAIRE:** Yes.

14 **MR. GABRIEL POLIQUIN:** Okay. What happens if
15 that information is classified?

16 **MR. BENOÎT DICAIRE:** Well, you're bringing a
17 good point here. Depending on the level of classification,
18 but there's handling protocols aside -- assigned to that. So
19 it would only be shared with people that have the proper
20 clearances around some of those elements.

21 **MR. GABRIEL POLIQUIN:** Yeah. And just
22 generally, would it be shared, you know, of your own
23 initiative or would you have to check with the Cyber Centre
24 first, for instance?

25 **MR. BENOÎT DICAIRE:** Well it depends on the
26 circumstance for classified information. There's -- it comes
27 sometimes with caveats, where we're shown some information,
28 not necessarily given the information, and there's also some

1 caveats around sharing.

2 **MR. GABRIEL POLIQUIN:** Okay. Understood.

3 And again, we'll talk about that in more detail later on.

4 So when you -- so while we're on the topic,
5 talking specifically about information that you receive from
6 CSE, and again, just speaking very generally, if you could --
7 and again, not saying what that information is, but how is it
8 packaged? Like, what do you receive from CSE?

9 **MR. BENOÎT DICAIRE:** It's mostly technical
10 bulletins.

11 **MR. GABRIEL POLIQUIN:** And what are those?

12 **MR. BENOÎT DICAIRE:** Technical information
13 requesting a particular collaboration on sharing of
14 information or highlighting suspicious activity or
15 reconnaissance type of information. You know, "I'm seeing a
16 pattern from the sensor program that we're part of." So
17 they'll ask some questions around, you know, technical
18 information.

19 **MR. GABRIEL POLIQUIN:** So if I understand you
20 correctly, they are in the nature of requests for
21 information, but also just information provided? Is that ---

22 **MR. BENOÎT DICAIRE:** That's correct. If
23 there's risk, they would highlight risk. And if they're
24 asking for particular information, then they would be asking
25 us for help on, you know, collaborating on deciphering some
26 information, some technical information, if they need it.
27 But again, this type of collaboration is on a need-to-know
28 basis.

1 **MR. GABRIEL POLIQUIN:** Okay. And would you
2 describe -- are you satisfied with the level of information
3 that you obtained to do your job?

4 **MR. BENOÎT DICAIRE:** Yes, no, I think that we
5 have a strong collaboration with the Cyber Centre. It's
6 evolving over the years, as you know, as the cyber landscape
7 is evolving quite a bit. So there is definitely more
8 collaboration, more willingness to share, but again, around
9 the caveats assigned to, you know, our mandate, specifically.
10 So my specific mandate is to protect the infrastructure, and
11 protect members, and the continuity of Parliament. So they
12 have different mandates tied to intelligence and protecting
13 the Government of Canada and other types that are beyond my
14 mandate. So they share content based on what my mandate --
15 what they can share based on my mandate.

16 **MR. GABRIEL POLIQUIN:** Right. So if I
17 understand you correctly, they have a broader mandate to
18 protect national security. You have a mandate to protect ---

19 **MR. BENOÎT DICAIRE:** That's ---

20 **MR. GABRIEL POLIQUIN:** --- the House of
21 Commons ---

22 **MR. BENOÎT DICAIRE:** --- correct.

23 **MR. GABRIEL POLIQUIN:** --- infrastructure;
24 correct?

25 **MR. BENOÎT DICAIRE:** Correct.

26 **MR. GABRIEL POLIQUIN:** Okay. But in that
27 context, where they provide information that help you do your
28 job, to what extent does foreign interference come up? Do

1 you ever know, let's say, an attack is perpetrated by a
2 foreign actor?

3 **MR. BENOÎT DICAIRE:** Attacks are happening
4 very frequently and as you know, Parliament is a prime
5 target. So you can suspect that foreign actors are also
6 targeting the cyber infrastructure.

7 You know, depending on, you know, activities
8 around the world, the threat level goes up and down based on,
9 you know, Canada's position and Parliament's position around
10 some of those. And you'll see it also when we, you know,
11 have delegations or foreign dignitaries coming, you know,
12 that might have been -- so those threat factors are all
13 coming into play around that. But you can assume that we
14 don't always know who the actor is behind, but we know that
15 there's threats every day.

16 **MR. GABRIEL POLIQUIN:** Right. And sometimes
17 you may not know that a foreign actor is behind the certain
18 threat, but is that information ever relevant for your job?
19 Ever helpful?

20 **MR. BENOÎT DICAIRE:** Well it's always
21 relevant to the continuity of Parliament; right? So as I
22 clearly stated, you know, that's our mandate, is really
23 allowing the tools and protecting the information so that
24 members of Parliament can do their job. And, you know, those
25 threats, you know, depending on the political climate or the
26 geo-tensions around the world, you know, have an impact on
27 our ability to sit in Parliament. So it's always in that
28 kind of context.

1 collaboration, I mean, they don't always know the scenario.
2 The collaboration is really broad. But at the same point in
3 time, the important factor is, you know, the continuity of
4 Parliament. And again, I'm kind of overstating the same
5 comment, but that's the reality here, is really my mandate is
6 really not to do intelligence gathering or these types of
7 scenarios. I'm really focused on continuity of Parliament
8 and allowing members to sit.

9 So -- and depending on the classification
10 level, we might not have the classification required to
11 handle some of the information that they might have or
12 possess. So our staff have a maximum clearance of top
13 secret, and some of this information is beyond top secret.
14 So ---

15 **MR. GABRIEL POLIQUIN:** Okay.

16 **MR. BENOÎT DICAIRE:** --- they couldn't share
17 it with us.

18 **MR. GABRIEL POLIQUIN:** Okay. Understood.
19 And while we're on that topic, so who in your unit has the
20 classification to what level?

21 **MR. BENOÎT DICAIRE:** A variety of staff have
22 the -- have different levels of clearances, depending on
23 their roles.

24 **MR. GABRIEL POLIQUIN:** Okay. So not all ---

25 **MR. BENOÎT DICAIRE:** It's really -- no, not
26 all of them, because it's really on a need-to-know basis
27 around that scenario.

28 **MR. GABRIEL POLIQUIN:** Okay. And before I

1 forget, Mr. McDonnell, in your unit, who has -- what kind of
2 employees have security clearances, and what level?

3 **MR. PATRICK McDONELL:** Technical Surveillance
4 Countermeasures Team would be top secret. RMI, Risk
5 Management Investigations, top secret. And open-source
6 intelligence, top secret.

7 **MR. GABRIEL POLIQUIN:** Okay. That's helpful.
8 So going back to the topic of cyber attacks
9 and operational posture on that, I just want to make sure we
10 address that topic. And here I just want to give you an
11 opportunity to comment. We heard from members of Parliament
12 last week, Mr. McKay and Mr. Genuis, who mentioned, you know,
13 their take on cyberattacks and one event in particular,
14 APT31, that we're going to cover in a minute. Mr. Genuis
15 mentioned that it would be useful in his view, to get
16 notification of cyberattacks when they've happened or if they
17 are about to happen. Just notification of cyberattacks, so
18 that MPs can better protect themselves. I just want to give
19 you an opportunity to comment. Is that -- from a practical
20 standpoint, what's your take on that?

21 **MR. BENOÎT DICAIRE:** Well, the scale of
22 things, as again, parliament is a prime target, we're dealing
23 in hundreds of millions of attack attempts in a year. So the
24 practicality of briefing everyone at every instance would
25 create a serious operational burden. And most of those are
26 thwarted by either controls in place, or by, you know,
27 infrastructures in place.

28 That being said, we take every attack

1 seriously, every attack attempt seriously, and should there
2 be any risk to members of Parliament, specifically their data
3 or their devices, we would and have, you know, communicated
4 with them.

5 **MR. GABRIEL POLIQUIN:** And so ---

6 **COMMISSIONER HOGUE:** And just a question, who
7 is making the decision to advise or not the MPs?

8 **MR. BENOÎT DICAIRE:** It depends on criteria.
9 I would say, you know, depending on the risk. Like, is the
10 threat dealt with? Is it still active? Is there a risk of
11 further contamination, or if there's a risk of further risks,
12 those things would escalate through our cyber security
13 program and the cyber -- the person responsible for cyber
14 security or Chief Information Security Officer and ultimately
15 would come to me, you know, around that.

16 But there's parameters that don't require
17 escalation. So if there's an imminent threat, or if there's
18 a threat that's ongoing, the protocol is to advise right away
19 and to action, because we're trying to contain the risk, and
20 trying to remedy the situation. So then the cyber team
21 directly from the ground up are dealing with the member's
22 office directly at that point.

23 **MR. GABRIEL POLIQUIN:** Okay. So just to sum
24 up, like, what's the threshold where you would advise an MP
25 that, you know, a cyber attack has occurred?

26 **MR. BENOÎT DICAIRE:** Every time there's an
27 impact on their -- on their information, or there's an impact
28 on their devices.

1 **MR. GABRIEL POLIQUIN:** Okay. And by impact,
2 what could that be?

3 **MR. BENOÎT DICAIRE:** Well, an attack has
4 succeeded or the mechanisms -- there's a risk, there's a
5 vulnerability that needs to be addressed, or there's a usage
6 pattern, there's been a user or someone in their office has
7 clicked something that have generated an action that, you
8 know, potentially puts the infrastructure at risk, or puts
9 their information at risk. These type of scenarios. Or so -
10 --

11 **MR. GABRIEL POLIQUIN:** Okay. And I want to
12 just understand it as a layperson, I'm sure as we all do.
13 But say an email is received by an MP or their staff, and
14 somebody's clicked on it and then thereby heightened their
15 risk. Do you know about that, like, do you know they've
16 clicked?

17 **MR. BENOÎT DICAIRE:** There's two or three
18 ways that we would know. One is through monitoring, so we --
19 if you've clicked on a malicious email then it would start
20 generating abnormal patterns. We would see that through our
21 monitoring approach. The second is we've implemented a
22 phishing button, so they can report a suspicious email to IT
23 security directly. And third, is some members or their staff
24 report directly to our IT service centre, so 24/7 they can
25 call and report that this email is suspicious, can you look
26 at it, can you -- so these are the three most common
27 scenarios where we're flagged.

28 **MR. GABRIEL POLIQUIN:** Okay. And are cyber

1 attacks sometimes flagged by external partners?

2 **MR. BENOÎT DICAIRE:** Yes, it could be if some
3 pattern would be seen. It depends on the visibility, again,
4 because the complexity of our infrastructure is that those
5 visibility points are not necessarily -- because of the
6 architecture, they don't see everything.

7 **MR. GABRIEL POLIQUIN:** Okay.

8 **MR. BENOÎT DICAIRE:** So they would see
9 abnormal patterns that are leaving the parliamentary network
10 or entering the parliamentary network. But when it comes to
11 the parliamentary network themselves, they don't have
12 visibility.

13 **MR. GABRIEL POLIQUIN:** Right.

14 **MR. BENOÎT DICAIRE:** So they work with our
15 cyber team.

16 **MR. GABRIEL POLIQUIN:** So to make sure I
17 understand, your unit sees what's going on within the House
18 of Commons framework, but an external partner such as CSE may
19 not. Is that correct?

20 **MR. BENOÎT DICAIRE:** Yes. If you -- I'm not
21 wanting to go very technical here but ---

22 **MR. GABRIEL POLIQUIN:** Sure. No, we don't.

23 **MR. BENOÎT DICAIRE:** You know, the reality is
24 what is displayed outside our network and what happens inside
25 our network, we have thousands of IP addresses that are not
26 necessarily exposed to outside world. So what they see, or
27 what somebody could see outside doesn't necessarily correlate
28 to the inside. So what we need to do is now make that

1 correlation between external data and internal data to really
2 understand the threat.

3 **MR. GABRIEL POLIQUIN:** Okay. And speaking of
4 visibility, while we're on that topic, it's my understanding
5 that MPs are provided with parliamentary phones and
6 computers, but that they may have their own as well. And in
7 terms of visibility, how do you -- can you know what's going
8 on on an MP's personal device?

9 **MR. BENOÎT DICAIRE:** So we have policies in
10 place, an IT security policy and acceptable use policies that
11 prevent them from conducting parliamentary business on
12 personal devices. So that's the one first thing, scenario.
13 So it's all HOC managed devices. So parliamentary business
14 is done on House of Commons ---

15 **MR. GABRIEL POLIQUIN:** I'm sorry, hot, HOC?

16 **MR. BENOÎT DICAIRE:** House of Commons.

17 **MR. GABRIEL POLIQUIN:** House of Commons,
18 sorry.

19 **MR. BENOÎT DICAIRE:** House of Commons devices
20 that are managed through our infrastructure to my team. So
21 that's the scenario around that. We do allow some guests'
22 devices if you want, so personal laptop would connect to a
23 different architecture, so it's a guest Wi-Fi architecture
24 that's secured. But we don't manage those devices, and we
25 don't monitor those devices. To connect to the
26 infrastructure, you need to have a house managed device.

27 **MR. GABRIEL POLIQUIN:** Okay. And so what
28 happens in a scenario where a personal device may have been

1 used for parliamentary business or not, is compromised.

2 What's your jurisdiction, so to speak?

3 **MR. BENOÎT DICAIRE:** Well, the infrastructure
4 supporting guests' connectivity, we still monitor that
5 portion. So if we see an abnormal pattern we would
6 interject, you know around that, potentially cut the access
7 and to remedy the impact potentially. But there's
8 segregation between, you know, our parliamentary network and
9 our guest network.

10 So there is these scenarios that there is
11 these controls in place in place to prevent, you know,
12 impacts, or mitigating impacts around some of those
13 scenarios. But if we have the visibility, if it's connected
14 -- if it's not connected to our guest network then I have
15 zero visibility.

16 **MR. GABRIEL POLIQUIN:** Okay.

17 **MR. BENOÎT DICAIRE:** If it's connected to our
18 guest network, then we have a possibility to see some
19 activity.

20 **MR. GABRIEL POLIQUIN:** Right. So if my
21 understanding is correct, say I bring my phone and it's not a
22 parliamentary phone, and I'm on the guest Wi-Fi at House of
23 Commons, and it's compromised by a phishing email or
24 something. Can that person come to your service and say,
25 "Look, what can I do about this?"

26 **MR. BENOÎT DICAIRE:** That would be -- we
27 wouldn't see that type of compromise because then you
28 wouldn't be on our email infrastructure. So to see a

1 phishing email it would have to go through the email
2 infrastructure we have.

3 So if you have a phone that's personal,
4 that's on Gmail, and there's a phishing email on Gmail, I
5 wouldn't have that visibility. I would see if the device is
6 exhibiting, you know, a pattern of trying to call out to a
7 malicious site, or a home base that is malicious, I would see
8 some of the traffic around that. But I wouldn't necessarily
9 see what the source of the issue is compared to a managed
10 system where we have more visibility.

11 **MR. GABRIEL POLIQUIN:** Right. And say we
12 accept you don't have visibility on a personal device, but as
13 an MP I know it's been compromised somehow and you know, I'm
14 having trouble with this. Can you help that person, can you
15 help that MP?

16 **MR. BENOÎT DICAIRE:** We would do best effort.
17 Our mandate is really tied to house managed devices, and
18 house information, and house infrastructure. So we truly
19 don't have a mandate for personal devices.

20 **MR. GABRIEL POLIQUIN:** Okay. So again, this
21 ties to points that were brought up by Mr. Genuis and Mr.
22 McKay, you know, that sometimes, the difference between
23 Parliamentary work, electoral work, and personal matters,
24 sometimes gets blurry. So I know that there's a policy in
25 place that says, well, you know, your jurisdiction and your
26 visibility, your physical visibility anyway is limited to
27 your system.

28 But that, you know, that distinction gets

1 blurred, and can you do anything to help them if something
2 happens? Say an MP receives an email on their parliamentary
3 phone -- or on their personal phone from a constituent, it's
4 about an electoral matter, but the conversation is also about
5 a parliamentary matter.

6 MR. BENOÎT DICAIRE: Okay.

7 MR. GABRIEL POLIQUIN: Does that change
8 anything?

9 MR. BENOÎT DICAIRE: No, really the records
10 of visibility is -- where we have eyes, is the managed
11 devices.

12 MR. GABRIEL POLIQUIN: Yeah.

13 MR. BENOÎT DICAIRE: That's the
14 responsibility we have and that's the mandate we have. The
15 Acceptable Use Policy does provision that, you know, there
16 could be certain personal, you know, checking an email,
17 checking your bank system, or these types of scenarios, using
18 parliamentary devices, but the opposite doesn't really apply.
19 I don't have visibility on something that's a personal
20 device.

21 MR. GABRIEL POLIQUIN: Right.

22 MR. BENOÎT DICAIRE: In a scenario like Mr.
23 Genuis, I wouldn't have seen anything.

24 MR. GABRIEL POLIQUIN: Okay. Now I take it
25 some MPs have two different phones for two different
26 purposes. MPs might have just one phone that they do
27 everything on, maybe it's separate accounts, but it's on the
28 same phone. From a practical standpoint, you know, does

1 having two phones help your job? Having the same phone, does
2 that impede your job? Does it make any difference?

3 **MR. BENOÎT DICAIRE:** Well the bylaws are
4 pretty specific today and I'm not the right person to ---

5 **MR. GABRIEL POLIQUIN:** Right. And I'm not
6 asking you about the bylaws. I know that you can't comment
7 on, you know, the application of the policy, but, you know,
8 as a person who is responsible for ensuring the security, is
9 having just one phone, does that create an extra technical
10 vulnerability?

11 **MR. BENOÎT DICAIRE:** Like I said, our mandate
12 is really through the House managed devices, so whether
13 there's a personal phone or not in the equation, if somebody
14 has a different phone, ---

15 **MR. GABRIEL POLIQUIN:** Right.

16 **MR. BENOÎT DICAIRE:** --- it really doesn't
17 change my mandate. If they start using ---

18 **MR. GABRIEL POLIQUIN:** Okay. Say they do
19 everything from their parliamentary phone, ---

20 **MR. BENOÎT DICAIRE:** Yes.

21 **MR. GABRIEL POLIQUIN:** --- does that make any
22 difference? Does that ---

23 **MR. BENOÎT DICAIRE:** Well we would see more.
24 We would see -- but again, we -- the parliamentary phones are
25 there for parliamentary business.

26 **MR. GABRIEL POLIQUIN:** Okay.

27 **MR. BENOÎT DICAIRE:** That's the scope.

28 **MR. GABRIEL POLIQUIN:** Okay. I'll turn now

1 to a specific event that we all know now as the event
2 attributed to APT31. So that happened in January 2021. And
3 if you could remind us, Mr. Dicaire, how long you've been in
4 your role?

5 **MR. BENOÎT DICAIRE:** I started my position in
6 October 2023.

7 **MR. GABRIEL POLIQUIN:** Twenty twenty-three
8 (2023). Okay. So you weren't in that role when this attack
9 happened. But perhaps you can help us anyway in terms of
10 institutional response. The event came to light to the
11 public in June 2024, I believe. So what was your role in
12 respect to the response to that, institutional response of
13 the House of Commons to that?

14 **MR. BENOÎT DICAIRE:** So the cyber security
15 team would have -- so the knowledge I have from the gathering
16 that we've done and the extensive search that we've done, and
17 the interviews, and internally is indeed we collaborated with
18 the Cyber Centre in January 2021.

19 **MR. GABRIEL POLIQUIN:** M'hm. Okay.
20 Specifically to ---

21 **MR. BENOÎT DICAIRE:** Specific to an
22 information collecting campaign at the time. That was the
23 way it was earmarked.

24 **MR. GABRIEL POLIQUIN:** So you're saying that
25 the attack was an information collection campaign? Is that
26 your ---

27 **MR. BENOÎT DICAIRE:** That's the way it was
28 portrayed in 2021.

MR. GABRIEL POLIQUIN: Okay. And what else can you tell us about that event and its repercussions from the point of view of the House of Commons, you know, in as much as you know about it from the information gathering you've done?

MR. BENOÎT DICAIRE: At the time, you know, from -- this was a very common attack vector, these types of scenarios, and some of the information that was shared at the time from the bulletins is that, you know, it was information collecting. But it wasn't -- it was specifically said that it wasn't malicious, or likely not malicious, I should say.

So again, when we have protocols in place, when there's a bulletin that's provided to us, and there's been several in that period of time in the first four or five months of January to April, we collaborate, we collaborate and provide as much information and -- but our mandate is really, at this point in time, to always protect parliamentarians and protect the infrastructure.

MR. GABRIEL POLIQUIN: Okay. If we could pull a document, CAN.SUM27.1, please? Thank you.

So this is an annex to a topical summary prepared by Government of Canada, being CAN.SUM27, which we may refer to later on.

--- EXHIBIT No. CAN.SUM.000027:

PRC Email Operations Against
parliamentarians

--- EXHIBIT No. CAN.SUM.000027.001:

Tab A - Chronology of Events: Email

Tracking Link Campaign Targeting

Canadian parliamentarians

MR. GABRIEL POLIQUIN: This is a chronology of events that relates to APT31. I know that this isn't your document, but I have just some specific terminological questions in association with that, just to help us understand it.

If you could scroll down to February 3rd, 2021? Oh, February 3rd. Sorry. There we are. There we are.

So just to summarize, the first few points are about information that your unit has received from the Cyber Centre. Is that correct?

MR. BENOÎT DICAIRE: Yeah.

MR. GABRIEL POLIQUIN: You're familiar with this document?

MR. BENOÎT DICAIRE: Yeah. I'm familiar with the document.

MR. GABRIEL POLIQUIN: Right. And so at February 3rd, it says:

"The Cyber Centre Incident Handler follows up to request feedback on January 22nd report."

And says:

"The HoC Senior IT Security Analyst..."

So that person would be within your unit; correct?

MR. BENOÎT DICAIRE: Yes.

1 **MR. GABRIEL POLIQUIN:** Okay. And:

2 "...responded to the Cyber Center
3 Incident Handler and indicated that
4 the issue was handled internally."

5 Now, again, I know you weren't there at the
6 time, but can you comment more generally, when we say
7 "handled internally", what does that mean?

8 **MR. BENOÎT DICAIRE:** Okay. So the current
9 protocol, and it's tied to our mandate, is the risk to
10 Parliament infrastructure, risk to parliamentary information,
11 or parliamentary devices. So if information is shared about
12 a possible attack, or possible attack vector, then our first
13 lens at this is really around how do we protect ourselves and
14 are we, you know, are we -- have we been breached or have we
15 been -- do we have to invoke our incident management
16 protocol?

17 So in this particular case, as we've
18 discussed in the past, you know, the investigation or the
19 lens that brought us there to say that it was handled
20 internally is that there was no more threat to -- there was
21 no threat. It was a combination of the investigation and the
22 assessment of the security analyst was that there was no
23 threat to the IT infrastructure.

24 **MR. GABRIEL POLIQUIN:** And when you say no
25 threat, does that mean no breach or is that something
26 different?

27 **MR. BENOÎT DICAIRE:** No breach at this point
28 in time, because in particular -- in this particular case,

1 with the parameters that were shared in the bulletin, they
2 were specifically asking for technical information based on a
3 very specific date range, from the 18th of January to the 21st
4 of January. So upon investigation with this information, we
5 noticed that the emails that were associated with those IP
6 addresses and the technical information never reached members
7 of Parliament. They were quarantined.

8 **MR. GABRIEL POLIQUIN:** Okay. I see.

9 So and just to confirm, if we could scroll
10 down a little bit to February 17th? I believe there are two
11 February 17th dates. Hold on. just scroll up, please.
12 Okay.

13 So just making sure that I have the right
14 reference.

15 Oh, if you could, yeah, scroll down to the
16 next 17th of February one?

17 Right. So the second paragraph there the:

18 "HoC director, IT Security, provided
19 the Cyber Centre's Incident
20 Management team with a printed
21 document containing a sample
22 malicious email and the names of
23 eight MPs who were intended
24 recipients of malicious emails."

25 So I've got a couple of questions about that.
26 You said earlier that the information you had was that it was
27 likely not malicious.

28 **MR. BENOÎT DICAIRE:** That's what the bulletin

1 indicated at the time.

2 **MR. GABRIEL POLIQUIN:** Okay. And so did that
3 change by February 17th?

4 **MR. BENOÎT DICAIRE:** No.

5 **MR. GABRIEL POLIQUIN:** Okay. And so of
6 course this may be a question for the folks who prepared this
7 document, but do you know why it says "malicious email" here?
8 And you may not.

9 **MR. BENOÎT DICAIRE:** Well the attack tactic
10 that was being advertised and wasn't necessarily said at that
11 point in time, but multiple -- you know, a year after the
12 bulletin, there was a bulletin in June 2022 that was way more
13 specific based on, you know, a year of information, but at
14 the time, we knew of the pattern that they were looking at in
15 this particular email, which was a method through a pixel
16 type of threat, meaning that through an embedded image, they
17 would trigger a collection of data that would be sent back to
18 this malicious ---

19 **MR. GABRIEL POLIQUIN:** And I guess that's
20 known as a pixel reconnaissance?

21 **MR. BENOÎT DICAIRE:** That's it.

22 **MR. GABRIEL POLIQUIN:** Something -- okay.

23 **MR. BENOÎT DICAIRE:** But in this case of the
24 House of Commons, we have protections at multiple levels. As
25 you know, our SITE cyber security program has proactive
26 measures and reactive measures, and one of those proactive
27 measures is disabling of downloading of images in email. So
28 they're not downloaded by default, they're prevented from

1 being opened. So specifically a user or a recipient would
2 have to go click to download that email. So by default that
3 that's not happening.

4 So -- but the fact that these emails never
5 reach -- that were part of that date range never reached the
6 MPs, you know, that's basically -- that's basically -- that's
7 an area. But the malicious email part, that was part of the
8 bulletin, it wasn't coming from us; a bulletin that indicated
9 likely not malicious, that's their documentation, our
10 partners.

11 **MR. GABRIEL POLIQUIN:** Okay. And maybe a
12 later assessment, but that's a question for them.

13 **MR. BENOÎT DICAIRE:** Yeah.

14 **MR. GABRIEL POLIQUIN:** Okay. I had two
15 questions, now I actually have three.

16 My second-to-last about that point, you
17 mentioned how when you see the email you'd have to click for
18 it -- for the malicious effects to kick in. So is that due
19 to a measure that's taken at the network level that, you
20 know, images aren't downloaded automatically?

21 **MR. BENOÎT DICAIRE:** It's a configuration
22 that we have through our email infrastructure, an email
23 security posture, if you want to call it. Email is one of
24 the biggest vector of threats, so we have a configuration
25 that is restricted that prevents those -- the likelihood of
26 those types of attacks being successful. It doesn't
27 eliminate them because I don't control the users.

28 **MR. GABRIEL POLIQUIN:** Somebody might click?

1 **MR. BENOÎT DICAIRE:** Some people might click.
2 So that's the scenario.

3 **MR. GABRIEL POLIQUIN:** Okay. And so that
4 measure of protection, is that something that users can opt
5 in and out of?

6 **MR. BENOÎT DICAIRE:** No.

7 **MR. GABRIEL POLIQUIN:** So it's a blanket
8 protection.

9 **MR. BENOÎT DICAIRE:** It is a protection
10 mechanism ---

11 **MR. GABRIEL POLIQUIN:** Okay.

12 **MR. BENOÎT DICAIRE:** --- built in for the
13 parliamentary email system.

14 **MR. GABRIEL POLIQUIN:** Okay. Taking a step
15 back before I get to my last question on that, so I don't
16 forget it, so does the House of Commons have -- and we'll get
17 to more detail on that in a minute, but do they have
18 briefings to MPs and other users on best practices for their
19 personal devices as well?

20 **MR. BENOÎT DICAIRE:** For the personal? So in
21 general as part of our IT security program we have an
22 awareness filler. So -- and it is a very effective mechanism
23 in terms of a defence tactic, right? So awareness around
24 users and behaviours in these types of scenarios. So over
25 the years so we send multiple bulletins; we call them Cyber
26 Vigilance Bulletin, and we do briefings at Caucus, and these
27 types of scenarios around best practices and different threat
28 factors, phishing, spear phishing, you know, ransomware, all

1 of these types of scenarios.

2 Some of our bulletins are actually
3 specifically talking about personal devices in some cases,
4 but they're in the spirit of parliamentary information. So
5 in 2023, you know, we change and approach it, if you're
6 trying to consume -- one of the bulletins specifically was
7 we've implemented multifactor identification, so if you're
8 trying to consume something on a parliamentary infrastructure
9 from outside as exposed to the internet, but with a personal
10 device and not your HOC device, then you would be challenged
11 for that second factor identification.

12 These are parameters that we put in place
13 here to protect parliamentary information that is accessible
14 outside of the privy of a parliamentary device.

15 **MR. GABRIEL POLIQUIN:** Right, okay.
16 Understood. And so this may be too specific of a question,
17 then, but just following up on that, as part of those
18 bulletins, do you include, you know, toggling on this
19 protection device of, you know, not downloading automatically
20 images that come through email; is that a piece of advice
21 that's transmitted in your bulletins?

22 **MR. BENOÎT DICAIRE:** I wouldn't have the
23 specific information about that particular case because
24 they're configurations -- there're some configurations that
25 are not behavioural based, such as that. It's -- but we do
26 have multiple parameters as part of our awareness campaign;
27 "Don't click on links," you know, "Assume that it's a
28 verified sender, somebody you would know," these type

1 scenarios are all best practice, so on prior to clicking.
2 And when in doubt, you now, use the phishing email, phishing
3 button to report it so we can verify it, or call us and we
4 can do that verification with you before you click.

5 So there's the best practices around
6 influencing that cyber safety, if you want, or safe
7 behaviours.

8 **MR. GABRIEL POLIQUIN:** Okay. And so turning
9 to my last question on this point, which I haven't forgotten,
10 it says here that there were eight MPS who were intended
11 recipients of malicious emails. And so if my understanding
12 is correct, those MPs did not receive -- like, let's put it
13 this way, those eight MPs, those emails did not end up in
14 their inboxes; is that correct?

15 **MR. BENOÎT DICAIRE:** That is correct. Our IT
16 security team reached out, though, to those eight MPs prior
17 to understanding -- this is happening very fast. So before
18 even confirming that those emails were quarantined, the cyber
19 team reached out to those eight MPs to see if they had
20 received anything in regards to that. So two members
21 acknowledged that they didn't receive anything, but they were
22 asking if -- should we need to -- we'll look out for it, type
23 of scenarios. But then it was easily determined, you know,
24 very rapidly afterwards that those emails were quarantined
25 and never reached for those particular date range.

26 **MR. GABRIEL POLIQUIN:** Okay. But you reached
27 out to them anyway.

28 **MR. BENOÎT DICAIRE:** We had reached out to

1 them, so there was an email that was sent the same day by the
2 security to the Members' mailbox.

3 **MR. GABRIEL POLIQUIN:** Okay. Thank you for
4 that.

5 Let's turn now briefly to the witness
6 summary, so WIT128, please. Okay, if you could scroll down
7 to paragraph 70, please? Seventy (70); seven zero, please.

8 So it's the third sentence from that
9 paragraph. Again, this paragraph pertains to February 17th,
10 which we've just discussed. The third sentence is:

11 "The original information they
12 received [that] related to MP IP
13 addresses, which they assessed had
14 not been compromised."

15 And we're talking about the -- just to be
16 clear, your unit.

17 **MR. BENOÎT DICAIRE:** M'hm.

18 **MR. GABRIEL POLIQUIN:** Right. So "He" being
19 you:

20 "He indicated that no contextual
21 information was shared in the report
22 received by CCCS, so they had no way
23 of knowing whether this was a state-
24 sponsored attack or otherwise."

25 And correct me if I'm wrong but this is at
26 the time of February 17th.

27 **MR. BENOÎT DICAIRE:** Correct.

28 **MR. GABRIEL POLIQUIN:** So when you say there

1 was no information in the report received by CCCS, just to
2 clarify, what report is that?

3 **MR. BENOÎT DICAIRE:** So this is the first
4 report that we received on January 22nd, 2021.

5 **MR. GABRIEL POLIQUIN:** And is that what you
6 referred to earlier as technical bulletins?

7 **MR. BENOÎT DICAIRE:** Yeah, it is -- I don't
8 know, it's called a Cyber Event Report.

9 **MR. GABRIEL POLIQUIN:** Okay. And just
10 speaking from, again, your general experience in this role, I
11 know you weren't there at the time, but is the knowledge that
12 an attack was state sponsored, does that make a difference in
13 your operational posture?

14 **MR. BENOÎT DICAIRE:** At the time it wouldn't
15 have because, again, the scenario is the same, right? Our
16 mandate is protecting the IT infrastructure and ensuring
17 that, you know, continuity of Parliament. So in that sense,
18 no. But, you know, in our renewed, you know, mandate and MOU
19 with -- that is just recently signed, you know, we're
20 focusing a lot more on the information-sharing aspect.

21 But, again, there's an evolution that needs
22 to happen because, again, there's clearances tied to access
23 to specific information. But there is a renewed
24 collaboration with our partners to ensure that, you know,
25 recommendations as far as bulletins are more accurate, or
26 contextual information would be given so that, you know, we
27 -- and it's mostly around how we work so that we can
28 collaborate more extensively on that -- on providing more

1 information, you know, while staying within our mandate.
2 Again, my team's mandate is not, you know, national security
3 and not necessarily intelligence. So we are happy to be good
4 collaborative partners, but there is an extent to which our
5 mandate, you know, takes us. But there is definitely, as
6 part of our MOU and as part of our organizations, both
7 organization, a willingness to provide more contextual
8 information based on, you know, the evolution of their own
9 mandate and the ministerial directives that they have to
10 abide to in helping them in their own mandate.

11 **MR. GABRIEL POLIQUIN:** Okay.

12 **COMMISSIONER HOGUE:** And is it useful for you
13 to get more information if we place ourselves as of today?

14 **MR. BENOÎT DICAIRE:** Well, it's always useful
15 to have more context. It's not always possible to have
16 because there's a lot of recognizance activity at the time.
17 It's like piecing -- trying to piece a puzzle together. They
18 might have three pieces of that puzzle, but it doesn't paint
19 that full picture yet. So as you saw in the evolution of
20 some of those bulletins, there's an evolution of that
21 situation that brought us from 2021 to 2024. So there is
22 lessons learned that are tied to how we collaborate and how
23 we can share information and contribute to both our mandates.
24 So, in some cases, the -- it's what's useful for me is in the
25 discourse of my own mandate in protecting parliament.

26 **COMMISSIONER HOGUE:** Thank you.

27 **MR. GABRIEL POLIQUIN:** Okay. And so this is
28 an MOU you've recently finalized with ---

1 MR. BENOÎT DICAIRE: Yes.

2 MR. GABRIEL POLIQUIN: --- the Cyber Centre;
3 correct?

4 MR. BENOÎT DICAIRE: Yeah, it's finally --
5 it's -- I think it was signed last week ---

6 MR. GABRIEL POLIQUIN: Okay.

7 MR. BENOÎT DICAIRE: --- the MOU, and we are
8 still in negotiation on -- we're still finalizing the
9 associated documents that are really the methodology of how
10 we are working as per the MOU.

11 MR. GABRIEL POLIQUIN: Okay. When you say
12 associated documents, what do you mean?

13 MR. BENOÎT DICAIRE: So CONOPS, so a way that
14 we engage, the formalized protocol for engagement.

15 MR. GABRIEL POLIQUIN: Okay. And are you
16 satisfied with this new MOU that your unit will be getting
17 the ---

18 MR. BENOÎT DICAIRE: Yes.

19 MR. GABRIEL POLIQUIN: --- the right
20 information?

21 MR. BENOÎT DICAIRE: Yes.

22 MR. GABRIEL POLIQUIN: Okay. If we could
23 turn now to WIT128 while still on the interview summary,
24 please? And if you could scroll down to paragraph 79,
25 please? Okay. So let's start with the first sentence here.
26 So,

27 "The targeted MPs were not informed
28 by the HOC administration in 2022

1 because the threat activity never
2 reached them."

3 So I'm just trying to reconcile that with
4 what you said earlier that they were notified. I just don't
5 understand.

6 **MR. BENOÎT DICAIRE:** So they weren't -- there
7 was a -- on the January 22nd bulletin 2021, as part of our
8 investigation, we did send an email to those 8 members, once
9 we correlated the IP address to the member's email, to see if
10 they had reached the email, but, clearly, as part of the
11 investigation, we also found out that our email system hadn't
12 done its job in quarantine. So that was the only time that
13 was notified around those scenarios. So ---

14 **MR. GABRIEL POLIQUIN:** Okay. Okay. Now
15 going back to an earlier topic, this is the third sentence,
16 "Had HoC IT known that it was a
17 state-sponsored campaign, they may
18 have looked at it with a heightened
19 sense of awareness for monitoring and
20 business continuity purposes."

21 Is this what you were referring to earlier?

22 **MR. BENOÎT DICAIRE:** Yes. Just like we --
23 when we have a special event at the House, not necessarily
24 cyber, but that is of public interest where it would generate
25 more interest and would potentially, you know, risk the
26 infrastructure because there's too many people consuming
27 those services, then we have the same heightened sense of
28 monitoring and awareness to ensure that, you know, we can

1 ensure that those important events are happening unhindered
2 from technical failures.

3 **MR. GABRIEL POLIQUIN:** Okay. Understood. If
4 we could turn now to another document, so CANSUM27, please?
5 So we'll stick on this page for now, that paragraph in
6 italics. Just to summarize, this is a document that's
7 prepared by the Government of Canada that summarizes some
8 intelligence that it received. So, of course, the document
9 is based on intelligence and not evidence, and the document -
10 - this document here does not contain the caveats and
11 limitations that are on the original information, but, of
12 course, you know, it applies as well.

13 If we could turn to paragraph 9 of that
14 document, please? And again, we're on that famous February
15 17th date of 2021. It says,

16 "...CSE delivered a SECRET-level
17 briefing to the HoC's IT Security
18 officials, including the Director IT
19 Security. CSE's brief was delivered
20 by CSE subject matter experts with
21 CSIS officials also in attendance.
22 [And] the brief focused on the threat
23 actor designated as APT31. Country
24 tactics, and classes of targets that
25 have historically been of interest to
26 the threat actor, such as U.S. and
27 Canadian politicians, were explicitly
28 shared."

1 And so -- and I realize you weren't there at
2 the time. You were not at this meeting; correct? Okay.

3 **MR. BENOÎT DICAIRE:** Correct.

4 **MR. GABRIEL POLIQUIN:** And so I just want to
5 understand, it seems that there was some information that was
6 delivered to the HoC IT's security officials about the fact
7 that this was a foreign threat; correct?

8 **MR. BENOÎT DICAIRE:** Correct.

9 **MR. GABRIEL POLIQUIN:** Okay. And so I just
10 want to reconcile that with what was said earlier in the
11 interview summary that, you know, it would have been nice to
12 have that information at the time. Just help us just
13 understand.

14 **MR. BENOÎT DICAIRE:** Well, it's not that
15 abnormal when information comes to light on some things, but
16 at this point in time, the keyword here is "suspected". I
17 mean, I think that that was -- it's very preliminary in the
18 timeline around, you know, confirmation and these types of --
19 so I think the key word here is, you know, the -- suspected
20 to come from the following, you know, but they were asking
21 also for our help in trying to piece that puzzle together.
22 So as part of the same meeting, we also shared some relevant
23 metadata, so not actual emails from MPs, but actual
24 information that we've gathered from based on their bulletins
25 to help them in their recognizance efforts and in their
26 intelligence-gathering efforts. So, yes, there was some -- a
27 classified briefing that we -- one of our directors was shown
28 and couldn't -- you know, needed to -- that classified

1 briefing was happening in a secure facility, and that
2 document was not provided to him. So there is definitely
3 caveats around ---

4 **MR. GABRIEL POLIQUIN:** Sure.

5 **MR. BENOÎT DICAIRE:** --- handling that type
6 of information.

7 **MR. GABRIEL POLIQUIN:** Sure. And I'll have a
8 question about that in a second, but while we're on here, I
9 just want to -- what we're interested in is making sure that,
10 you know -- or knowing whether your unit has the information
11 that it needs. And so what I'm understanding is that, yes,
12 it can be useful to have information about whether or not an
13 operation is by a foreign actor. Did your unit have the
14 information it needed at the time? And I know you weren't
15 there, but, you know, from an institutional standpoint, if an
16 IT director under your purview receives information like
17 that, are you satisfied that you have the information you
18 need to change your operational stance or not?

19 **MR. BENOÎT DICAIRE:** If I can meet my
20 mandate, which is, you know, assess and that the
21 parliamentary infrastructure wasn't breached, or there's no
22 risk from a cyber perspective to the parliamentary, or the
23 parliamentary infrastructure, or the continuity of
24 parliament, then it satisfies my needs, because I am not a
25 national intelligence agency.

26 **MR. GABRIEL POLIQUIN:** Okay. So I'm almost
27 close to the end of my time. Yeah, I had just one more
28 question on this document at paragraph 11. So at paragraph

1 11 it makes reference to,

2 "The 2021 APT31 cyber event
3 highlighted three "lessons learned"
4 within CSE regarding the response to
5 the ongoing threat..."

6 So, again, this isn't your document, but we
7 talk about here at paragraph 2, so (ii) -- oh, sorry, (iii),
8 so, "CSE officials..." -- this is part of their lessons
9 learned, but,

10 "CSE officials also worked with [the]
11 HoC teams to ensure that the HoC
12 adopted the full range of measures
13 offered by CSE's cyber security
14 program to better defend and respond
15 to cyber threats."

16 And you may or may not be able to comment on
17 what those measures are, but have they been implemented?

18 **MR. BENOÎT DICAIRE:** I can't comment on the
19 measures that we implemented. I can tell you that we have a
20 strong relationship with CSE and Cyber Centre, and that they
21 offer different -- a various amount of services.

22 **MR. GABRIEL POLIQUIN:** Okay. But are those
23 measures mentioned in the MOU, the new MOU, at all, or?

24 **MR. BENOÎT DICAIRE:** We have access to the
25 full range of their services.

26 **MR. GABRIEL POLIQUIN:** Okay. Okay. I have
27 one last question that may not be able to answer, but you can
28 maybe help us out. One of the questions that comes up in

1 this Commission is, well who is responsible for what? Who is
2 responsible for informing MPs? Here MPs seem to have been
3 informed at some point that they were targeted by an attack.
4 Suppose you have another incident a little bit like this one,
5 where this is investigated by you internally, but also
6 external partners are aware this is going on. Do you have a
7 view on who should be responsible for informing MPs?

8 **MR. BENOÎT DICAIRE:** I think it depends on
9 what the question, and what the situation is, and what the
10 mandate is, and those criteria have to be -- so if it's
11 something that has to do with a cyber risk around
12 infrastructure and continuity of Parliament, definitely we
13 are there. And then if it's something that has to do with
14 under the privy of national security agencies, then, you
15 know, we would work in collaboration through my partner here,
16 the sergeant-at-arms, you know, around those. So it's
17 definitely there's an opportunity to evolve our collaboration
18 while respecting our individual mandates.

19 **MR. GABRIEL POLIQUIN:** Okay. Those are my
20 questions, Mme Commissaire.

21 **COMMISSIONER HOGUE:** Thank you. You're right
22 on.

23 So we'll come back at 2:00 o'clock sharp,
24 because we have a long day today, so if we want to make sure
25 to be able to go until the end. Be back at 2:00 and we'll do
26 the same.

27 Thank you.

28 **THE REGISTRAR:** Order, please.

1 The sitting of the Commission is now in
2 recess until 2:00 p.m.

3 --- Upon recessing at 12:40 p.m.

4 --- Upon resuming at 2:02 p.m.

5 **THE REGISTRAR:** Order, please.

6 This sitting of the Foreign Interference
7 Commission is now back in session.

8 The time is 2:02 p.m.

9 **COMMISSIONER HOGUE:** First one is counsel for
10 Michael Chong.

11 **--- CROSS-EXAMINATION BY MR. FRASER HARLAND:**

12 **MR. FRASER HARLAND:** Good afternoon,
13 Commissioner.

14 I'd like to start with some questions on
15 security briefings.

16 And if we could, Mr. Court Operator, bring up
17 WIT128.EN, please? And if we could go to paragraph 61?

18 It's a question for you, Mr. McDonell. At
19 paragraph 61 there, it says that you note that you had been
20 advocating in favour of these types of briefings, which are
21 security briefings to members of Parliament, prior to the
22 recommendations made in the Procedure and House Affairs
23 Committee. So my question is, how long had you been
24 advocating for those briefings? I just want to understand
25 your views on that matter.

26 **MR. PATRICK McDONELL:** I first started
27 advocating for those briefings in 2019.

28 **MR. FRASER HARLAND:** In 2019? Okay.

1 And Madam Commissioner, I'm going to ask for
2 your leave to take the witness to the NSICOP report. I did
3 not put it in my list of documents, so if there's an
4 objection, I understand, but it's a well-known document at
5 this point, so.

6 **COMMISSIONER HOGUE:** It's fine if they can
7 answer your question. If they cannot answer your question,
8 they will let you know.

9 **MR. FRASER HARLAND:** Absolutely. So that is
10 at COM363.

11 **--- EXHIBIT No. COM0000363:**

12 Special Report on Foreign
13 Interference in Canada's Democratic
14 Processes and Institutions

15 **MR. FRASER HARLAND:** Are you familiar with
16 this document, Mr. McDonell?

17 **MR. PATRICK McDONELL:** Yes.

18 **MR. FRASER HARLAND:** Okay. And if we could
19 go to paragraph 126, which I think is on page 62 of the PDF?

20 **MR. PATRICK McDONELL:** So in this paragraph,
21 we see that in December 2019, the Clerk of the Privy Council
22 sought the Prime Minister's authorization to implement
23 briefings. The Prime Minister didn't respond. And the same
24 question was sought again in December of 2020, and that
25 package included a draft instruction for letters to the
26 Ministers of Public Safety and Defence to coordinate the
27 briefings.

28 So my question to you, Mr. McDonell is if in

1 December of 2019 Public Safety had come to you, as was
2 instructed here, and sought to carry out those briefings, I
3 take it you would have been happy to assist to ensure that
4 those briefings could be carried out?

5 **MR. PATRICK McDONELL:** Yes.

6 **MR. FRASER HARLAND:** Thank you. I want to
7 turn now to another matter, which is the House of Commons'
8 awareness of the PRC, the People's Republic of China's
9 targeting of my client, who is the Honourable Michael Chong.

10 At paragraphs 80 to 81 of your witness
11 statement, it indicated that you didn't receive any specific
12 intelligence about the targeting of Mr. Chong. Is that
13 right?

14 **MR. PATRICK McDONELL:** That is right.

15 **MR. FRASER HARLAND:** So nothing from CSIS?
16 Nothing from Public Safety?

17 **MR. PATRICK McDONELL:** Not to me.

18 **MR. FRASER HARLAND:** Okay. So forgive me if
19 it's stating the obvious, but you could not possibly have
20 done anything about the targeting of my client without any
21 information having been provided to you? Would you agree
22 with that?

23 **MR. PATRICK McDONELL:** I would.

24 **MR. FRASER HARLAND:** Okay. Those are my
25 questions. Madam Commissioner, thank you very much.

26 **COMMISSIONER HOGUE:** Thank you.

27 Next one is counsel for Erin O'Toole. I
28 think it's on Zoom.

1 **MR. THOMAS JARMYN:** Thank you, Commissioner.

2 **COMMISSIONER HOGUE:** Oh, you're on mute.

3 Okay.

4 **--- CROSS-EXAMINATION BY MR. THOMAS JARMYN:**

5 **MR. THOMAS JARMYN:** Thank you, Commissioner.

6 I represent Erin O'Toole and many of my
7 questions actually were addressed by Commission counsel, so I
8 only have a few.

9 HoC01 speaks to the residential and
10 constituency office security program. And as I understand
11 it, that is a program whereby there's risk assessments
12 carried out and then security measures are developed for MPs
13 based upon your understanding of the nature and severity of
14 the threat. Is that correct?

15 **MR. PATRICK McDONELL:** It's not a risk
16 assessment per say. That would be something different. We
17 do a security evaluation of the sites, whether it's a
18 constituency site or a residential site. And based on that
19 evaluation, a decision is made on what security measures,
20 camera, video, contacts, alarms, would be in place -- would
21 have to be installed and put in place to provide an
22 appropriate level of security.

23 **MR. THOMAS JARMYN:** Without getting into the
24 particulars of any specific MP's security measures, my
25 understanding is that there's a range of security measures
26 applied to specific -- or given to particular MPs ranging
27 from personal alert devices, home monitoring, all the way up
28 to actual personal security. Who makes those determinations?

1 **MR. PATRICK McDONELL:** The personal security
2 is done on a case-by-case basis. If a site security is
3 required at the constituency office, sometimes post-incident
4 at a residence, where there's been vandalism or an incident
5 at the MP's residence, so that's done on a case-by-case
6 basis. The respective leaders of the political parties do
7 have the right to request personal security escort.

8 **MR. THOMAS JARMYN:** That seems like a
9 distinctly different process for physical security as related
10 to digital security, which seems to be a one-size fits all
11 approach to security devices and the digital presence. Is
12 that fair?

13 **MR. PATRICK McDONELL:** I can't comment on the
14 digital world. That doesn't fall within my area of
15 responsibilities.

16 **MR. THOMAS JARMYN:** Possibly, Mr. Dicaire,
17 you could comment?

18 **MR. BENOÎT DICAIRE:** I think it depends on
19 the context, so I just -- I want clarity a bit more on the
20 question itself, because it's different types of risk that
21 we're trying to manage.

22 **MR. THOMAS JARMYN:** I guess the question is,
23 is the approach to digital security uniform among all MPs or
24 is it tailored based upon the particular threats, for
25 example, that some of the MPs last week testified to?

26 **MR. BENOÎT DICAIRE:** I would say it's a
27 combination of both. There's parameters that are uniform in
28 terms of if you look at it's a layered approach, right, to

1 cyber security. So there's going to be common elements
2 within the parameter. There's maybe common elements within
3 the digital ID, if you want, or the accounts. There's going
4 to be common parameters at the system level or at the
5 infrastructure level. But then depending on the threats,
6 then we would tailor the approach specifically to a
7 particular attack vector, should we require to do it.

8 **MR. THOMAS JARMYN:** But those parameters are
9 only associated with the assessment of risk in relation to
10 parliamentary systems and devices?

11 **MR. BENOÎT DICAIRE:** That's correct.

12 **MR. THOMAS JARMYN:** So in contrast to
13 physical security, where we could be looking at a residence
14 or a constituency office, we don't engage in the same
15 analysis of personal digital presence for protection?

16 **MR. BENOÎT DICAIRE:** That would be a question
17 for Pat more than anything else.

18 **MR. PATRICK McDONELL:** Could you repeat the
19 question?

20 **MR. THOMAS JARMYN:** Well so there's a
21 contrast between physical security, where there, from what
22 you've told me, are processes in place to protect a personal
23 residence, potentially transit between personal residence and
24 office, et cetera, as contrasted with digital security, where
25 it doesn't seem there's any investment of protection related
26 to a personal digital presence, only the parliamentary
27 digital presence.

28 **MR. PATRICK McDONELL:** Yeah, so I would stick

1 with my original answer and what I'm responsible for and let
2 the conclusions be drawn from there.

3 **MR. THOMAS JARMYN:** Okay. And so if the --
4 based upon what you testified to when Commission counsel was
5 examining you and Mr. Dicaire, you're guided by the policies
6 of the Board of Internal Economy in terms of what will and
7 won't be protected. So if an expansion was required, it
8 would have to be the BOIE that would make that choice? Is
9 that correct?

10 **MR. PATRICK McDONELL:** That is correct.

11 **MR. THOMAS JARMYN:** Okay. And does the House
12 carry out a risk assessment when a member of Parliament
13 leaves office?

14 **MR. PATRICK McDONELL:** To the best of my
15 knowledge, no.

16 **MR. THOMAS JARMYN:** Some Members have been
17 very active parliamentary careers, very outspoken on issues
18 that cause them to be targets during their parliamentary
19 career. And so again, if such an assessment in post-
20 parliamentary life protection were to be applied for, that
21 would be a BOIE decision too? Is that correct?

22 **MR. PATRICK McDONELL:** Not necessarily. If
23 there is a threat based on -- well, if the threat assessment
24 reveals that there is a *bonafide* threat out there, I would
25 imagine that the RCMP Protective Operations, Public Safety
26 would be in that discussion.

27 **MR. THOMAS JARMYN:** Okay. Those are my
28 questions, Commissioner. Thank you very much.

1 COMMISSIONER HOGUE: Thank you.

2 Counsel for Jenny Kwan.

3 --- CROSS-EXAMINATION BY MR. SUJIT CHOUDHRY:

4 MR. SUJI CHOUDHRY: My name is Sujit
5 Choudhry. I'm counsel for Jenny Kwan.

6 I have some questions about the APT31
7 incident that we've been discussing quite a bit, and I think,
8 Mr. Dicaire, I think those are probably mostly directed to
9 you.

10 And so I was hoping we could get pulled up
11 again WIT129. Thank you. And could we please go down to --
12 the page with paragraphs 13 to 15? Thank you very much.

13 And so I know that you weren't at this
14 meeting, and you weren't involved in these decisions, and so
15 I understand your answer might be you don't know, but we --
16 but this is now before us and so I'd like to ask you some
17 questions about this if I could.

18 MR. BENOÎT DICAIRE: Yeah.

19 MR. SUJIT CHOUDHRY: Okay. And so it's about
20 the decision that was taken in February -- on -- in the wake
21 of the February 17th, 2021 meeting between Mr. Touati and
22 members of CSIS and the CSE it would seem regarding the
23 attack and the information that was provided. And if I
24 understand it correctly here, after the briefing, the
25 decision was taken that since the attack was not successful,
26 it was therefore not necessary to warn the MPs. Is that
27 fair?

28 MR. BENOÎT DICAIRE: That's a fair

1 assessment.

2 MR. SUJIT CHOUDHRY: Okay. Could you tell me
3 who -- I know this came up, but I want to get a bit more
4 precision on this. Who made that decision?

5 MR. BENOÎT DICAIRE: I think this is the
6 normal protocol, if we were -- again, this morning as part of
7 my testimony, if we were to advise of every attack, we would
8 be -- we're talking about hundreds of millions of attack
9 attempts.

10 MR. SUJIT CHOUDHRY: Okay.

11 MR. BENOÎT DICAIRE: So I think we would have
12 a problem in being able to scale.

13 MR. SUJIT CHOUDHRY: Okay. And so just to
14 pursue this a bit, would -- even if the decision was made by
15 you or a member of your team, which is what I think the
16 answer is, would the -- are there circumstances in which the
17 speaker would ever be advised that you'd decided not to warn
18 a member of parliament?

19 MR. BENOÎT DICAIRE: I think if there were a
20 risk, inherent risk to the House of Commons, the continuity
21 of operation, the infrastructure, the information, something
22 of serious nature, it would go to the clerk of the House of
23 Commons and first, and then ---

24 MR. SUJIT CHOUDHRY: Okay.

25 MR. BENOÎT DICAIRE: --- through that
26 channel, then a determination would be to advise the speaker
27 on it.

28 MR. SUJIT CHOUDHRY: So is it fair to say

1 that what would go to the clerk first and then possibly with
2 the speaker would be threats to the operation of the Commons
3 as an institution?

4 **MR. BENOÎT DICAIRE:** As an institution, yes.

5 **MR. SUJIT CHOUDHRY:** Okay. But that's
6 different than, let's say, interference with the performance
7 of duties by a member of parliament?

8 **MR. BENOÎT DICAIRE:** It's different, yeah.

9 **MR. SUJIT CHOUDHRY:** Okay. And then would --
10 and I think I know the answer to this question, are there any
11 circumstances under which the Board of Internal Economy would
12 ever be advised of a cyber security attack, even if it was
13 not successful?

14 **MR. BENOÎT DICAIRE:** In those parameters? I
15 don't think so.

16 **MR. SUJIT CHOUDHRY:** Okay. And so I ---

17 **MR. BENOÎT DICAIRE:** It's not successful.

18 **MR. SUJIT CHOUDHRY:** Okay. And so just to
19 pursue this point a bit, so you -- I think you've been
20 referred to the testimony of MPs Genius and MP McKay, who
21 were both targeted by this attack, and they have drawn a
22 direct line between being targets and the work they do as
23 parliamentarians, in particular, as part of the IPAC, this
24 interparliamentary group involving China that's a global
25 group. And so they have sort of said they would have liked
26 to have been told. And that they -- had they been told, they
27 could have taken protective measures. So, for example, they
28 might have known about this, let's call it the pixel attack.

1 I'm not a technical person, so forgive me if I'm getting it
2 wrong. And so I'd like maybe to take you to -- to not look
3 at what's happened, but to think about things on a go-forward
4 basis.

5 **MR. BENOÎT DICAIRE:** M'hm.

6 **MR. SUJIT CHOUDHRY:** Okay? So on a go-
7 forward basis, if your team became aware that an attack was
8 state sponsored, even if it was not successful, do you think
9 the member of parliament in question or the members of
10 Parliament in question should be advised?

11 **MR. BENOÎT DICAIRE:** If -- it's a tricky
12 question to answer. Yes, they should be advised, but by who?

13 **MR. SUJIT CHOUDHRY:** Okay.

14 **MR. BENOÎT DICAIRE:** And is it part of my
15 mandate to provide that advice? I'll give you the example
16 specifically for Mr. Genius, there is no possibility I could
17 ever advise because we -- it wasn't a House of Commons device
18 that was targeted, so we didn't have any information about
19 Mr. Genius.

20 **MR. SUJIT CHOUDHRY:** So I see. Whereas, for
21 Mr. McKay, it was a House of Commons device?

22 **MR. BENOÎT DICAIRE:** Yes, it was.

23 **MR. SUJIT CHOUDHRY:** Okay. And so then let's
24 focus on House of Commons devices then. So for -- so if a
25 member of parliament's House of Commons device was targeted,
26 and if your team -- and it was unsuccessful, but your team
27 came into possession of information that the attack was state
28 sponsored, going forward, should that member of parliament be

1 advised?

2 **MR. BENOÎT DICAIRE:** Would be a collaboration
3 effort between if there's a recommendation from the security
4 intelligence agencies that they would have a particular angle
5 to want to warn -- because, again, this goes beyond my
6 mandate.

7 **MR. SUJIT CHOUDHRY:** Right.

8 **MR. BENOÎT DICAIRE:** So if they would make a
9 recommendation based on their assessment or based on
10 information I might not be privy to, then they would -- then
11 it would be a collaboration between the security agencies and
12 us and then a decision would be made based on risks, or based
13 on impacts, or based on potential other factors.

14 **MR. SUJIT CHOUDHRY:** And would the warning,
15 or the information, or the briefing come from your team, or
16 from the intelligence agencies, or both?

17 **MR. BENOÎT DICAIRE:** Probably in a
18 combination of the both. So if we participate into an
19 investigation or into the forensics tied to a cyber attack,
20 then they potentially wouldn't require us to be at the table,
21 but if it is completely on their privy, they would coordinate
22 with us to just coordinate the briefing and they would lead
23 the briefing.

24 **MR. SUJIT CHOUDHRY:** Okay. You know, one of
25 the things we're trying to grapple with are these silos of
26 different responsibilities and different legal instruments.
27 So you've probably heard the term "threat reduction measure",
28 and I think that was posed to Mr. McDonell as well. And so,

1 you know, from a layperson's perspective, this type of a
2 briefing about a thwarted cyber attack might -- feels like a
3 threat reduction measure of a sort. It might not be the type
4 of threat that CSIS classifies this as, but it feels like
5 that to a member of parliament. Would you agree?

6 **MR. BENOÎT DICAIRE:** You would have to ask a
7 member of parliament.

8 **MR. SUJIT CHOUDHRY:** Okay. Fair enough. So,
9 look, can I take you to CANSUM27, please? And could we go to
10 paragraph 11(i), or 11(i).

11 So, Mr. Dicaire, are you -- you're familiar
12 with this document?

13 **MR. BENOÎT DICAIRE:** Yes, I am.

14 **MR. SUJIT CHOUDHRY:** So I want to ask you a
15 question about 11(i). And what it says there for the record
16 is that,

17 "Immediately following the 17
18 February meeting, with the [House of
19 Commons], CSE officials internally
20 expressed concern that the [House of
21 Commons] had not been given
22 sufficient information to appreciate
23 the significance of the threat."

24 And so I wanted to draw your attention to
25 that sentence and relate it to an answer you gave to
26 Commission counsel about the nature of the information that
27 was provided to your team, and I recognize you weren't there
28 in 2021. And you honed in on the word "suspected" attack,

1 and said the fact that it was suspected might have meant that
2 it didn't pass a certain threshold. But this evidence
3 suggests that perhaps the level of suspicion was higher than
4 just suspected and that information wasn't communicated to
5 you. So I want to circle back to your -- to this issue and
6 ask you this. If the information had presented to you with a
7 bit more certainty, recognizing that we can never be
8 absolutely certain about where threats come from, would you
9 at that point, would it have been appropriate at that point
10 for your team to have advised the member of parliaments --
11 members of Parliament in question?

12 **MR. BENOÎT DICAIRE:** Again, I think the
13 parameters that would have been looked at would have been
14 from the angle of threat to the member specifically at that
15 time for that cyber attack specifically, and the level of
16 risk tied to this attack. So in partnership, of course, it
17 is a partnership with the security agencies, we would have
18 had certain, you know, a dialogue around, okay, what do we do
19 here, but in this context, we didn't have a lot of
20 information, so it's hard for me to speculate what we would
21 have done if we had more information. But at the same point
22 in time, recommendations would have been with more
23 information, probably more prescriptive.

24 **MR. SUJIT CHOUDHRY:** Okay. Thank you, sir.
25 Thank you, gentlemen, for your time.

26 **COMMISSIONER HOGUE:** Thank you. Next one is
27 the Concern Group.

28 **MR. GABRIEL POLIQUIN:** I understand Concern

1 Group doesn't have any questions.

2 COMMISSIONER HOGUE: No questions? RCDA?

3 MR. GUILLAUME SIROIS: No questions either.

4 COMMISSIONER HOGUE: Human Rights Coalition.

5 --- CROSS-EXAMINATION BY MS. SARAH TEICH:

6 MS. SARAH TEICH: Good afternoon. We heard
7 last week from MPs Genuis and McKay and they both expressed
8 concerns about the possibility that in relation to the APT31
9 cyber attacks, members of diaspora communities with whom they
10 were in contact may have been inadvertently exposed. Do you
11 share these concerns?

12 MR. PATRICK McDONELL: I didn't hear the
13 question. I'm sorry.

14 MS. SARAH TEICH: Is this better?

15 MR. PATRICK McDONELL: Hopefully.

16 MS. SARAH TEICH: Okay. Let's try this
17 again.

18 MR. PATRICK McDONELL: Okay.

19 MS. SARAH TEICH: We heard from MPs Genuis
20 and McKay last week and they both expressed concerns about
21 the possibility that in relation to the cyber attacks,
22 members of diaspora communities with whom they were in
23 contact may have been inadvertently exposed. Do you share
24 these concerns?

25 MR. PATRICK McDONELL: I have no comment on
26 that.

27 MR. BENOÎT DICAIRE: I think that's beyond
28 our mandate. Our mandate is parliamentarians and

1 parliamentary devices.

2 **MS. SARAH TEICH:** Okay. In general -- and
3 now I'll ask generally about your policies. If a
4 parliamentary account is compromised, does the House of
5 Commons administration look at or investigate potential
6 impacts on diaspora community members who are in contact with
7 the compromised account?

8 **MR. BENOÎT DICAIRE:** I think that the
9 analysis that's going to be done is going to be on the impact of
10 the attack or the compromise and then the scale of it. So
11 should it have ripple effects, regardless of which community,
12 it would be looked at from that perspective. It's really a
13 technical evaluation at that point in time and understanding
14 the depth of the attack or the success of that attack will
15 determine the action.

16 **MS. SARAH TEICH:** Okay. And according, again
17 generally, to your policy, if you were to find out that
18 members of diaspora communities were impacted, would you let
19 them know?

20 **MR. BENOÎT DICAIRE:** If they were part of the
21 technical evaluation, if they were in a scope, I would
22 suspect that, you know, we would action -- take the
23 appropriate actions. It's hard to comment on a very broad
24 statement like that one.

25 **MS. SARAH TEICH:** Okay. Would it be helpful
26 if you had a policy that would tell you in such and such a
27 case, we would notify them or we would offer them these
28 supports? Because it sounds like right now it's on a case-

1 by-case basis.

2 **MR. BENOÎT DICAIRE:** I think our focus is on
3 parliamentarians and parliamentary infrastructure. I don't
4 know about you, Pat, but that's the scenario on our side. So
5 our focus is really around the mandate that we are given.

6 **MS. SARAH TEICH:** Okay. Can we please pull
7 up HOC1? And can we scroll to the top at page 12? Thank
8 you.

9 Here it says:

10 "The House administration maintains
11 strong partnerships..."

12 I won't read the whole sentence:

13 "...including with RCMP, CSIS, Public
14 Safety, and CSE..."

15 Have you ever recommended to one or more of
16 these organizations that they should provide support to
17 members of diaspora communities that may have been impacted
18 by a cyber attack on members of Parliament?

19 **MR. BENOÎT DICAIRE:** Not to my knowledge.

20 **MS. SARAH TEICH:** Should the House of Commons
21 administration make such a recommendation in the future?

22 **MR. BENOÎT DICAIRE:** That is up to the
23 Commission to look at some of those findings.

24 **MS. SARAH TEICH:** Okay. No further
25 questions. Thank you.

26 **COMMISSIONER HOGUE:** Thank you.

27 AG.

28 **--- CROSS-EXAMINATION BY MR. GREGORY TZEMENAKIS:**

1 **MR. GREGORY TZEMENAKIS:** Good afternoon. My
2 name is Gregory Tzemenakis. I'm Government counsel. I'm
3 just going to ask you some questions of clarifications from
4 your witness statements, and where appropriate, I will call
5 them up.

6 I will also use the term "Member" and "MP"
7 interchangeably to refer to a Member of the House of Commons.

8 So I want to start with some questions on
9 security. Am I correct that security clearances are not
10 mandatory for members of Parliament?

11 **MR. BENOÎT DICAIRE:** That's correct.

12 **MR. GREGORY TZEMENAKIS:** House administration
13 is not responsible for providing security clearances to
14 members of Parliament? That's done through another vehicle;
15 correct?

16 **MR. PATRICK McDONELL:** We don't provide
17 security clearances to members of Parliament.

18 **MR. GREGORY TZEMENAKIS:** And am I also
19 correct that House administration does not offer direct
20 support for IT matters that extend beyond official
21 parliamentary accounts, such as the personal email accounts,
22 unless it's incidental, if I can put it that way, to
23 parliamentary business?

24 **MR. BENOÎT DICAIRE:** That's correct.

25 **MR. GREGORY TZEMENAKIS:** And MPs are not
26 technically entitled to use devices that have not been
27 authorized by your services, sorry, the Division that you
28 lead, to conduct parliamentary business on personal devices?

1 Is that correct?

2 **MR. PATRICK McDONELL:** That's correct.

3 **MR. GREGORY TZEMENAKIS:** But it -- in the --
4 it is -- sorry. From your testimony of earlier today, I also
5 heard you to say that you -- the House administration does
6 not have an independent way to determine whether or not an
7 MP's personal device has been compromised, because it's not
8 within your mandate and it's not within the scope of the what
9 I'll call parliamentary IT network that you manage? Is that
10 correct?

11 **MR. BENOÎT DICAIRE:** Our mandate is
12 parliamentary.

13 **MR. GREGORY TZEMENAKIS:** Right. But an MP
14 can come to you if there is an issue and ask for your
15 assistance; correct?

16 **MR. BENOÎT DICAIRE:** And we'll do it on a
17 best effort basis.

18 **MR. GREGORY TZEMENAKIS:** Best effort basis.
19 And am I also correct -- this is a question for you, sir, am
20 I also correct that Members do not have an express obligation
21 to report attempts either at physical security or other
22 issues of concern to them, including foreign interference, to
23 your office, to the sergeant-at-arms?

24 **MR. PATRICK McDONELL:** That's correct.

25 **MR. GREGORY TZEMENAKIS:** So I want to turn to
26 the topic of partnerships. Am I correct that the House
27 administration collaborates with external cyber security
28 partners such as CSE, CSIS, and others?

1 **MR. PATRICK McDONELL:** Correct. For CSE.

2 For myself.

3 **MR. GREGORY TZEMENAKIS:** And that you also
4 have strong partnerships with the security intelligence,
5 local law enforcement, government agencies, and the
6 government agencies include RCMP, CSIS, Public Safety, and
7 CSE?

8 **MR. PATRICK McDONELL:** Yes.

9 **MR. GREGORY TZEMENAKIS:** Yes. And more
10 formally, the sergeant-at-arms has an MOU with CSIS and the
11 RCMP; correct?

12 **MR. PATRICK McDONELL:** Correct.

13 **MR. GREGORY TZEMENAKIS:** And the CIO has an
14 MOU with CSE?

15 **MR. PATRICK McDONELL:** Correct.

16 **MR. BENOÎT DICAIRE:** That's correct.

17 **MR. GREGORY TZEMENAKIS:** And that MOU was
18 recently amended this week, I believe? Is that correct?

19 **MR. BENOÎT DICAIRE:** I'm not sure. Last
20 week, peut-être.

21 **MR. GREGORY TZEMENAKIS:** Okay. I want, if I
22 can direct your attention to -- and I'm going to ask the
23 Court Reporter to pull up WIT129, English, and go to
24 paragraph 8, please?

25 Yeah, this is an interview that was conducted
26 with Mr. Touati. And I believe, sir, you were present, Mr.
27 Dicaire?

28 **MR. BENOÎT DICAIRE:** That's correct.

1 **MR. GREGORY TZEMENAKIS:** And at paragraph 8,
2 he says, Mr. Touati says:

3 "The information received, mainly of
4 a technical nature, is 'sufficient to
5 enable the House of Commons to
6 determine whether the measures it is
7 putting in place are mitigating the
8 risks.'"

9 Do you have any reason to depart from that
10 statement, sir?

11 **MR. BENOÎT DICAIRE:** No.

12 **MR. GREGORY TZEMENAKIS:** No. Thank you. I
13 want to turn to the next topic, which is briefings. My
14 understanding, Mr. McDonell, is that the House coordinated
15 security intelligence and law -- with security intelligence
16 and law enforcement partners to provide unclassified foreign
17 interference briefings to caucus members of all recognized
18 parties in the house?

19 **MR. PATRICK McDONELL:** Correct.

20 **MR. GREGORY TZEMENAKIS:** And that was in
21 fact done and that included not only the Liberal Party and
22 the Conservative Party, but the other recognized parties in
23 the House?

24 **MR. PATRICK McDONELL:** And independent
25 members.

26 **MR. GREGORY TZEMENAKIS:** And independent
27 members. Thank you. And just generally speaking, do you
28 agree that more training and more education about FI, FI

1 activities, and FI threats would, in addition to any other
2 efforts made by the Government of Canada, as well as the
3 public, be a good thing for members of Parliament to have?

4 **MR. PATRICK McDONELL:** Yes.

5 **MR. GREGORY TZEMENAKIS:** So I want to switch
6 topics a little bit and talk about the ability to contact
7 your office, sir.

8 So last week we heard some suggestions from
9 an MP, including from the former leader of the opposition,
10 the Honourable Mr. O'Toole, that -- and these are my words,
11 I'm paraphrasing his words, not his words, to the effect that
12 he may not have known who to contact if he had concerns about
13 FI, whether it was in relation to a member, a senator, or
14 someone else. Am I right that he could have contacted your
15 office for guidance and support?

16 **MR. PATRICK McDONELL:** Yes.

17 **MR. GREGORY TZEMENAKIS:** And was that the
18 case -- is that a relatively new phenomenon, or is that --
19 has that always been the case since you became sergeant-at-
20 arms in 2019?

21 **MR. PATRICK McDONELL:** It's always been the
22 case, but there's many Members and staff, because of their
23 portfolios, how busy they are, often they don't know where to
24 reach out. So in those briefings that we just talked about a
25 few minutes ago, when we brought in CSC, CSIS, RCMP, Public
26 Safety, we reminded the caucuses and the independents that if
27 you have a question in regards to anything security, you call
28 us and we'll coordinate it with the appropriate authority.

1 **MR. GREGORY TZEMENAKIS:** Thank you. I'm
2 going to ask some questions about APT31 and I'm going to
3 direct them to you, Mr. Dicaire.

4 So in the interview with Mr. Touati, he
5 described the relationship with CSC as a healthy
6 collaboration. Would you agree with that assessment?

7 **MR. BENOÎT DICAIRE:** I would agree.

8 **MR. GREGORY TZEMENAKIS:** You would. And the
9 following questions are to clarify what I understand some of
10 the key facts surrounding APT31. And if you disagree with
11 them, please feel free to do so.

12 Let me start with this. Am I correct that
13 the House of Commons IT group investigated and discovered
14 that the emails in question did not reach their intended
15 recipients and they were quarantined by the systems you have
16 in place?

17 **MR. BENOÎT DICAIRE:** From the first bulletin.
18 So the -- there was multiple bulletins. The first bulletins,
19 the emails were quarantined.

20 **MR. GREGORY TZEMENAKIS:** And that there was
21 no threat to Parliament or its infrastructure; correct?

22 **MR. BENOÎT DICAIRE:** That's correct.

23 **MR. GREGORY TZEMENAKIS:** And am I correct
24 that once you determined that the emails -- once it was
25 determined that the emails did not reach their recipients,
26 there was not a need to do something more? And that comes
27 from your witness statement. I can pull it up. It's at
28 paragraph 69, for the purposes of the record.

1 **MR. BENOÎT DICAIRE:** For the purpose of our
2 mandate, the threat was addressed.

3 **MR. GREGORY TZEMENAKIS:** All right. I'm
4 going to ask the Court Reporter to pull up WIT129, paragraph
5 13, which my friend just took you to. I'm going to take you
6 to a different part of that paragraph.

7 In this summary, Mr. Touati states that he
8 participated in a classified briefing of February 17th, and
9 then he states during this briefing:

10 "...Mr. Touati was informed that
11 government agencies suspected that a
12 malign hacking group with suspected
13 links to the People's Republic of
14 China, known as APT31, was
15 responsible for the activities
16 detected in January 2021 targeting
17 parliamentarians' email accounts."

18 Was that information relayed to you?

19 **MR. BENOÎT DICAIRE:** I was part of the
20 briefing when he said that.

21 **MR. GREGORY TZEMENAKIS:** All right. So at
22 that time in February of 2021, you knew that the event that
23 took place in January was linked to a hacking group suspected
24 -- sorry, was suspect -- was -- I'm not going paraphrase it.
25 Scratch that. Was -- you knew in February of 2021 that the
26 event that took place in January of 2021 was suspected to be
27 linked to the People's Republic of China through APT31?

28 **MR. BENOÎT DICAIRE:** My organization -- I

1 wasn't there at the time. My organization was briefed that
2 they suspected, so the statements on paragraph 13 are
3 correct.

4 **MR. GREGORY TZEMENAKIS:** Okay. And there's
5 also a reference in the other affidavit that all eight of the
6 MPs -- that emails were sent to all eight of the MPs that
7 were concerned, inquiring whether or not they had received an
8 email of -- the email in question; correct?

9 **MR. BENOÎT DICAIRE:** That was part of the
10 first few actions as part of the follow-up to the bulletin.

11 **MR. GREGORY TZEMENAKIS:** Okay. And all
12 eight MPs responded that they either had not or did?

13 **MR. BENOÎT DICAIRE:** Only two responded.

14 **MR. GREGORY TZEMENAKIS:** Only two responded.

15 So, Madam Commissioner, it seems that I have
16 11 seconds left, but I ask for your indulgence for four
17 minutes to just finish one last topic, please?

18 **COMMISSIONER HOGUE:** You're lucky there's
19 many that have no questions. So you can go on for four
20 minutes.

21 **MR. GREGORY TZEMENAKIS:** Thank you.

22 Mr. Dicaire, I just want to revisit your
23 testimony of earlier today when we were talking about the
24 initial bulletin that had been received from CSE in January
25 of 2021. And you'll recall you had a discussion with
26 Commission counsel around whether or not that event -- the
27 words used by CSC or the Cyber Security Centre was that it
28 was likely not malicious. Do you recall that discussion this

1 morning?

2 MR. BENOÎT DICAIRE: Yes.

3 MR. GREGORY TZEMENAKIS: And have you had an
4 opportunity to review that bulletin before appearing here
5 today?

6 MR. BENOÎT DICAIRE: Yes, I have the bulletin
7 right in front of me right now.

8 MR. GREGORY TZEMENAKIS: Okay. I'm going to
9 suggest to you, and we have certain rules in process here,
10 I'm going to suggest to you, and I anticipate that we will
11 hear from CSC on Thursday that the bulletin contains slightly
12 different information. So the first thing the bulletin
13 contained was technical information disclosing that the
14 emails contained a tracking link to it. Are you aware of
15 that -- or were you aware of that at the time and are you
16 aware of that now?

17 MR. BENOÎT DICAIRE: I'm aware of it now, as
18 I'm reading it right in front of me.

19 MR. GREGORY TZEMENAKIS: Okay. And that the
20 bulletin stated that the emails:

21 "...are likely targeting individuals as
22 part of an ongoing collection
23 campaign."? (As read)

24 MR. BENOÎT DICAIRE: That's correct.

25 MR. GREGORY TZEMENAKIS: And then -- I'm not
26 a technical person, so if there's a distinction, please
27 educate us. I understand that the bulletin also states that
28 the emails likely contained no malicious content, not that it

1 was likely not malicious. It's the content that wasn't
2 malicious. Is that right?

3 **MR. BENOÎT DICAIRE:** You're right.

4 **MR. GREGORY TZEMENAKIS:** And in plain
5 English to somebody like me, does that mean that it didn't
6 contain, for example, malware?

7 **MR. BENOÎT DICAIRE:** Yes, that would be one
8 good way of saying it.

9 **MR. GREGORY TZEMENAKIS:** Good way of saying
10 it. So the bulletin didn't say that the attack was likely
11 not malicious. It was commenting on the substance of what
12 the emails were concerned about?

13 **MR. BENOÎT DICAIRE:** That's it. There was
14 one word omitted this morning, as I recalled from my memory,
15 but now I'm reading it and it says "no malicious content".

16 **MR. GREGORY TZEMENAKIS:** And sir, my job is
17 just to make sure that the facts come out.

18 **MR. BENOÎT DICAIRE:** That's perfect.

19 **MR. GREGORY TZEMENAKIS:** And that's all. So
20 thank you for that clarification.

21 Thank you, Madam Commissioner, for the
22 indulgence of the extra time.

23 **COMMISSIONER HOGUE:** Thank you.

24 So the attorneys for the House. Do you have
25 [no interpretation]?

26 **MR. MICHEL BÉDARD:** [No interpretation]

27 **COMMISSIONER HOGUE:** [No interpretation]

28 **MR. GABRIEL POLIQUIN:** [No interpretation]

1 **COMMISSIONER HOGUE:** Thank you very much.
2 It's 20 to 3:00. The next [no
3 interpretation].

4 **THE REGISTRAR:** Order please.
5 This hearing of the Commission is now in
6 recess until 3:05 p.m.

7 --- Upon recessing at 2:42 p.m.

8 --- Upon resuming at 3:05 p.m.

9 **THE REGISTRAR:** Order please.
10 This sitting of the Foreign Interference
11 Commission is now back in session.

12 The time is 3:05 p.m.

13 **COMMISSIONER HOGUE:** Maitre MacKay, you are
14 going to [no interpretation].

15 **MR. JEAN-PHILIPPE MacKAY:** [No
16 interpretation]

17 **THE REGISTRAR:** [No interpretation]

18 **MR. STÉPHANE PERRAULT:** [No interpretation]

19 --- STÉPHANE PERRAULT, Affirmed:

20 --- EXAMINATION IN CHIEF BY MR. JEAN-PHILIPPE MacKAY:

21 **MR. JEAN-PHILIPPE MacKAY:** [No
22 interpretation] of an interview we held with you last August
23 8th. You were, at the time, accompanied by Mr. Caron, Madam
24 Villeneuve and Madam Torosian.

25 This is a document. You can see here the
26 French version. It's the translation of the original
27 summary. We can use the French document, but the original is
28 874.EN (sic).

--- EXHIBIT No. WIT0000074.EN:

Interview Summary - Elections Canada
(Stage 2)

--- EXHIBIT No. WIT0000074.FR:

Résumé d'entrevue: Élections Canada
(Stéphane Perrault, Serge Caron,
Josée Villeneuve et Susan Torosian)

MR. JEAN-PHILIPPE MacKAY: You've had the
opportunity to review this document before coming here today?

MR. STÉPHANE PERRAULT: Yes, absolutely.

MR. JEAN-PHILIPPE MacKAY: And you accept
that this document is part of your evidence before the
Commission?

MR. STÉPHANE PERRAULT: Absolutely.

MR. JEAN-PHILIPPE MacKAY: [No
interpretation] to be tabling three affidavits that accompany
this summary, 874.1, .2 and .3, which are the affidavits of
the three officials of Elections Canada who accompanied Mr.
Perrault during that interview. It isn't necessary that they
be tabled here or presented.

--- EXHIBIT No. WIT0000074.1:

Affidavit of Jose Villeneuve

--- EXHIBIT No. WIT0000074.2:

Affidavit of Serge Caron

--- EXHIBIT No. WIT0000074.3:

Affidavit of Susan Torosian

MR. JEAN-PHILIPPE MacKAY: The second
document I wish to produce, Mr. Perrault, is the

1 complementary institutional report, ELC.IR.2. We have it in
2 both official languages.

3 So it's ELC.IR.2.

4 It's a 27-page document. You recognize the
5 document that we see on the screen?

6 **MR. STÉPHANE PERRAULT:** I recognize what I
7 see.

8 **MR. JEAN-PHILIPPE MacKAY:** I can only see
9 part of the first page of this document, but it is a document
10 that was shared with the Commission. We have it in both
11 languages.

12 And you recognize that this document was
13 prepared by Elections Canada on behalf of the organization.
14 You do recognize its content as being part of your evidence
15 before the Commission?

16 **MR. STÉPHANE PERRAULT:** Yes. It's a document
17 that we prepared at the request of the Commission and we did
18 produce it and table it.

19 **MR. JEAN-PHILIPPE MacKAY:** In both official
20 languages. So we have EN and FR for both languages.

21 **--- EXHIBIT No. ELC.IR.0000002.EN:**

22 Elections Canada's Supplementary
23 Institutional Report August 2024

24 **--- EXHIBIT No. ELC.IR.0000002.FR:**

25 Rapport institutionnel supplémentaire
26 d'élections Canada

27 **MR. JEAN-PHILIPPE MacKAY:** Mr. Perrault, I'll
28 begin. You appeared before the Commission in March of last

1 year, and at that time you stated what the mandate of
2 Elections Canada was and what your role was. And I would ask
3 you to explain once again, generally speaking, what the role
4 of Elections Canada is and what your role is for Elections
5 Canada.

6 **MR. STÉPHANE PERRAULT:** As Chief Electoral
7 Officer, I'm the main administrator of the organization of
8 Elections Canada and I'm the main officer of the office,
9 which involves the Commissioner's office, but acting
10 independently.

11 Elections Canada's mandate is -- its main
12 mandate is the administration of federal elections, be they
13 by-elections or General Elections. This includes the
14 appointment of the 343 officers who can hire staff during
15 elections. This includes information campaigns, all the
16 preparatory work. It also includes, among other things, the
17 administration of the rules and the audits to verify that the
18 reports are faithful to the facts.

19 **MR. JEAN-PHILIPPE MacKAY:** We have
20 interpretation, Mr. Perrault, in both official languages, so
21 -- and in sign language, so I'd ask you, please, to slow down
22 somewhat, to not speak too quickly. And I'll remind you once
23 again if need be if I deem that you're speaking too quickly.

24 I just wanted to underscore this.

25 So quickly now, what's the relationship
26 between your organization and the Federal Elections Bureau?

27 **MR. STÉPHANE PERRAULT:** As Chief Elections
28 Officer, I appoint, in consultation with my colleague as

1 provided for by the Act, and we carry out administrative
2 tasks as well with regard to verification of the localities
3 that are chosen.

4 We also can carry out investigations in order
5 to enforce the law.

6 **MR. JEAN-PHILIPPE MacKAY:** Is it in that
7 context, and we discussed this during the interview, when the
8 Elections Commissioner wanted to obtain infrastructure to
9 deal with the confidential information you had a role to
10 play?

11 **MR. STÉPHANE PERRAULT:** Yes,
12 administratively. We are putting in place offices to allow
13 the Commissioner to retain secret documents -- top secret
14 documents.

15 **MR. JEAN-PHILIPPE MacKAY:** We're going to
16 talk soon about the obtention of evidence. Might you explain
17 to us quickly -- and you discussed this during our initial
18 interview. Does Elections Canada deem that it requires
19 facilities on site?

20 **MR. STÉPHANE PERRAULT:** We're consumers of
21 information, but not at the same level as the Commissioner.
22 For us, it's not necessary to be able to retain on site top
23 secret documents. They can be presented to us if need be.
24 It happens rarely. But more regularly, we are exposed to
25 secret documents and we do retain those documents.

26 **MR. JEAN-PHILIPPE MacKAY:** With regard to
27 foreign interference, might you discuss generally with us,
28 and we'll deal with details later, the way in which the theme

1 or the subject of foreign interference interacts with your
2 mandate?

3 **MR. STÉPHANE PERRAULT:** Elections Canada is
4 responsible for the security of the process. When I talk
5 about security, I'm talking about the security of its
6 physical infrastructures, security with regard as well to its
7 digital services, with regard to data. We work very closely
8 with the Cyber Security Centre, the experts in this field,
9 but we also have a play -- a role to play.

10 We also ensure the security of the
11 information that voters have in order to be able to vote. We
12 want to ensure that there's no misinformation, disinformation
13 targeting voters. We inform voters, and we also oversee the
14 social media environment, the media environment in order to
15 be able to intervene if there's false information that might
16 mislead voters with regard to the way of voting or the time
17 to vote. We want to ensure they're provided with correct
18 information.

19 There can be overlap with some foreign
20 interference situations, foreign interference situations that
21 we've seen. And I also said that we enforce the application,
22 observation of the financial rules. We want to ensure that
23 the *Elections Act* is respected with regard to finances,
24 expenditures and, of course, we can become involved in that
25 area as well. But generally speaking, we're not experts in
26 national security. We don't have first line, frontline role
27 in this area, but we must ensure the security of the
28 electoral process, and clearly there are aspects of foreign

1 interference that interest us.

2 **COMMISSIONER HOGUE:** Mr. Perrault, when you
3 say that your organization supervised the information that's
4 distributed, is this the information having to do with the
5 elections process, for example, how to vote, when to vote,
6 where to go, or is it broader than that, and do you also look
7 at the content, for example, of information products that can
8 circulate?

9 **MR. STÉPHANE PERRAULT:** [No interpretation]
10 blocked or something that might interfere with the vote or
11 the perception that Canadians have of the electoral process.

12 It's important to mention that we're not
13 interested in partisan discourses for or against a candidate.
14 When we do some research with keywords, we catch, if I can
15 say, all types of conversations which are public. We don't
16 get into private bubbles or conversations which might be of a
17 partisan nature, but we really focus on the need for
18 Canadians to be able to vote freely.

19 We don't have any specific expertise allowing
20 us to detect what's foreign and what's national. We simply
21 survey some 15 languages. But now are these people
22 expressing themselves in Canada or elsewhere or if their
23 influence might be from abroad. We don't have that
24 expertise.

25 **MR. JEAN-PHILIPPE MacKAY:** Mr. Perrault, I'd
26 like to discuss the issue of disinformation, and afterwards
27 we'll come back to the integrity of the elections,
28 interaction with other government agencies.

1 Now, for disinformation, you mentioned it in
2 your previous testimony before this Commission. Could you
3 briefly explain the infrastructure at Elections Canada which
4 does the work you just described, surveillance or surveying
5 social media, and how do you -- or different products
6 resulting of it you've exchanged with other partners,
7 government or other partners. Could you show us a picture of
8 the internal organization of Elections Canada on this issue?

9 **MR. STÉPHANE PERRAULT:** We have a team
10 dedicated to surveying social media. In the last election,
11 they surveyed about 15 languages and 67 platforms. Platforms
12 evolve with time. Some new ones appear and probably they'll
13 be on the increase in the next General Election.

14 So we do this continuously, not simply during
15 elections, but in between so as to better understand the
16 narrative that we see on the electoral process. So we look
17 at what's happening in provincial elections, American
18 elections to understand the types of topics which could lead
19 to misinformation on the electoral process.

20 We note that we often find some common themes
21 between jurisdictions, also themes concerning electors are
22 also fairly common.

23 And we produce weekly reports on trends and
24 major themes that we've seen. In election periods, we
25 prepare some daily reports, and these reports are shared with
26 our security partners, obviously, the elections federal
27 Commissioner, and with our partners which are members of the
28 Five Group -- the Group of Five -- the Five Eyes and the

1 rapid response group of Global Affairs.

2 This is information that we collect for our
3 own purposes and that we share with others.

4 **MR. JEAN-PHILIPPE MacKAY:** When we look at
5 your situational report, you mention the intents before
6 disinformation or -- you mentioned the things that are the
7 focus of some specific research at Elections Canada.

8 Will you explain how you spot the intentions
9 behind disinformation or the source of this disinformation?

10 **MR. STÉPHANE PERRAULT:** For us, what's
11 important is that the available information to Canadians will
12 be correct. We don't want them to be misinformed about the
13 process.

14 Now, we want to understand the intentions
15 behind misinformation. It's not particularly useful for our
16 purposes. It might be useful for some of our partners and
17 for the Commissioner in some specific cases, but for
18 informing Canadians it's not an exercise we delve into.

19 We often have some content on social media
20 that circulates a lot, and the same content, depending on the
21 persons who share it, could have some good or bad intentions
22 behind it. And we can talk of disinformation or
23 misinformation, but in our case it's not useful to know this.
24 It's not useful and we don't have the expertise required to
25 determine the source of disinformation.

26 We survey about 15 languages and whether it's
27 in a non-English or non-French language could mean that we're
28 dealing with foreign interference, obviously. For us, the

1 source is something very useful to make sure that the content
2 is adequate and correct.

3 **MR. JEAN-PHILIPPE MacKAY:** When, for example,
4 you detect some aspects which can misguide voters, how does
5 Elections Canada react to this type of information?

6 **MR. STÉPHANE PERRAULT:** The main mechanism is
7 to make sure that our content will be adjusted to amplify
8 some key messages which present proper information to
9 electors, voters. Yes, we can intervene within the digital
10 platforms. We can show that some message is wrong, and each
11 digital platform has their own policy to deal with it.

12 We don't ask for the information to be
13 withdrawn. Up to now, we thought it was simply sufficient to
14 mention errors and, on our side, to push correct information,
15 to make it available.

16 One of the reasons behind the survey we have
17 outside of the election period is to constantly adapt our
18 message to make sure that we follow the conversations on the
19 elections in Canada.

20 **MR. JEAN-PHILIPPE MacKAY:** And in which way
21 does Elections Canada broadcast these messages? How does ---

22 **MR. STÉPHANE PERRAULT:** How do we distribute
23 this information? We have several mechanisms. Let me
24 elaborate a bit.

25 In my mandate, my mandate is to inform
26 Canadians on the electoral process. There are four major
27 axes.

28 First of all, what we call the voter

1 information campaign is of a more general order. The mandate
2 is to inform all the population of the electoral process,
3 either through our website where we have a lot of content on
4 the electoral process, or during elections through publicity
5 campaigns, advertising campaigns or the voters' information
6 map or the voters' guide.

7 All this targets the general population, and
8 typically it orients Canadians to our website where we have
9 more detailed information, so that's the more general type of
10 intervention.

11 We also have some community officers which
12 are hired during the electoral campaign organized -- at the
13 last election, there were about 1,500. And they're hired to
14 work to groups within communities which might face some
15 obstacles to participate in the elections. We're talking
16 about the homeless, Indigenous people, ethnocultural groups,
17 youth or elderly people who need some care.

18 So the returning officers, based on the
19 composition of their community, will hire these people and we
20 can work with these communities and inform them -- better
21 inform them on the electoral process.

22 And the ethnocultural communities, to give
23 you an order of scale, there were about 200 in the last
24 elections. These are community relations officers.

25 **MR. JEAN-PHILIPPE MacKAY:** Let me come back
26 on this.

27 In the first interview with you, it was
28 mentioned that -- in a discussion on foreign interference,

1 the issue of the secret ballot was raised as a concern in
2 some communities.

3 Is it through these community relations
4 officers or through these information campaigns that you've
5 learned this, that these type of concerns emerged? Is this
6 concern, in fact -- is this how Elections Canada acts to make
7 sure that voters of all categories become familiar with
8 protection mechanisms?

9 **MR. STÉPHANE PERRAULT:** In the last few
10 months, we increased all our content on protection mechanisms
11 in all our communications. All our community relations
12 officers which -- were offered some more explicit
13 explanations on the secret ballot. That's what is important
14 to understand for people who might seem insecure or have some
15 concerns about their participation to the vote.

16 But it's not the only mechanism we have, and
17 I come to the third component of our information mandate. We
18 have a program called "Inspiring Democracy". It's based on a
19 group of -- community groups which have some special
20 relations with some copy communities. There are about 800
21 intervenors who use material we prepare for them to help
22 people better understand how to participate in the election,
23 as in the voter or candidate or simply the electoral worker.

24 Now, among them are about 100 with which we
25 sign contracts and we assign them to a specific task, but
26 others work on a voluntary basis.

27 There are about 40 of such groups who work
28 with ethnocultural communities.

1 Again, the content of protection measures was
2 highlighted, reassuring people as to the secrecy of the
3 ballot and, finally, information to citizenship which targets
4 young voters. We have programs to be in schools which
5 present some content. Also, again, we've improved this
6 content in the past while.

7 So these are the major mechanisms we use to
8 inform Canadians.

9 **MR. JEAN-PHILIPPE MacKAY:** I'd like to see
10 WIT74.

11 I'd like to direct your attention to
12 paragraph 28, Mr. Perrault, and I'd like to hear what you
13 have to say about this topic, which was also discussed during
14 the interview. There's some information which might lead to
15 believe that some foreign states might use some groups or
16 community organizations in Canada as intermediates in the
17 context of foreign interference.

18 I'd like you to elaborate on this since
19 Election Canada deals with community groups. Is this a
20 concern? Is this something that you have in mind when you
21 hire or you work with certain groups?

22 **MR. STÉPHANE PERRAULT:** As I said in my
23 interview because that was a reaction to a question I was
24 asked, we don't have any mechanism which allows us to check
25 with security services to get information about these groups.
26 These groups we create with the information we've prepared,
27 so we give them products of Elections Canada to present and
28 to work with in the community.

1 So I'm not concerned that these tools will be
2 used for foreign interference purposes.

3 **MR. JEAN-PHILIPPE MacKAY:** And when you
4 mentioned that -- it's important, is that you don't want
5 groups to use these opportunities to try to influence the
6 vote.

7 **MR. STÉPHANE PERRAULT:** Well, they're going
8 to have some partisan activities. Those who don't have a
9 contractual relationship with us are not -- don't necessarily
10 have to be neutral. We even give this information to
11 political Parties.

12 Of the 800 groups we work with, some might
13 have some political leanings, but groups which work
14 contractually with Elections Canada must be neutral. So
15 there's a mix of groups, but all these groups use products
16 which were prepared by Elections Canada in which we flag the
17 electoral process.

18 **MR. JEAN-PHILIPPE MacKAY:** Now, we have four
19 programs that you've just mentioned. And as we said in the
20 interview, some new Canadian groups might suffer some
21 transnational repression. In which way does Elections Canada
22 answer to some of these concerns, and how do we deal with the
23 potential consequences of some forms of intimidation aiming
24 to influence Canadians not to vote or to vote for a certain
25 Party based on the pressures they might be under?

26 **MR. STÉPHANE PERRAULT:** Well, it's a topic of
27 concern and other organizations than Elections Canada are
28 also interested in this. But there are two things to

1 highlight.

2 One thing we should explain to electors is
3 that there does exist a multitude of ways to vote, whether in
4 the ballot office or voting by anticipation or by the mail,
5 and it can even be in the office of another returning officer
6 in an urban context where there are many ridings.

7 Voters must feel comfortable voting, so
8 that's one element.

9 The other element that we mentioned is the
10 confidentiality, the secrecy of voting. There are processes
11 in place to ensure that one's vote remains secret,
12 confidential, and Canadians must be reassured in this, in the
13 knowledge that no one else will be able to know how they
14 voted.

15 **MR. JEAN-PHILIPPE MacKAY:** Another question
16 in this with regard to the accessibility of information.
17 What are the measures put in place by Elections Canada to
18 ensure that the information can be communicated so as to be
19 well understood by Canadians who don't necessarily understand
20 English or French?

21 **MR. STÉPHANE PERRAULT:** Well, we have a broad
22 gamut of products. We have the guide that's available in
23 languages, 49 languages plus English and French, with 16
24 Aboriginal languages and 33 other languages spoken throughout
25 the country.

26 We also produced for the next elections a
27 guide for the media of other cultural groups, groups speaking
28 Cantonese, Punjabi, Mandarin in particular, to explain the

1 process, but also the protection mechanisms for the voting
2 process.

3 So we do have a variety of sources of
4 information. Voters can communicate with us and we have an
5 interpretation service that allows us to interact with people
6 in close to 200 languages. So we do offer this service to
7 Canadians.

8 **MR. JEAN-PHILIPPE MacKAY:** Coming back to
9 disinformation and misinformation, in the summary of the
10 interview -- and we can see it on the screen, paragraph 54.

11 We're talking about the rapid response of
12 Foreign Affairs -- Global Affairs Canada. And Ms. Torosian,
13 I think, mentioned this. Elections Canada is still trying to
14 reach an agreement with information sharing -- on information
15 sharing with Global Affairs Canada, and we've been told that
16 the objective of this agreement is to ensure the proper
17 functioning of our elections the next time around.

18 So what would the objective be when you talk
19 about formalizing the situation?

20 **MR. STÉPHANE PERRAULT:** It's to provide
21 clarity with regard to the circumstances, what is to be
22 shared, when, with whom. We want to frame the relationship
23 for both organizations.

24 This is done informally at present, and we
25 believe it would be preferable to have more precise framework
26 with regard to information sharing.

27 **MR. JEAN-PHILIPPE MacKAY:** Does Elections
28 Canada have reports on misinformation with regard to the

1 elections process? Does it have relationships with other
2 agencies, other departments within the Canadian government?

3 **MR. STÉPHANE PERRAULT:** We share our reports
4 with various partners within the SITE group. I used the
5 acronym earlier. So it's Global Affairs, it's CSIS, the RCMP
6 and the Communications Security Establishment. It's a group
7 that's active when elections are held, and it was also active
8 in the spring of 2023. It becomes involved with by-
9 elections.

10 And there's also an electoral security
11 organization that exists at the level of Deputy Minister, and
12 this group groups together a broader number of participants
13 involved in security and safety, and it's via this working
14 group, this task force, that information is circulated.

15 **MR. JEAN-PHILIPPE MacKAY:** We'll come back to
16 these structures in a few minutes. But prior to that, you
17 mentioned during our interview with you in the summer that
18 artificial intelligence is a concern for you. It is
19 something that must be watched. We have to be able to react
20 to the growing role and impact of artificial intelligence in
21 the information ecosystem. And I'd like to hear you with
22 regard to this concern that you shared with us.

23 **MR. STÉPHANE PERRAULT:** This is a phenomenon
24 that's emerging and it's evolving very quickly. The Cyber
25 Security Centre deals with this in its regular reports.

26 There's deep fake, "hyper-trucage" in French.
27 We follow what happens in the States. We'll be following
28 this closely in the upcoming American elections.

1 C-65 is going to be studied on the Hill
2 shortly and I will be appearing in the context of the study
3 of this Bill dealing with deep fakes. To date, we haven't
4 seen this widely spread in Canada, but in the U.S., in the UK
5 this is a frequent issue.

6 We want to combat the circulation of false
7 information in the context of elections. We're going to
8 discuss this with the producers of platforms that use AI. We
9 want to ensure that the information produced via AI will not
10 be misleading because that could amplify false information
11 with regard to the electoral process.

12 **MR. JEAN-PHILIPPE MacKAY:** I'm now going to
13 show another document to help us with my next line of
14 questioning.

15 So CAN4997 (sic).

16 **--- EXHIBIT No. CAN004599:**

17 Site Status Update and Summary of
18 Foreign Interference Threats to
19 Canadian Democratic Institutions-2023

20 **MR. JEAN-PHILIPPE MacKAY:** It's a document,
21 Mr. Perrault, to give you some context, it's an update of the
22 Task Force. It's SITE, MSRE in French. So we can use the
23 English acronym.

24 It's an update for the Deputy Ministers
25 committee that you mentioned earlier, that working group that
26 deals with coordination around election security.

27 When we look at this first paragraph here,
28 elections are described as being a window of opportunity.

28 So all that we can do to increase the

1 security of the process is what interests us, and this is
2 motivated -- greatly motivated by the growth, the increase of
3 the threat that we started noting in 2016-2017. It started
4 prior to that, but it increased as of those dates. And this
5 was motivated, generated via information we received on the
6 risks in other foreign states.

7 **MR. JEAN-PHILIPPE MacKAY:** When you talk
8 about the coordination apparatus for the security of
9 elections, and you did discuss this during your first
10 appearance, I would like to hear you once again on the
11 origins of this coordination apparatus for the security of
12 elections and how do these committees operate and what's your
13 relationship with those committees and your participation.

14 **MR. STÉPHANE PERRAULT:** Well, going back to
15 the 2016 elections, there was also the Brexit situation. In
16 both cases, we saw situations of concern with regard to
17 foreign interference with these two events, the Presidential
18 elections and then Brexit.

19 In 2017, the following year, I met with the
20 Privy Council experts and experts at the Communications
21 Security Establishment with a view to increasing our
22 collaboration with these organisms.

23 Prior to this, there were always security
24 exercises before an election. There were meetings with
25 partners involved in security. We discussed scenarios
26 typically, possible terrorist situations that could arise or
27 national disasters or safety issues, but it was more physical
28 than cybernetic, and it deal more with physical security

1 rather than misinformation, disinformation, et cetera.

2 After the American Presidential elections, we
3 saw interference via social media, we saw cyber attacks aimed
4 at infrastructure, namely, that of the Democratic Party in
5 the U.S. I noted, and I wasn't alone in this, that there
6 then was an important change in the environment that required
7 an ongoing and closer relationship with the security forces
8 and organizations encompassing other issues and concerns.

9 So those were my meetings. The government
10 itself had similar reflections in the following months and we
11 saw the establishment of coordination groups for election
12 security. Connection Canada co-chairs this with the Privy
13 Council, so the DGs, the Deputy Ministers and others sit
14 together and these meetings are periodical. And their aim
15 is, first and foremost, to ensure that we well understand the
16 respective mandates of the various partners involved.

17 There are tabletop exercises aimed at
18 refining the interactions that could be required in specific
19 situations, and in that context, typically, there are also
20 briefings on security situations, the evolution of threats,
21 et cetera. And this is something that continued to exist at
22 varied frequencies, and this has been ongoing since then, so
23 prior to the elections of 2019. And it's well established at
24 present.

25 **MR. JEAN-PHILIPPE MacKAY:** So we're seven
26 years down the road today. Do you deem that this apparatus,
27 that these committees have fulfilled their mission and
28 continue to fulfil it?

1 **MR. STÉPHANE PERRAULT:** Yes, absolutely,
2 they're still necessary, very necessary. We must also
3 understand that, within the government, there is constant
4 turnaround of staff and there are people who arrive in those
5 organizations who don't necessarily understand the electoral
6 process, the various mandates, and these are people who don't
7 necessarily know each other as well.

8 And there can be situations where you must
9 intervene quickly, and it's better if people know each other,
10 understand their mandates, have established practices to
11 validate the interactions and the respective mandates of each
12 intervenor. So it's essential that this be maintained.

13 **MR. JEAN-PHILIPPE MacKAY:** Briefly, what's
14 the relationship between the committees, coordinating
15 committees for elections, and the SITE working group? How do
16 the two entities interact?

17 **MR. STÉPHANE PERRAULT:** Well, there is some
18 overlap amongst partners, participants. The SITE group
19 participants also sit on the coordinating group and, during
20 meetings, they share information coming from the SITE group.

21 **MR. JEAN-PHILIPPE MacKAY:** During your prior
22 appearance before the Commission, there was talking of the
23 43rd and 44th elections. Have there been changes with regard
24 to the coordination of security since 2021?

25 **MR. STÉPHANE PERRAULT:** Coordination was
26 maintained between elections. What's new since the spring of
27 2023 is that the government decided to call upon the SITE
28 group during by-elections. Prior to that, this group only

1 intervened during General Elections.

2 The coordination group, as I stated earlier,
3 continues to sit at variable frequencies, but we put in place
4 the SITE group and made it active during by-elections with
5 follow-up reports. And during these elections, there are
6 regular meetings with the coordination group with regard to
7 the Deputy Ministers and the Directors-General for
8 information sharing purposes.

9 **MR. JEAN-PHILIPPE MacKAY:** So we have some
10 witnesses from the SITE working group who will testify before
11 the Commission. But in your case, during the General
12 Elections, you're not a member of the Panel of Five set up by
13 the protocol, the public protocol in case of major electoral
14 incident. But according to protocol, there is a mechanism, a
15 communication mechanism, between this panel and yourself. If
16 there's an event which impacts the administration of
17 elections, it's not the panel which will be making the public
18 announcement, but it will be you. Is that correct?

19 **MR. STÉPHANE PERRAULT:** Yes, that is correct.
20 Elections Canada is independent versus the government and
21 security partners. We cooperate very closely, but each of us
22 have our own responsibilities.

23 So the Panel of Five, as we sometimes call
24 it, which does not include the CO of Elections Canada -- I am
25 not part of it -- but there's an understanding that if there
26 should be an announcement concerning the security of our
27 elections, the parties would be informed. There's also an
28 understanding that if there's an issue which deals simply

1 with the electoral administration and which is part of my
2 mandate and if I need -- if I believe I need to inform
3 Canadians publicly, I would be making that announcement. But
4 it could be accompanied by some partners in cyber security
5 matters, for example.

6 In the same way, if the panel had to take a -
7 - pronounce itself publicly during an election, obviously it
8 would not be a surprise for me, and there might be situations
9 where there are some parallel announcements. All of this is
10 possible. It's not something which has been tested yet.

11 In terms of partial elections, because we're
12 not in a transition convention, the Panel of Five is not
13 active. It's a group of Deputy Ministers of which I'm not
14 part, which, at that time, would play some of the same role.
15 But if I understand correctly, it would communicate through
16 Ministers would be making the announcement.

17 Again, it's not up to me to present the
18 details, but I am aware of this dynamic and I had the same
19 expectations as if there would be an announcement during a
20 partial election, that I would be informed or, if I had to
21 make an announcement, I would inform the -- through the
22 coordination committee, I would inform our partners. No one
23 is trying to surprise each other.

24 **MR. JEAN-PHILIPPE MacKAY:** The Deputy
25 Ministers that you've -- Mr. Perrault's mentioned is the
26 group responsible for DM CIR, and you'll have some witnesses
27 who will explain how this functions this committee of Deputy
28 Ministers.

1 Last topic I'd like to deal with you, Mr.
2 Perrault, okay, let's talk about cyber security.

3 Is it possible to show on the screen COM601,
4 French version. COM601.

5 Mr. Perrault, to situation you, it's an
6 update of 2023 by the CSE.

7 **THE REGISTRAR:** Could you repeat this?

8 **MR. JEAN-PHILIPPE MacKAY:** COM601.

9 **THE REGISTRAR:** This document is not in our
10 database.

11 **MR. JEAN-PHILIPPE MacKAY:** Well, I don't want
12 to take too much time, but Mr. Perrault, in this document
13 they mention that there's been a worldwide increase in cyber
14 threats against democratic institutions and the electoral
15 processes.

16 And in this context, you mentioned during an
17 interview -- during both interviews that Elections Canada has
18 taken some measures in the past few years to strengthen cyber
19 security. I'd simply like to hear you briefly on Elections
20 Canada's response to the increasing cyber threats. How do
21 you proceed to protect your infrastructures?

22 **MR. STÉPHANE PERRAULT:** As I shared earlier,
23 we have a strengthened relationship with what become the
24 Canadian Centre of Cyber Security, but which is a
25 subcomponent of CSE as of 2017. We are aware of the
26 increased threat through this relationship and through these
27 reports.

28 We favourably welcome all the reports that

1 the Canadian Centre gives us, especially in terms of
2 surveillance of our infrastructures. Each apparatus at
3 Elections Canada, a tablet, a computer, a cell phone is
4 continuously under surveillance by the Canadian Cyber
5 Security Centre.

6 Now, no one is protected against cyber
7 attacks, but we're alert to it and we take into account in
8 all our activities involving technological infrastructures,
9 practically all of our activity. We have 100 systems
10 involved in the federal elections, so we're quite aware of
11 that.

12 We also reach out campaigns with our
13 employees, especially through about phishing expeditions. We
14 want our staff to be aware of this and we train them, and we
15 also train the returning officers. We also want to make them
16 aware of these situations during the elections.

17 So we've increased our reach-out activities,
18 and we also -- our surveillance of our infrastructures in
19 cooperation with the Canadian Cyber Security Centre.

20 **MR. JEAN-PHILIPPE MacKAY:** I'll stop here,
21 Madam Commissioner. I'll give the floor to my colleague.

22 **COMMISSIONER HOGUE:** Thank you.

23 Counsel Sheppard?

24 **--- EXAMINATION IN-CHIEF BY MR. DANIEL SHEPPARD:**

25 **MR. DANIEL SHEPPARD:** For the record, it's
26 Daniel Sheppard, Commission counsel.

27 Mr. Perrault, I'd like to move to a new area,
28 and that's the regulation of political finance.

1 So when you testified before the Commission
2 back in March, you noted the fact that the *Canada Elections*
3 Act contains rules about how different entities collect,
4 expend, and report expenditures related to the electoral
5 process, and that conversation took place kind of in the
6 specific context of nomination contests.

7 Today I'm going to talk to you a little more
8 generally about those rules, but before I kind of get into
9 the substance of it, maybe I can just invite you to explain
10 why it is that we have political finance rules within our
11 electoral system.

12 **MR. STÉPHANE PERRAULT:** So generally
13 speaking, the *Elections Act* seeks to establish a level
14 playing field among -- or rather level the playing field
15 amongst electoral competitors and seeks to prevent the undue
16 influence of money. And it does that through a number of
17 mechanisms including transparency rules; contribution limits,
18 which have evolved over the years; spending limits for
19 entities that participate in the electoral process, meaning
20 candidates, parties, and third parties; and in recent years
21 has expanded third-party rules to include pre-writ
22 expenditures.

23 **MR. DANIEL SHEPPARD:** Okay. And I think
24 you've quite helpfully set out some of the details of the
25 system in your supplementary institutional report, and so I'm
26 not going to pull that up, people can make reference to that.

27 Today I'm going to focus more specifically on
28 contributions so the question of who is allowed to give money

1 and who's allowed to kind of accept that money and then kind
2 of expend it on certain regulated activities.

3 Before I get into those rules, I think it's
4 going to be helpful for us to understand who it is we're
5 talking about when it comes to regulated entities. So who
6 are the subjects of these rules in the first place. So can
7 you just indicate who it is that we're regulating with these
8 rules?

9 **MR. STÉPHANE PERRAULT:** Sure, and there's an
10 important distinction. There are, on the one hand, third
11 parties, which are subject to slightly different rules, and
12 then there's the rest of the entities, namely nomination
13 contestants, candidates, leadership contestants, parties, and
14 electoral district associations. And they are subject to a
15 more, I would say, consistent or coherent set of rules
16 regarding contributions.

17 **MR. DANIEL SHEPPARD:** Okay. So let's start
18 with the easy stuff. Let's put third parties aside for a
19 moment, although I'll be bringing us back to that topic and
20 we'll talk about the "Everyone else" that has kind of these
21 more consistent rules.

22 When it comes to all of those other groups,
23 who's allowed to make a contribution to those entities?

24 **MR. STÉPHANE PERRAULT:** So only individuals
25 who are either Canadian citizens or permanent residents can
26 make a contribution to any of those entities.

27 **MR. DANIEL SHEPPARD:** Could the Court
28 Operator pull up CAN4599?

1 And this was a document that Mr. MacKay had
2 taken to you a few minutes ago, the SITE briefing to the
3 Deputy Minister ESCC.

4 And if we could scroll down to page 3,
5 please? Under the heading, "Money, and the first word there
6 is "HASA," which I believe stands for hostile activities by
7 state actors, and what this says is:

8 "HASA also channeled monetary
9 donations and other assistance to
10 preferred candidates in elections
11 with the intent of fostering a bond
12 of obligation to the foreign state
13 and/or its proxies. This is usually
14 done via trusted interlocutors such
15 as proxy agents or co-opted community
16 organizations." (As read)

17 I'm not going to talk to you about this
18 briefing in particular, but I take it this sort of
19 information has been conveyed to you in the past via the
20 security and the intelligence community as a foreign
21 interference activity that may take place in Canada.

22 **MR. STÉPHANE PERRAULT:** I am aware of that
23 risk, certainly.

24 **MR. DANIEL SHEPPARD:** Is what is described in
25 this document permitted under the political finance rules?

26 **MR. STÉPHANE PERRAULT:** It is not.

27 **MR. DANIEL SHEPPARD:** Okay. What makes it
28 not permitted?

1 **MR. STÉPHANE PERRAULT:** Well, there's a
2 number of things, but contributions must be made out of a
3 person's own funds. So one person cannot accept money to
4 pass it on to a regulated political entities. In French we
5 call that "les contributions dirigés", but that is unlawful
6 under the Act. So that's certainly one thing. And of
7 course, foreign states and foreigners cannot make
8 contributions, directly or indirectly, to political entities.

9 **MR. DANIEL SHEPPARD:** And am I right that
10 there's also kind of a general anticircumvention rule that
11 says you're not allowed to structure transactions in a way
12 that seeks to evade the basic rules of the regime?

13 **MR. STÉPHANE PERRAULT:** Correct. So no
14 system can be perfectly airtight, and I can expand on that.
15 But this is the regime, these are the rules that govern it.

16 **MR. DANIEL SHEPPARD:** Okay. And we may get
17 to some of the issues that may exist in the regime.

18 So while this type of activity is not
19 permitted, there is at least some reporting, at least by the
20 SITE Task Force, that this is a strategy that foreign actors
21 may engage in. Which I think takes us away from the rules
22 and to the question of, kind of in practice how are those
23 rules implemented?

24 And I think we can take this document down.

25 So can you explain what are some of the
26 things that players within the political finance realm are
27 expected to do in order to ensure compliance with a rule that
28 says only a citizen, or a permanent residence may make a

1 contribution?

2 **MR. STÉPHANE PERRAULT:** So maybe I should
3 start by dividing the ways in which money can flow and the
4 scenarios that are alluded to in this document.

5 In any system money can flow out, what we
6 call outside the regime. It is not lawful to make
7 contributions in cash in excess of \$20. It doesn't mean it
8 doesn't happen. The fact that we have low spending limits,
9 however, makes it difficult to spend large amounts of money
10 in electoral competitions without being noticed by
11 competitors. So it's not saying it's not possible, it
12 certainly is, but there is a limitation that comes with the
13 existence of a spending limit.

14 If someone were to want to funnel that money
15 through the regime so that it finds its way into the campaign
16 account, it would have to go to use proxies; essentially, use
17 persons to bring that money, who have the ability to make
18 contributions.

19 We have low contribution limits. In Canada
20 they are, right now, set at \$1,725 annually. And that is a
21 total sum of the contributions can be made to the candidates
22 and the local district associations within a political party
23 or within a family. There's a small amount of contribution,
24 and in fact, on average contributions tend to be around \$200.
25 So if one were to try to fragment contributions and find
26 people to funnel that money, they would have to find a very
27 large number of willing partners to do that. So just kind of
28 put that in context, so I'm not saying it's impossible, but

1 it is difficult, and it's difficult not to be seen doing that
2 in any large kind of way.

3 The Political Financing Unit receives returns
4 and audits them on their face. It doesn't do an
5 investigation, but it does what we call horizontal audits.

6 So it looks at contributions across a
7 political family to make sure that people who do bring money
8 have not over contributed, in excess of the annual limits.
9 We also publish the names of every person who contributes
10 more than \$200 in a given year. So that is visible to the
11 general public. People who contribute can be seen. We do
12 not have information that would allow us to vet whether all
13 of these contributors are either Canadian citizens or
14 permanent residents. That's not information that we possess.
15 But by publishing the information, the logic of the system is
16 to make it available to the -- in full daylight, so that if
17 there are situations of unlawful contribution, they can be
18 possibly identified by other ---

19 **MR. DANIEL SHEPPARD:** And that's some of the
20 things that Elections Canada is able to do to kind of
21 implement that rule. Moving to the regulated entities
22 themselves, are they under an obligation to inform a
23 potential donor that they have to be a citizen or a permanent
24 resident?

25 **MR. STÉPHANE PERRAULT:** We encourage them to
26 do so, and I'm aware that they do so as a matter of good
27 practice. They have only a legal obligation to return
28 contributions once they are made aware that it is unlawful,

1 either because it exceeds the limit or it comes from an
2 unallowed source, but they have no legal obligation to
3 ascertain the source of the contribution as being a valid
4 source.

5 **MR. DANIEL SHEPPARD:** And so I take it then
6 that if they don't have a duty to ascertain that it's from a
7 lawful source they would not, for example, be under an
8 obligation to require a donor to provide proof of citizenship
9 or permanent residency?

10 **MR. STÉPHANE PERRAULT:** Correct. I'm aware
11 that many have a checkbox when they make their contributions
12 and go through that step. I think that's valuable, but there
13 is no documentary evidence that's required.

14 **MR. DANIEL SHEPPARD:** Right. And I think you
15 referred a -- to essentially a trust-based system whereby you
16 ask the question, but you trust that the answer that you're
17 receiving from the donor is truthful and accurate?

18 **MR. STÉPHANE PERRAULT:** Correct.

19 **MR. DANIEL SHEPPARD:** Okay. Let's move on
20 and talk about third parties, the one that you've said have
21 different rules. Before we talk about those rules, can you
22 give a basic definition of what is a third party?

23 **MR. STÉPHANE PERRAULT:** So there are
24 technical differences between the pre-writ and the writ
25 period, but, generally speaking, a third party is any entity
26 other than a registered party, or a candidate, or a district
27 association. That's generally speaking the scope of what
28 we're covering there. So it's anybody, foreign or domestic,

1 individual or group, corporation or otherwise, not being one
2 of those three.

3 MR. DANIEL SHEPPARD: Okay. And as I
4 understand it, there's limits on expenditures for regulated
5 activities during pre-election period when there's a ---

6 MR. STÉPHANE PERRAULT: Correct.

7 MR. DANIEL SHEPPARD: --- fixed date election
8 and then during the election period itself, from the writ to
9 the election for certain types of activities like certain
10 forms of advertising or partisan activities. Is that a
11 general description of ---

12 MR. STÉPHANE PERRAULT: That is kind of ---

13 MR. DANIEL SHEPPARD: --- some of the rules?

14 MR. STÉPHANE PERRAULT: Yes, we can get into
15 the nitty-gritty of the details, but, yes, and those
16 categories of expenses have been expanded in Bill C-76. They
17 used to include only election advertising during the election
18 period. Now they include partisan activities and surveys and
19 partisan advertising in the pre-writ period.

20 MR. DANIEL SHEPPARD: Okay. And so if we're
21 talking about contributions that are being made to fund these
22 types of regulated activities and the scope of those
23 activities have changed over time, are third parties limited
24 to using funds from citizens or permanent residents in order
25 to engage in those activities?

26 MR. STÉPHANE PERRAULT: So they cannot use
27 funds from foreign sources. They can use contributions from
28 individuals, or groups, or entities that are not foreign

1 entities, so it's not limited to Canadian citizens and
2 permanent residents in the sense that you could have
3 corporate money, or unions, or association's money, and they
4 can also use their own funds for that purpose.

5 **MR. DANIEL SHEPPARD:** Okay. And it's
6 probably obvious, but just to make the point explicit, when
7 you're talking about foreign sources, that will include
8 entities like foreign governments or foreign political
9 parties?

10 **MR. STÉPHANE PERRAULT:** Right. Or entities
11 that have no activities in Canada.

12 **MR. DANIEL SHEPPARD:** And then we've also
13 kind of briefly touched on the fact that there is certain
14 reporting requirements and that third parties are required to
15 disclose to Elections Canada information about contributions
16 they receive and expenditures they make, and that information
17 is made public by Elections Canada once certain thresholds
18 are passed; is that right?

19 **MR. STÉPHANE PERRAULT:** Correct. That is
20 correct.

21 **MR. DANIEL SHEPPARD:** In the course of your
22 discussions with the Commission, you identified a number of
23 issues that exist in terms of transparency when it comes to
24 contributions and expenditures from third parties, and I'd
25 like to talk to you about some of them. I think they're
26 closely related, but I'm going to try to break them up into
27 three kind of categories. The first is one that you've
28 already mentioned, and that's a third party relying on their

1 own funds when it comes to reporting their expenditures.

2 **MR. STÉPHANE PERRAULT:** Right.

3 **MR. DANIEL SHEPPARD:** Can you just explain
4 what that is and what sort of transparency issues you view
5 that to give rise to?

6 **MR. STÉPHANE PERRAULT:** Sure. I mean, that
7 is an area of concern. We've seen over the last few
8 electoral cycles the percentage of third-party expenditures
9 that are funded, or their contributions that are of their own
10 funds go from 8 per cent I think it's close to 40 per cent
11 now. So increasingly, we see third parties relying on their
12 own funds. And that may include money they've amassed over
13 the years from different sources. It should not be money
14 received for the specific purpose of regulated activities
15 under the Act, but it can be money received from General
16 purposes. It can include commercial revenue or donations and
17 can include in the mix donations from foreign sources. At
18 some point in time, this is all fungible money and it's their
19 own assets, it's their own funds. And so when they use that
20 money, they are using their own funds, and in this way, a
21 certain amount of illegal funding could find its way in third
22 party's expenditures during an election or a pre-writ
23 campaign.

24 **MR. DANIEL SHEPPARD:** And so when they report
25 the use of their own funds, the reporting doesn't kind of go
26 beyond that and provide any indication of the ultimate source
27 of that money?

28 **MR. STÉPHANE PERRAULT:** Correct, and that's

1 why -- and probably get into that, made recommendations to
2 that effect.

3 **MR. DANIEL SHEPPARD:** We -- you've predicted
4 kind of my next area of questioning, but let's talk about
5 some of the other related transparency issues. And the next
6 one is kind of an extension of the own funds issue you've
7 identified, and it's when entities do receive funds from a
8 variety of sources. And I'd like you to imagine an entity
9 that is receiving funds from sources, some domestic, but
10 also, some international, and we can imagine potentially from
11 a foreign government or political party.

12 **MR. STÉPHANE PERRAULT:** Right.

13 **MR. DANIEL SHEPPARD:** And they receive these
14 funds from various sources outside of the election period,
15 they amass it, an election is called, and they now begin to
16 make expenditures on regulated activities and report it as
17 the use of their own funds. Is the political finance regime
18 kind of equipped to trace out and identify a foreign source
19 of funds in that type of scenario?

20 **MR. STÉPHANE PERRAULT:** So there are two
21 scenarios. One is -- which is this one, and the answer, of
22 course, is no, unless they are essentially funded from
23 foreign sources, as long as they have some domestic sources
24 as well. It cannot assign dollar figures to particular
25 categories of expenditures, one for their rent or hydro bill
26 and one for their election campaign activity. So it's all
27 fungible. It is possible that, indirectly, groups may be
28 using foreign funds to support their activities, including

1 campaigning. So that's one area.

2 Another area is third party A receives money
3 from a range of groups, including group B, and reports as
4 money from group B. Group B is a Canadian group, but we
5 don't know where group B gets its funding. So there's a
6 limited degree of transparency. It does not reach all the
7 way down to individual contributors as citizens or permanent
8 residents. So there is a limited amount of transparency in
9 the regime as it exists today.

10 **MR. DANIEL SHEPPARD:** And so the hypothetical
11 I gave was kind of an intermixing of funds from different
12 sources. And it sounds like what you're describing in
13 addition to that is a chain of contributions ---

14 **MR. STÉPHANE PERRAULT:** Correct.

15 **MR. DANIEL SHEPPARD:** --- whereby
16 contributions flow from one entity to another entity to
17 another entity, and you can only trace back the source of
18 those funds really one step to who gave it to the ultimate
19 spender; is that fair?

20 **MR. STÉPHANE PERRAULT:** That's correct. And
21 so both scenarios are, in my view, problematic.

22 **MR. DANIEL SHEPPARD:** And going back, then,
23 to the scenario that was described in that SITE briefing --
24 and we can pull it up if you'd like, but just kind of
25 thinking about this foreign interference threat that's been
26 identified by the security and intelligence community, do you
27 view these types of transparency issues we've just been
28 talking about as raising kind of problems or concerns with

1 respect to foreign interference of a financial nature in the
2 Canadian electoral process?

3 **MR. STÉPHANE PERRAULT:** Certainly. But I
4 would say there's a greater degree of concern for third
5 parties because of the different rules that are at play.

6 **MR. DANIEL SHEPPARD:** So you've made
7 reference to the fact that you've made some recommendations
8 in this area.

9 If the Court Operator could please pull up
10 ELC54.

11 **--- EXHIBIT No. ELC0000054:**

12 Meeting New Challenges -
13 Recommendations from the Chief
14 Electoral Officer of Canada following
15 the 43rd and 44th General Elections

16 **MR. DANIEL SHEPPARD:** And while that's coming
17 up, Mr. Perrault, I take it that it's actually part of your
18 formal mandate as Chief Electoral Officer to make
19 recommendations to Parliament about reforms to our electoral
20 laws. Is that ---

21 **MR. STÉPHANE PERRAULT:** It is. It's provided
22 for in the Act and this report that you see is a report that
23 I made after the last two General Elections.

24 Normally we tend to see one after each GE.
25 The time span between the last two was very short and it was
26 the pandemic, so there was none between the two.

27 **MR. DANIEL SHEPPARD:** Okay. And if we could
28 scroll to page 20. And kind of starting in this area, you're

1 discussing some of the issues with respect to third parties.
2 Right here there's a registration threshold, but if we go
3 further down, I think you discuss in your report some of the
4 concerns about transparency.

5 And so if we can kind of scroll down and
6 there, third party contributions, I think, is where the
7 discussion begins.

8 And if we continue to go down to page 22, we
9 see there Recommendation 2.3.1. You've provided a
10 recommendation in terms of some potential reforms to how the
11 contribution rules for third parties ought to operate.

12 Can you just explain to the Commissioner what
13 your recommendation has been in this area?

14 **MR. STÉPHANE PERRAULT:** So in a nutshell,
15 that the ability to use one's own funds would be limited to
16 those entities that are either individuals, Canadian citizen
17 or permanent resident, or groups that are not what I call
18 fundraising entities, that is, groups that we see no more
19 than 10 percent. And the threshold is somewhat arbitrary,
20 but groups that do not significantly rely on contributions as
21 part of their revenues on an annual basis.

22 So only those entities would be allowed to
23 use their own funds. Other entities would have to
24 exclusively rely on contributions received by individuals
25 that are Canadian citizens or permanent residents that are
26 placed in a bank account, as is the case now, and used for
27 their regulated expenditures.

28 **MR. DANIEL SHEPPARD:** So the recommendation

1 is that for many third parties, essentially make the rules
2 similar to or the same as the earlier rules we discussed for
3 all of the other regulated entities.

4 **MR. STÉPHANE PERRAULT:** Correct. Correct.

5 **MR. DANIEL SHEPPARD:** And maybe just for a
6 point of clarity, are you able to give an example of a type
7 of third party that would exist in that exception for the
8 non-fundraising type of entities?

9 **MR. STÉPHANE PERRAULT:** A commercial entity
10 that has, you know, commercial revenue -- a union would
11 receive union dues -- but do not rely on donations.

12 **MR. DANIEL SHEPPARD:** In response to a
13 question that Mr. McKay asked you, you made reference to Bill
14 C-65. I take it that's a statute you're -- or rather, a Bill
15 that you're familiar with?

16 **MR. STÉPHANE PERRAULT:** Somewhat, yes.

17 **MR. DANIEL SHEPPARD:** Yes.

18 This is a statute that implements at least
19 some of the recommendations that have been made in this
20 report.

21 **MR. STÉPHANE PERRAULT:** That is correct.

22 **MR. DANIEL SHEPPARD:** And in particular, does
23 Bill C-65 reflect this recommendation that you've made?

24 **MR. STÉPHANE PERRAULT:** It does.

25 **MR. DANIEL SHEPPARD:** So once again thinking
26 about this in terms of foreign interference threats in
27 particular, do you think that these proposed changes would go
28 some distance to addressing some of the issues that have been

1 identified in terms of the use of contributions within the
2 electoral system as a form of foreign interference?

3 **MR. STÉPHANE PERRAULT:** I believe that they
4 would. I believe they serve a broader purpose in terms of
5 transparency, but certainly they include protection against
6 the introduction of foreign funds in the regulated activities
7 of third parties.

8 **MR. DANIEL SHEPPARD:** But as well, a point
9 you've also made earlier in your testimony is that, of
10 course, there are the rules but there are people who seek to
11 avoid the application of the rules.

12 I take it you'd agree that this
13 recommendation or Bill-65 would not be a perfect solution,
14 that one could still evade the rules by using proxies or
15 other means to obscure financial transactions.

16 **MR. STÉPHANE PERRAULT:** It is always
17 possible. As I said earlier, though, the Canadian system
18 has, relatively speaking, when you compare around the world,
19 very little money involved in our political system. I think
20 that's a virtue, not a fault. And it does reduce the ability
21 of that free-flowing of illicit funding. It does not
22 eliminate it.

23 **MR. DANIEL SHEPPARD:** So those are all of the
24 questions I'd like to ask specifically about political
25 finance, but I am going to stick with the topic of some of
26 the recommendations that you've made in this document and
27 Bill C-65.

28 And I'd like to focus on two recommendations

1 that you've made. I think you've discussed a number of them
2 in your interview summary, and if participants would like to
3 ask you questions about that, I'm sure they will.

4 The first area of recommendations that I'd
5 like to talk to you about has to do with platform
6 transparency, so a fairly different topic.

7 Could we go to page 29 of this document?

8 And this is a section of your report in which
9 you're discussing the role of online platforms and what they
10 do and the influence they have in the information environment
11 surrounding elections.

12 And if we scroll down to page 30, you make
13 two particular recommendations with respect to transparency.

14 Could you just describe what those
15 recommendations are and what your thinking was behind making
16 them?

17 **MR. STÉPHANE PERRAULT:** So essentially, it's
18 to increase the accountability of platforms regarding how
19 they deal with information, including in the first case how
20 they deal with paid electoral communications, but also how
21 they deal with misinformation specifically around ways to
22 vote early, the electoral process.

23 So right now, there is no transparency. Some
24 platforms may disclose their policies. They can change their
25 policies. In many cases, we don't know exactly what those
26 policies are, so it's very difficult for Canadians to
27 understand or hold the platforms at least morally accountable
28 for how they deal with disinformation and campaign activities

1 during the writ period.

2 **MR. DANIEL SHEPPARD:** And so I take it just
3 in terms of how this would operate -- and I'll use Facebook
4 as just one example, but it could be any number of entities.

5 Under this recommendation, they would be
6 required to publish and make available to the general public
7 whatever their policy happens to be in dealing with these two
8 areas you've identified.

9 **MR. STÉPHANE PERRAULT:** Correct. So it is,
10 in that regard, a modest proposal. It calls for more
11 transparency. It does not set specific standards in that
12 respect.

13 **MR. DANIEL SHEPPARD:** And that's my next
14 question because certainly there have been calls in some
15 quarters for kind of baseline legislated standards, not just
16 saying "Tell us what you're going to do", but a requirement
17 to adhere to certain basic threshold rules.

18 I wonder why you chose to make this more
19 modest proposal and not to propose any type of kind of
20 substantive regulation in this area.

21 **MR. STÉPHANE PERRAULT:** This is, first of
22 all, a beginning. I think it's important to start with
23 transparency. I'm not necessarily opposed to minimal
24 standards. However, I think we have to be careful when we
25 get into prescribing content rules and asking for takedowns.

26 I think there's a risk of backlash. I think
27 there is a universe out there of people who are very
28 sensitive to the issue of state censorship, and that feeds

1 narratives that are -- tend to be hostile to the whole
2 electoral process.

3 So in our case, we've not asked platforms to
4 take down information. We respond with correct information.
5 And in this case, I've not -- I've chosen not to impose or
6 recommend imposing content requirements, but rather, start
7 with the transparency.

8 **MR. DANIEL SHEPPARD:** And then moving from
9 your recommendations to Bill C-65, are these recommendations
10 reflected in that Bill?

11 **MR. STÉPHANE PERRAULT:** They are not.

12 **MR. DANIEL SHEPPARD:** They are not. The
13 other recommendation that I wanted to discuss with you has to
14 do with false statements respecting the electoral process.
15 And so if the Court Operator could please scroll up to page
16 25? And in this section of your report, you note that
17 there's no specific prohibition in the *Canada Elections Act*
18 against making false statements about the electoral process
19 itself. Why is that a concern for you?

20 **MR. STÉPHANE PERRAULT:** So there are specific
21 -- there are provisions, for example, on obstructing the vote
22 and preventing from voting. And we've relied on that in the
23 past. We -- the Commissioner has relied on that in the past
24 for certain prosecutions. But there is no general
25 prohibition that would catch a broader range of scenarios
26 that do not necessarily prevent people from voting or are not
27 necessarily aimed at preventing people from voting, but
28 rather, aimed at undermining the voting process, and in

1 particular, in undermining trust in the process and trust in
2 the results. That is in no way captured by the current
3 rules. And that is something that could be leveraged by
4 nefarious actors, including foreign state actors.

5 **MR. DANIEL SHEPPARD:** And so could you then
6 describe kind of the structure of the provision that you've
7 recommended should be enacted to kind of address that gap?

8 **MR. STÉPHANE PERRAULT:** So my recommendation
9 is for a fairly high standard or strict requirement, which
10 calls for a dual *mens rea* element, if I can use the legal
11 aspect, dual mental element. One is the fact that the person
12 would have to know that the information that they are
13 publishing or disseminating is false. Certainly, there is no
14 intent to capture people who share information that they
15 believe to be true, and, in fact, we should be open to those
16 conversations. But if the person knows the person -- that
17 the information to be false, and that's a second requirement,
18 publishes the information in order to undermine trust in the
19 electoral process, or undermine trust in the results, then I
20 believe that there is a very strong case for the prohibition
21 of this kind of content.

22 **MR. DANIEL SHEPPARD:** So let's talk about
23 that mental element a little bit more. The Commission has
24 certainly heard quite a lot of evidence about the challenge
25 of misinformation and disinformation, and tomorrow we'll be
26 hearing a fair bit more about that topic. Why not simply
27 prohibit knowingly false statements about the electoral
28 process itself? Why add an additional mental element?

1 **MR. STÉPHANE PERRAULT:** Well, I think there
2 are a number of circumstances where a person -- expanding
3 here, outside of the electoral process, but there are
4 different reasons why people may lie or exaggerate, and the
5 line between lying and exaggerating may be a blurry one. And
6 so I think it has to be clear that the person knows beyond a
7 reasonable doubt that this information is false.

8 **MR. DANIEL SHEPPARD:** Okay. And in addition,
9 your proposal requires them to have kind of one of two
10 purposes.

11 **MR. STÉPHANE PERRAULT:** Correct.

12 **MR. DANIEL SHEPPARD:** One purpose is to
13 disrupt the conduct of the election, and the other purpose is
14 to undermine the legitimacy of the election or its results.
15 And if you go and you spend some time reading the *Canada*
16 *Elections Act*, as I know we all have, you'll see this
17 reference to disrupting the conduct of the election appear in
18 provisions that already exist, but the notion of undermining
19 the legitimacy of the election or of its results seems to be
20 a new type of concept that you're recommending be introduced.
21 And I wonder if you could just speak to why is it that you
22 felt it was important to cover not just disrupting the
23 election, but undermining confidence as well?

24 **MR. STÉPHANE PERRAULT:** I think it's an
25 essential element. There's already a number of, as you've
26 noted, offences regarding disrupting the conduct. And I
27 think the main area where we're lagging -- lacking is on that
28 second component of undermining trust in the process or the

1 results. We do see narratives of this nature and we see them
2 internationally in different jurisdictions. And I think
3 there are a concern to the health of our democracy and even
4 the stability of government. So the extent that various
5 actors including foreign state actors could leverage
6 misinformation tools to push our narratives that undermine
7 trust in the outcome of the election, trust in the legitimacy
8 of the election or its results, that would be a significant
9 threat to our democracy, and I think it's important to
10 address that.

11 **MR. DANIEL SHEPPARD:** And in terms of Bill C-
12 65, does that Bill incorporate your recommendations in this
13 portion of your report?

14 **MR. STÉPHANE PERRAULT:** In part, but not to
15 the element that we've just discussed regarding undermining
16 trust in the electoral process or the results. That is not
17 included in Bill C-65.

18 **MR. DANIEL SHEPPARD:** So what is included is
19 a provision relating to knowingly false statements made about
20 the electoral process with the intent to disrupt the conduct
21 of the election, but it does not include those same knowingly
22 false statements made in order to undermine the legitimacy of
23 the election or its results?

24 **MR. STÉPHANE PERRAULT:** Not at this time, no.

25 **MR. DANIEL SHEPPARD:** Okay. Thank you. We
26 can take that document down.

27 So we've talked a little bit about
28 recommendations that you've made previously. I'd like to

1 move now to be a little bit more forward looking at
2 recommendations that may be to come. In your interview, you
3 made note of the fact that Elections Canada is in the process
4 of considering new or additional recommendations, which could
5 include changes to the rules relating to nomination contests
6 and leadership contests, as well as some other topics.
7 First, are those recommendations ready to be made public to
8 the Commission?

9 **MR. STÉPHANE PERRAULT:** They are not. We're
10 still working on that, and we're hearing from the
11 participants in the Commission and taking good note of what's
12 being discussed.

13 **MR. DANIEL SHEPPARD:** So this is an ongoing
14 process ---

15 **MR. STÉPHANE PERRAULT:** It is.

16 **MR. DANIEL SHEPPARD:** --- within Elections
17 Canada?

18 **MR. STÉPHANE PERRAULT:** Yes.

19 **MR. DANIEL SHEPPARD:** Am I right in hoping or
20 assuming that at some point those recommendations will be
21 made available to the Commission for the Commissioner's
22 consideration?

23 **MR. STÉPHANE PERRAULT:** It is certainly my
24 intention to make them available in time for the policy
25 discussions stage of the Commission's mandate and, of course,
26 I'll make them to Parliament as well, as per my mandate.

27 **MR. DANIEL SHEPPARD:** If we're not able to
28 get into very much of the substance of your deliberations in

1 this respect, could you talk about why it is that you've
2 engaged in this process? And in particular, what is it that
3 has caused you to start reflecting on the existing rules that
4 apply to nomination and leadership contests?

5 **MR. STÉPHANE PERRAULT:** I think the testimony
6 we've heard in this Commission and the work of the -- what's
7 referred to as the NSICOP Committee both have highlighted the
8 vulnerability of nomination contests in particular, but also,
9 leadership contest potential to cases of foreign
10 interference. I think the trust of Canadians has been shaken
11 in that regard. So both for the reason of better protecting
12 the processes, but also, reinforcing trust of Canadians, I
13 think it's important to consider what can be done.

14 **MR. DANIEL SHEPPARD:** And in thinking about
15 what can be done, one of the values you identified during
16 your interview as being important was party autonomy, and I
17 think you described it as an important value in our
18 democratic system. Can you expand on that and explain, first
19 of all, what you mean by party autonomy, and then why you
20 view it as an important value in our system.

21 **MR. STÉPHANE PERRAULT:** Certainly. I think
22 that's something you've heard from other witnesses and,
23 certainly, I've heard from parties in my discussions with
24 them, and I share, to a certain degree, their perspective in
25 the sense that the freedom of parties to determine how they
26 will determine, how they will decide who runs under their
27 banner, when those decisions take place, including the right
28 to decide not to accept as one of their candidates someone

1 who's been selected at the local level because that person
2 may have in the past done things or said things that do not
3 reflect the values of the party. This is really at the core
4 of political party's freedom, in my view, just as much as
5 deciding what their party platform is. So parties in Canada
6 have enjoyed and should continue to enjoy a certain degree of
7 latitude in deciding not only who runs for them, but what are
8 the circumstances that surround that decision, including to
9 disallow a person to be a candidate for their party.

10 **MR. DANIEL SHEPPARD:** I take it then this is
11 one of the values, though perhaps not the only one, that
12 you're taking into account as you consider possible reforms
13 to the system for nomination and leadership contests?

14 **MR. STÉPHANE PERRAULT:** That is correct. I
15 do believe that there are ways to look at reinforcing the
16 nomination and leadership contest rules without necessarily
17 taking away from parties the freedom that they enjoy and the
18 selection processes that they put in place.

19 **MR. DANIEL SHEPPARD:** One particular reform
20 proposal that has been discussed in public is to assign the
21 duty to kind of run nomination contests and leadership
22 contests to Elections Canada. That is a topic that you were
23 able to discuss in your interview with Commission counsel.
24 And I wonder if you'd just like to take this opportunity to
25 kind of express your views about whether that is an
26 appropriate role for Elections Canada to undertake?

27 **MR. STÉPHANE PERRAULT:** It's certainly not
28 one that is possible in the system that we have, and that's

1 the main point. Even accepting the freedom of parties inside
2 their rules, one could theoretically conceive a situation
3 where Elections Canada is called upon to administer whatever
4 rules the parties put in place.

5 We do not have fixed date elections in
6 Canada. We have byelections that come at any time in the
7 electoral cycle. We have general elections that, as we know,
8 can happen at any time in the electoral cycle.

9 There are nomination processes -- nomination
10 contests that take place across the country and the lead up
11 to the 43rd GE, we had, I believe, somewhere around 850 that
12 are known to us, they may not all be known to us, around 700
13 for the last general election.

14 The timing of these are unknown. The
15 duration of these are unknown to us. They may be a few hours
16 and a few weeks long, but that varies from party to party.

17 Elections Canada does not have a permanent
18 decentralized infrastructure to deal with that kind of
19 administration. In fact, even with a permanent
20 infrastructure, like Australia has, it would be extremely
21 difficult to conduct or oversee the nominations in the same
22 way that we oversee the elections themselves.

23 So I think in terms of administrating the
24 nomination contests, I do not see that as something that we
25 could do.

26 Again, it doesn't mean that the rules or the
27 safeguards around nomination and leadership contests cannot
28 be improved.

1 **MR. DANIEL SHEPPARD:** Well, Mr. Perrault, I
2 will await your eventual recommendations with interest, but
3 at this time, Madam Commissioner, those are all my questions.

4 **COMMISSIONER HOGUE:** Thank you, MR. Sheppard.
5 We'll take a 10-minute break before beginning
6 the cross-examination. So that means 4:45.

7 **THE REGISTRAR:** Order, please. À l'ordre,
8 s'il vous plait.

9 This hearing of the Commission is now in
10 recess until 4:45 p.m. Cette séance de la Commission est
11 maintenant suspendue jusqu'à 16 h 45.

12 --- Upon recessing at 4:34 p.m./

13 --- Upon resuming at 4:51 p.m.

14 **THE REGISTRAR:** Order, please. À l'ordre,
15 s'il vous plait.

16 This sitting of the Foreign Interference
17 Commission is now back in session. Cette séance de la
18 Commission sur l'ingérence étrangère est de retour en
19 session.

20 The time is 4:51 p.m. Il est 16 h 51.

21 **MR. DANIEL SHEPPARD:** Madam Commissioner,
22 it's Dan Sheppard for the Commission.

23 I know I said those were all of my questions.
24 During the break I realized I actually had forgotten to ask
25 one, and with your permission, if I could take another minute
26 of our time.

27 **COMMISSIONER HOGUE:** Go ahead.

28 --- MR. STÉPHANE PERRAULT, Resumed:

1 --- EXAMINATION IN-CHIEF BY MR. DANIEL SHEPPARD (cont'd):

2 **MR. DANIEL SHEPPARD:** If the Court Operator
3 could bring up WIT74.

4 And Mr. Perrault, this is just another one of
5 the Bill C-65 amendments that I just wanted to ask you a
6 question about.

7 If we can go to page 20 and look at -- down
8 under 8.4 "Undue Foreign Interference".

9 The undue foreign interference provision, as
10 I understand it, prohibits a number of foreign actors,
11 including political Parties, governments and entities like
12 that, from unduly influencing an electoral to vote or refrain
13 from voting or casting their ballot in certain ways. And
14 just so that we're all clear, there's a particular definition
15 of what constitutes "undue foreign influence".

16 Can you just explain what is "undue foreign
17 influence"?

18 **MR. STÉPHANE PERRAULT:** So "undue influence"
19 is -- make sure I'm not going to mess it up, but it's either
20 -- it's influencing electors to vote for a particular Party
21 or candidate or vote against through either spending money or
22 contravening any law of Canada. And that clause allows the
23 Commissioner of Canada Elections to gain access to -- creates
24 an extra-territorial dimension to the provision as well and
25 gives her a mandate to investigate that.

26 It does exclude a number of activities, and
27 perhaps this is what you're wanting me to get to. It does
28 exclude things that are merely the expression of like opinion

1 or media articles that are supportive or critical of a Party
2 or candidate.

3 **MR. DANIEL SHEPPARD:** Right. So I guess kind
4 of inherent in the notion of prohibiting undue foreign
5 influence is that there are forms of foreign influence that
6 are not prohibited ---

7 **MR. STÉPHANE PERRAULT:** Correct.

8 **MR. DANIEL SHEPPARD:** --- by the legislation,
9 and so you've kind of touched on those.

10 Could you give an example of kind of the sort
11 of thing that a foreign government or state might do to kind
12 of potentially induce an elector to vote in a particular way
13 that would not violate the undue influence provision?

14 **MR. STÉPHANE PERRAULT:** So again, if a state
15 actor merely expresses his or her personal opinion, then that
16 would not constitute undue influence. If media articles are
17 published and are connections to a state actor -- the BBC
18 comes to mind, but there are other examples -- this would not
19 constitute undue influence.

20 **MR. DANIEL SHEPPARD:** And then bringing you
21 forward to recommended changes, as this provision is
22 currently drafted, I understand it only applies during the
23 election period itself.

24 **MR. STÉPHANE PERRAULT:** That is correct.

25 **MR. DANIEL SHEPPARD:** And you've made a
26 recommendation to change that. Is that right?

27 **MR. STÉPHANE PERRAULT:** I have recommended
28 that it be expanded to the previous period, but, in fact, as

1 I sit here today, I think Bill C-65 is correct in expanding
2 it at all times. There's no reason to put a time limitation
3 on that.

4 **MR. DANIEL SHEPPARD:** So if Bill C-65 were
5 enacted as it's currently drafted, the undue foreign
6 influence -- the undue influence provision would prohibit the
7 conduct that we described earlier regardless of when it
8 occurs in respect of our elections.

9 **MR. STÉPHANE PERRAULT:** That is correct. But
10 it would not cover nomination or leadership contests. That's
11 a separate conversation.

12 **MR. DANIEL SHEPPARD:** I think I may have
13 taxed the indulgence I've been granted, so I won't go down
14 that path.

15 Madam Commissioner, I appreciate that
16 opportunity.

17 **COMMISSIONER HOGUE:** Thank you.

18 So the first one is the Concern Group.

19 **--- CROSS-EXAMINATION BY MR. NEIL CHANTLER:**

20 **MR. NEIL CHANTLER:** Good afternoon.

21 **MR. STÉPHANE PERRAULT:** Good afternoon.

22 **MR. NEIL CHANTLER:** I'm Neil Chantler,
23 counsel for the Chinese Canadian Concern Group.

24 Mr. Perrault, I'm going to start with a
25 question arising from your testimony earlier this afternoon.
26 And it's simply the rules are clear surrounding third-party
27 financing and the prohibition against receiving funds
28 contributed by a foreign entity; correct?

1 **MR. STÉPHANE PERRAULT:** Correct.

2 **MR. NEIL CHANTLER:** The problem seems to be
3 enforcement of those rules.

4 I'm just trying to get a sense of the scale
5 of this problem. Can you tell me whether such cases are ever
6 identified and investigated by Elections Canada?

7 **MR. STÉPHANE PERRAULT:** So if they were to be
8 -- just for clarity, if they were to be investigated, it
9 would be by the Commissioner of Canada Elections.

10 I do not recall a case we would have made a
11 referral for that specific prohibition, but I may be
12 incorrect in that regard.

13 **MR. NEIL CHANTLER:** And sorry, you do not
14 recall such case.

15 **MR. STÉPHANE PERRAULT:** I do not recall.

16 **MR. NEIL CHANTLER:** Thank you.

17 **MR. STÉPHANE PERRAULT:** It's important just
18 to keep in mind that the problem that I'm laying out here or
19 that I was trying to explain is that, as third parties use
20 their own funds, it's very difficult to parse out within
21 these funds what is foreign funding and what is domestic
22 funding.

23 **MR. NEIL CHANTLER:** My next questions are
24 about the data collection conducted by Elections Canada on
25 voter participation rates, particularly among diaspora
26 communities.

27 Elections Canada conducts surveys and
28 collects data on a population is calls "new Canadians";

1 correct?

2 **MR. STÉPHANE PERRAULT:** Correct.

3 **MR. NEIL CHANTLER:** And this category is
4 defined as people who have attained citizenship since the
5 last federal election, so they haven't voted in a federal
6 election before.

7 **MR. STÉPHANE PERRAULT:** Correct.

8 **MR. NEIL CHANTLER:** This category is not
9 limited to new Canadians who might identify with one of our
10 many diaspora communities. The category is much broader than
11 that.

12 **MR. STÉPHANE PERRAULT:** It is. There's
13 overlap, but it's much broader, yes.

14 **MR. NEIL CHANTLER:** And it does not capture
15 members of our diaspora communities that have been in Canada
16 for a long time.

17 **MR. STÉPHANE PERRAULT:** It does not.

18 **MR. NEIL CHANTLER:** Now, the Terms of
19 Reference of this Inquiry recognize that Canada's diaspora
20 groups are among the most vulnerable to foreign interference.
21 You're familiar with that.

22 **MR. STÉPHANE PERRAULT:** I am.

23 **MR. NEIL CHANTLER:** And it's clear from your
24 testimony today that Elections Canada sees education and
25 outreach to Canada's diaspora communities as an important
26 part of its mandate.

27 **MR. STÉPHANE PERRAULT:** Yes.

28 **MR. NEIL CHANTLER:** This includes educating

1 diaspora members on the voting process, the secret vote,
2 methods of voting and so on; correct?

3 **MR. STÉPHANE PERRAULT:** Yes.

4 **MR. NEIL CHANTLER:** And obviously, that has
5 value in its own right, but it's also your response, I
6 believe, in your evidence to foreign interference itself.
7 People need to know where to vote in any event, but it's
8 especially important in the context of foreign interference
9 to assure people the system is sound; correct?

10 **MR. STÉPHANE PERRAULT:** Absolutely.

11 **MR. NEIL CHANTLER:** And this is to combat the
12 harmful effects of mis and disinformation that are sometimes
13 spread about the voting system; correct?

14 **MR. STÉPHANE PERRAULT:** I agree.

15 **MR. NEIL CHANTLER:** And it's also a way to
16 respond to intimidation of voters who may not vote because
17 they fear they may be -- it may be discovered by their home
18 country who they voted for.

19 **MR. STÉPHANE PERRAULT:** They may not
20 understand or appreciate the secrecy of the vote in Canada.

21 **MR. NEIL CHANTLER:** And this is why education
22 and outreach is so important.

23 **MR. STÉPHANE PERRAULT:** Agreed.

24 **MR. NEIL CHANTLER:** And at this point in
25 time, Elections Canada does not know the democratic
26 participation rates of members of different diaspora groups,
27 for example, such as Chinese Canadians, because it's not
28 measured. Is that right?

1 **MR. STÉPHANE PERRAULT:** Not at this point in
2 time, no.

3 **MR. NEIL CHANTLER:** And so you'd agree that
4 Elections Canada does not know if its education and outreach
5 efforts are having the desired effect of increasing
6 participation?

7 **MR. STÉPHANE PERRAULT:** I'd want to be very
8 careful here when we talk about participation rates. There
9 are so many factors that come into play when we talk about
10 participation. There's motivation, there are barriers, there
11 may be intimidation. It's very, very difficult. In fact, we
12 believe it's not possible to identify and isolate factors.
13 It doesn't mean that we should not evaluate the quality of
14 our products and find ways to evaluate whether they are
15 useful to the communities, but participation may not be the
16 right measure for that.

17 **MR. NEIL CHANTLER:** We do know, based on
18 Elections Canada's own surveys, that new Canadians have a
19 lower turn out at elections compared to other Canadian
20 voters; correct?

21 **MR. STÉPHANE PERRAULT:** I believe that's the
22 case, yes.

23 **MR. NEIL CHANTLER:** And of course, perhaps
24 stating the obvious, but the outcome of low participation
25 among a particular group of Canadians is that group of
26 Canadians' interests are underrepresented in our House of
27 Commons?

28 **MR. STÉPHANE PERRAULT:** That is the case.

1 **MR. NEIL CHANTLER:** And this is a problem
2 that we should certainly be striving to fix?

3 **MR. STÉPHANE PERRAULT:** Just to be clear,
4 Elections Canada's concern is with addressing barriers. It
5 is not about stimulating participation. It's a sensitive
6 area because there are political dynamics involved in
7 stimulating or encouraging participation. We want to make
8 sure that Canadians who want to participate have the
9 information and do not face undue barriers. And that
10 includes understanding the protections that they have or the
11 options that they have for voting in a federal election. So
12 that's why we're focusing our efforts there.

13 **MR. NEIL CHANTLER:** Many of the types of
14 hostile actions by foreign states that we've identified
15 discussed in this Inquiry that you've spoken to earlier today
16 would amount to those kinds of barriers; correct?

17 **MR. STÉPHANE PERRAULT:** Some do.

18 **MR. NEIL CHANTLER:** And so Elections Canada
19 has, within its mandate, the removal of those barriers?

20 **MR. STÉPHANE PERRAULT:** Correct.

21 **MR. NEIL CHANTLER:** Could the Court Operator
22 please call up ELC54? This is a document, Mr. Perrault,
23 called *Meeting New Challenges: Recommendations from the Chief*
24 *Electoral Officer of Canada Following the 43rd and 44th*
25 *General Elections*. I presume you're familiar with it?

26 **MR. STÉPHANE PERRAULT:** I am.

27 **MR. NEIL CHANTLER:** If we could please scroll
28 to page 61? The paragraph starting with, "Elections Canada

1 does not have..."

2 MR. STÉPHANE PERRAULT: Correct.

3 MR. NEIL CHANTLER: There it is. I'll read
4 it aloud.

5 "Elections Canada does not have a
6 clear legislative mandate to collect
7 demographic information about
8 electoral participants."

9 It goes on to explain why, or the consequence
10 of that, and then it says:

11 "Crucially, the lack of legislative
12 mandate also means that demographic
13 data about electoral participants is
14 not fully available to Parliament or
15 researchers."

16 Now, if we can scroll further down the page
17 to the recommendation that arises from this discussion,
18 9.4.1? And it says:

19 "To further progress toward a more
20 inclusive and representative
21 electoral system, a new legislative
22 mandate should be included in the Act
23 to allow Elections Canada to collect,
24 on a voluntary basis, and make
25 publicly available anonymized
26 demographic data about electoral
27 participants, including gender,
28 ethnic origin, age, Indigenous status

1 and disability."

2 I'm sure you'll agree with me that this type
3 of granular demographic data on electoral participants would
4 greatly assist Elections Canada in combating the harmful
5 effects of foreign interference on voter participation rates?

6 **MR. STÉPHANE PERRAULT:** It would certainly
7 help us get a better picture of those who participate,
8 including as candidates in the electoral process. It would
9 be on a voluntary basis though. We do not want to compel
10 people to disclose any information that they do not wish to
11 disclose.

12 **MR. NEIL CHANTLER:** No, but it would allow
13 you to not only tailor your responses and your education and
14 your outreach better, but it would allow you to see whether
15 those efforts were having any results?

16 **MR. STÉPHANE PERRAULT:** I would hope so, yes.

17 **MR. NEIL CHANTLER:** Thank you. Those are my
18 questions.

19 **MR. STÉPHANE PERRAULT:** Thank you.

20 **COMMISSIONER HOGUE:** Thank you.

21 So next one is RCDA.

22 **--- CROSS-EXAMINATION BY MR. GUILLAUME SIROIS:**

23 **MR. GUILLAUME SIROIS:** [No interpretation]
24 briefly hear you about the financial independence of
25 Elections Canada.

26 If a government is not satisfied with your
27 work, could they withdraw the funding for Elections Canada or
28 could they decide not to renew your funding?

1 **MR. STÉPHANE PERRAULT:** Oh, yes, in part, but
2 the government would need the approval of the House of
3 Commons. The House of Commons votes on the budget.

4 But Elections Canada has two sources of
5 funding, an annual appropriation which has to be voted every
6 year which could vary according to the will of
7 parliamentarians. It covers the salaries of staff members
8 with an indeterminate duration. We are talking about about
9 55 (sic) positions, so there is a dependency on the annual
10 budget.

11 Under the Act, there is a provision which is
12 found in virtually all provincial jurisdictions in Canada.
13 It's called the statutory authority. It's permanent
14 legislative authorities to start spending as I deem necessary
15 to prepare the elections. Of course, I am accountable. I
16 appear before the Senate to account for expenses, but I
17 decide on the scope and the time of the spending considering
18 that we don't know when the election will be called.

19 **MR. GUILLAUME SIROIS:** So is the second part
20 of the spending specific to an election, for example,
21 surveillance of social media?

22 **MR. STÉPHANE PERRAULT:** Yes, it is part of
23 our electoral preparation. And I use this provision to build
24 a team of social media surveillance so these things happen.
25 I have the ability to respond to set up a team, but I could
26 also make it permanent following the next election.

27 **MR. GUILLAUME SIROIS:** Thank you.

28 And why is it important to have this kind of

1 financial independence?

2 **MR. STÉPHANE PERRAULT:** Well, because of our
3 parliamentary system, we don't know the date of the election,
4 so it can change at any point. Also, to ensure some
5 independence. The choices that I make for which I am
6 accountable to parliamentarians, I make them without asking
7 for permission.

8 For example, the investment for information
9 campaigns for voters, they come under a statutory
10 authorization so I'm accountable for them, but I don't have
11 to ask for prior approval to the Parliament.

12 It is the same for the Commissioner here.
13 She has a statutory authority so she doesn't need a special
14 approval when she wants to start spending.

15 **MR. GUILLAUME SIROIS:** I would like to ask
16 you about indirect contributions. It's a more recent
17 phenomenon, online influencers. Let's say that we have an
18 influencer who is paid by a foreign state and who is
19 promoting a political Party or a political candidate. Would
20 that be considered as a contribution a political Party?

21 **MR. STÉPHANE PERRAULT:** There has to be an
22 agreement from an entity. If somebody puts up a signpost on
23 your lawn, then you are not deemed to have received a
24 contribution, but if you leave it for a while, then you are
25 deemed to have received it. It could come under the
26 provisions on undue influence.

27 It could also take the form of regulated
28 partisan activities, so there could be different angles to

1 review the situation.

2 **MR. GUILLAUME SIROIS:** I'm wondering whether
3 you're aware of the fact that some other branches of
4 government which are monitoring online speeches, are you
5 aware of that?

6 **MR. STÉPHANE PERRAULT:** I know that our
7 security partners have an interest in foreign actors'
8 speeches online, but you will have a chance to ask them your
9 questions.

10 Of course, Global Affairs has a group. We
11 call them the Rapid Response mechanism. It works with
12 international partners to understand what is being said in
13 the environment and still with a security angle, not with a
14 partisanship angle.

15 **MR. GUILLAUME SIROIS:** I wonder whether
16 Elections Canada considered to have a surveillance mandate
17 more from a political perspective considering that Elections
18 Canada has some independent that public servants may not
19 have, so it has more independence. So is that something that
20 Elections Canada has considered?

21 **MR. STÉPHANE PERRAULT:** It's a good question.
22 It's an important question, and I think I have to be very
23 clear. Elections Canada -- maybe this is not the answer that
24 you're seeking. Elections Canada should not have as a
25 mandate to monitor partisan speeches. I think it is
26 necessary to its independence that it should not be tasked
27 with determining the kind of speech that is being found. So
28 we're following the processes to inform Canadians about the

1 way that they can take part in the process.

2 Of course, I understand that it opens the
3 door to influence campaigns, and it's one of the great
4 challenges in our current society.

5 **MR. GUILLAUME SIROIS:** Well, there is
6 surveillance carried out by other government actors and also
7 by private actors, private companies which are under contract
8 with the government or non-profit organizations, so of
9 course, there are risks to political or partisan
10 surveillance.

11 So wouldn't it be better to have a totally
12 independent organization with this task?

13 **MR. STÉPHANE PERRAULT:** Well, there are
14 academic organizations which have an interest. There are
15 different lenses which can be carried out by various groups
16 on information. I think it's very healthy.

17 I don't think that a single lens could be
18 used, but I think that a Chief Electoral Officer should not
19 be just an arbiter of the political speeches.

20 **MR. GUILLAUME SIROIS:** Why?

21 **MR. STÉPHANE PERRAULT:** Well, because then
22 they would be taking sides. So I think that independence,
23 the impartiality of Elections Canada would be undermined.

24 **MR. GUILLAUME SIROIS:** In a context where
25 information is clearly false, it can be categorized as
26 information which does not impact the electoral processes.
27 So could this information eventually fall under the purview
28 of Elections Canada?

1 **MR. STÉPHANE PERRAULT:** I don't think so. Of
2 course, there are specific cases under section 91, lies about
3 the criminal record of a candidate, very specific cases that
4 would come under the mandate of the Commissioner. But such
5 offences have to be very specific when we're not talking
6 about the process.

7 **MR. GUILLAUME SIROIS:** Thank you. This
8 concludes my questions, Madam Commissioner.

9 **COMMISSIONER HOGUE:** Human Rights Coalition?

10 **(SHORT PAUSE/COURTE PAUSE)**

11 **MS. SARAH TEICH:** Good afternoon.
12 Can we please pull up WIT74? And scroll down
13 to paragraph 28. Thank you.

14 **--- CROSS-EXAMINATION BY MS. SARAH TEICH:**

15 **MS. SARAH TEICH:** Here you note that
16 Elections Canada does not ask CSIS to validate the community
17 organizations that EC works with. What work does Elections
18 Canada do with community organizations, and why?

19 **MR. STÉPHANE PERRAULT:** So we provide, to
20 anybody, in fact, but some organizations are part of a
21 network, and being part of the network they receive periodic
22 information bulletins and information about our activities.
23 But they are equipped with tools about -- that serve to
24 inform Canadians on how to participate, whether as an
25 elector, as a worker, or as a candidate.

26 So as I indicated earlier, we welcome anybody
27 to use those tools because they are vetted, proper
28 information that come from Elections Canada, and that's why

1 we are not concerned with the identity of -- the availability
2 of that tool is, in fact, not limited to that network.
3 Anybody can have access to them; they're on our website.

4 **MS. SARAH TEICH:** I see, okay.

5 Actually, that answers all of the questions I
6 was going to ask, so that will be the end of my questions.

7 **COMMISSIONER HOGUE:** Thank you.

8 Counsel for Erin O'Toole?

9 **MR. THOMAS JARMYN:** Thank you, Commissioner.

10 **--- CROSS-EXAMINATION BY MR. THOMAS JARMYN:**

11 **MR. THOMAS JARMYN:** Mr. Perrault, my name is
12 Tom Jarmyn, and I represent Erin O'Toole.

13 **COMMISSIONER HOGUE:** You're muted.

14 **MR. THOMAS JARMYN:** Oh.

15 **COMMISSIONER HOGUE:** Ah, okay.

16 **MR. THOMAS JARMYN:** Okay.

17 Mr. Perrault, my name is Tom Jarmyn, and I
18 represent ---

19 **MR. STÉPHANE PERRAULT:** Good afternoon.

20 **MR. THOMAS JARMYN:** --- I represent Erin
21 O'Toole.

22 If I could ask the reporter to bring up
23 WIT15?

24 **--- EXHIBIT No. WIT0000015.EN:**

25 Interview Summary: Leona Alleslev

26 **MR. THOMAS JARMYN:** And scroll down to the
27 bottom of page 1 and the top of page 3 [sic] where we're
28 looking at paragraph 3. So just a little bit further,

1 please. That's good, thank you.

2 This is the interview summary of a Leona
3 Alleslev, who was a member of Parliament and a candidate in
4 the Aurora riding. And she discusses some of the reports
5 that she'd heard about citizens who are -- were afraid to
6 vote.

7 Have you heard any reports similar to this
8 with respect to either the 2019 or 2021 elections?

9 **MR. STÉPHANE PERRAULT:** I have not, not
10 outside the work of this Commission. So this is something
11 that, of course, I'm aware of from herself, but I have not
12 received, for example, any intelligence to corroborate that
13 kind of information.

14 **MR. THOMAS JARMYN:** Okay. And Mr. Chiu
15 testified that he heard similar reports as well. Do you
16 recall that?

17 **MR. STÉPHANE PERRAULT:** I do. Again, these
18 are things that I've heard in the course of the work of the
19 Commission, and in part these are the piece of evidence that
20 have motivated my desire to increase awareness on protections
21 around the secrecy of the vote to reassure participants.

22 **MR. THOMAS JARMYN:** Mr. Chiu testified that,
23 in fact, what had been passed on to him was that voters were
24 afraid to even been seen as voting. So it's not -- it wasn't
25 secrecy of the ballot, it was the fact that they were even
26 showing up.

27 **MR. STÉPHANE PERRAULT:** Correct. There are
28 several ways to vote, and again, I alluded to that earlier.

1 Voters can vote in person at the polling stations where they
2 can be seen. They can vote by mail; they can vote at the RO
3 office. They can vote at another RO office. So in an urban
4 setting, they have the choice of neighbouring returning
5 offices across the city where they could go. So there are
6 different avenues for voters to participate, and I think it's
7 our role to make sure they understand these avenues, they
8 understand the secrecy of the vote, and then decide whether
9 or not to participate.

10 **MR. THOMAS JARMYN:** The specific allegation
11 of Ms. Alleslev is that agents of the Chinese Communist Party
12 were working in the local election office and in the polling
13 stations. And we don't know whether or not that's as an
14 employee of Elections Canada, or as a scrutineer from a
15 political party. What steps does Elections Canada take to
16 vet either its employees or to encourage parties from
17 inadvertently hiring agents of a foreign country?

18 **MR. STÉPHANE PERRAULT:** So we do conduct
19 security clearances for headquarters' employees, as well as
20 those who work in the offices of Returning Officers who deal
21 with Protected B information, so personal information, or who
22 have access to our IT systems.

23 It's important for everyone who is listening
24 or hearing the work of the Commission to understand that at
25 any given moment an election can be called, and within days
26 we must recruit and train roughly 230,000, 250,000 people.
27 So this system is not one in which we could conduct or even
28 ask security partners to conduct security clearances for

1 250,000 people within a matter of days.

2 So the protections around the voting process
3 lie elsewhere; they lie, as I said, in the various
4 opportunities to vote and the fact that the vote takes place
5 in public, in front of observers, and in the secrecy of the
6 ballot.

7 But the notion that we could screen 250,000
8 people in a number of days when we recruit all the way to the
9 weekend prior to polling day on Monday, is simply not an
10 option for us.

11 **MR. THOMAS JARMYN:** And so it's fair to say
12 that this risk is a structural necessity, not that has to be
13 managed?

14 **MR. STÉPHANE PERRAULT:** Correct. It's
15 inherent to our system.

16 **MR. THOMAS JARMYN:** Okay, thank you.

17 Mr. Sheppard asked a great deal of questions
18 about the third-party financing.

19 So if I could ask the Court Reporter to bring
20 up CAN11293?

21 **--- EXHIBIT No. CAN011293:**

22 China: Domination of Chinese-Language
23 Media in Canada Poses National
24 Security Threats - IM 30/2023

25 **MR. THOMAS JARMYN:** And this is a memorandum
26 from the Intelligence Assessment Secretariat, and I believe
27 the author, Mr. Green, will be testifying in about two weeks
28 from now. So I'd just like to scroll up a little bit so we

1 can see the entirety of the box entitled, "Key Judgment."
2 And if you look at the third bullet it says, "The CPC" --
3 that being the Communist Party of China:

4 "...controls narratives by limiting
5 opportunities for dissenting voices,
6 [redacted] by providing economic
7 incentives, [redacted] and fostering
8 censorship." (As read)

9 And then later on relates these efforts to
10 the ability to attempt to influence electoral outcomes.

11 Is it fair to say, first of all, that if
12 these activities occurred during the course of an election
13 period, they would offend the undue foreign influence
14 provisions of the Act?

15 **MR. STÉPHANE PERRAULT:** Not necessarily. So
16 as we discussed earlier, there are exceptions to the undue
17 influence clause in the *Canada Elections Act* that pertain to
18 media content; right? And that is one ---

19 **MR. THOMAS JARMYN:** Yes, but if they were --
20 if they were providing economic incentives, ---

21 **MR. STÉPHANE PERRAULT:** But that -- so
22 there's a range of conduct that you -- that this box refers
23 to. Yes. Yes, if they were providing economic incentives,
24 yes.

25 **MR. THOMAS JARMYN:** Yeah. And possibly also
26 the foreign contribution rules or the third-party
27 contribution rules as well?

28 **MR. STÉPHANE PERRAULT:** Possibly, yes.

1 **MR. THOMAS JARMYN:** Okay. And I'd like to go
2 down to paragraph 12 of this memo. Exactly. There.

3 And it says:

4 "The widespread use of WeChat
5 presents two enduring challenges."

6 (As read)

7 And then it talks about:

8 "More recently, opensource reporting
9 notes a coordinated disinformation
10 campaign aimed at WeChat dissuading
11 voters from supporting parliamentary
12 candidates with anti-China views in
13 2021." (As read)

14 It seems that the Communist Party of China is
15 employing -- using its own employees to attempt to do - -
16 carry out this behaviour on WeChat. This too would seem to
17 offend the undue foreign interference -- or foreign influence
18 provisions. Is that ---

19 **MR. STÉPHANE PERRAULT:** So I don't have the
20 facts behind this. As I noted earlier, there is an exception
21 for the media content. Whether this falls within that
22 exception is something that would be -- would have to be
23 determined.

24 **MR. THOMAS JARMYN:** Okay. Thank you. Mr.
25 Sheppard asked you about your recommendations regarding
26 transparency of online platforms. Is it correct that these
27 legal obligations would only apply to those platforms that
28 have a legal presence in Canada?

1 **MR. STÉPHANE PERRAULT:** It would apply to
2 those platforms that provide content in Canada.

3 **MR. THOMAS JARMYN:** So TikTok ostensibly has
4 a legal presence in Canada, so I would see how that would
5 fall in. Would -- how would WeChat, which is -- its platform
6 is entirely located in China, fall within the application of
7 those policies? Or do you understand that it wouldn't?

8 **MR. STÉPHANE PERRAULT:** So it depends how the
9 legislation is drafted. It's possible to draft legislation
10 to carry out -- to have extraterritorial aspects, I think
11 there has to be a significant nexus with Canada. So it would
12 depend on the drafting of the provision. My recommendation
13 does not go into those details in any way.

14 It does touch upon -- the point that you
15 raised touched upon the challenge of enforcing,
16 extraterritorially, some rules that may be devised to secure
17 the election.

18 **MR. THOMAS JARMYN:** Particularly with a
19 country where we do not have a mutual legal assistance
20 treaty? Is that correct?

21 **MR. STÉPHANE PERRAULT:** Correct. Again, this
22 is a matter for the Commissioner to speak to, but that is my
23 understanding.

24 **MR. THOMAS JARMYN:** Yeah. And if you saw
25 violations of any of these provisions, you would be referring
26 that to the Commissioner of Elections for investigation or
27 review and potential prosecution?

28 **MR. STÉPHANE PERRAULT:** That is correct.

1 **MR. THOMAS JARMYN:** In discussing the -- I'll
2 just conclude with this question. In discussing the
3 governance of political parties in leadership races and
4 nomination races, would you be in favour of a type of model
5 similar to the B.C. *Professional Governance Act*, which
6 essentially delegates to professions the authority to
7 regulate their profession as long as they meet the standards
8 of accountability and transparency set out in the Act? In
9 other words, Election Canada sets standards and relies upon
10 the political parties to apply those standards.

11 **MR. STÉPHANE PERRAULT:** So again, this is
12 something we need to consider at a later stage. I would say
13 two things.

14 First of all, I do believe there's room for
15 some standards, but there's also a need for flexibility, and
16 different parties will have different rules. So the level of
17 uniformity should not be necessarily very high. That's one
18 area.

19 My other comment is that we have roughly, at
20 election time, over 20 parties right now, or just below that.
21 Some parties are extremely small and hardly conduct any
22 nominations that are contested. And I think we'd have to
23 think about having standards that are tailored to the
24 realities of the different parties.

25 **MR. THOMAS JARMYN:** Okay. Those are all my
26 questions. Thank you very much, sir.

27 **COMMISSIONER HOGUE:** Thank you.

28 Counsel for Jenny Kwan?

1 **--- CROSS-EXAMINATION BY MS. MANI KAKKAR:**

2 **MS. MANI KAKKAR:** Good afternoon, Mr.
3 Perrault and Commissioner. My name is Mani Kakkar and I'm
4 counsel for Jenny Kwan.

5 This afternoon, Mr. Perrault, I just had a
6 few questions for you. One, a small housekeeping matter that
7 I was curious about.

8 You had mentioned that third parties that
9 donate individuals are asked if they are allowed to make
10 those donations on an honour system by checking a box. Are
11 you aware if Elections Canada knows or has identified cases
12 of foreigners donating money?

13 **MR. STÉPHANE PERRAULT:** So we have made
14 referrals or we've asked questions about, for example, if we
15 see a cheque that's from a foreign bank, we will raise that
16 question with the relevant entity. So this is something we
17 do look into, and there have been referrals for foreign
18 contributions.

19 **MS. MANI KAKKAR:** Okay. I appreciate your
20 answer on that point. I want to turn for a moment to the
21 regulation of nomination and leadership contests. Mr.
22 Sheppard had brought you to this and had indicated the
23 importance of regulating nominations, as you agreed, that
24 this process and Commission has showed that there are
25 loopholes being taken advantage of. Did I understand your
26 testimony?

27 **MR. STÉPHANE PERRAULT:** I think there's been
28 a recognition that it is largely unregulated and therefore an

1 area of vulnerability.

2 **MS. MANI KAKKAR:** Thank you. And I
3 appreciate that you can't speak to the specific
4 recommendations that you may make later this month or prior
5 to the policy phase of this Commission, but I wanted to
6 understand a little bit about what any regulations in this
7 area might mean for Elections Canada's budget and capacity?

8 **MR. STÉPHANE PERRAULT:** It would be more for
9 the capacity of the Commissioner of Canada Elections, and
10 depending on the rules that are imposed, whether there are
11 enforceability challenges that she would face.

12 So for example, if there are rules regarding
13 the nomination process, regarding the participation, but
14 there is no paper trail that is kept by the parties or the
15 district associations, then that presents challenges for her.
16 But the concerns are not so much financial, as they are about
17 enforceability.

18 **MS. MANI KAKKAR:** I appreciate that. And
19 maybe I'll take a step back so we can understand what this
20 means not just at the broader level of regulations, as you
21 mentioned, it will affect the OCCE, but more specifically,
22 with some of the recommendations that you've specified.

23 First, I'd like to take you to your summary,
24 WIT74. Paragraph 110 in particular.

25 In this paragraph, you describe the challenge
26 that you would have as Elections Canada, an organization that
27 springs into life in electoral districts across the country
28 when an election is called, if you were in fact administering

1 nomination and leadership contests. You talk about the
2 operational difficulty that you would have. And that's part
3 of the reason why it's clear from your interview summary that
4 that's not the path that Elections Canada is likely to
5 recommend?

6 **MR. STÉPHANE PERRAULT:** Correct.

7 **MS. MANI KAKKAR:** However, if -- you do
8 provide some baseline regulations, like those, if we scroll
9 up to paragraph 108. Will that mean that Elections Canada
10 now has to act for a longer period of time or an extended
11 period of time, given that there will be some of these
12 measures in place for nomination contests -- nomination and
13 leadership contests?

14 **MR. STÉPHANE PERRAULT:** No, not necessarily.

15 **MS. MANI KAKKAR:** Okay. Are you able to
16 elaborate a little bit on that point? And I appreciate ---

17 **MR. STÉPHANE PERRAULT:** Well, for example, if
18 there's a mandatory -- a legislative requirement to vote,
19 this is something that would be administered by the parties
20 and their district associations. Should there be a complaint
21 regarding someone voting that is not entitled to vote, then
22 that complaint would be handled by the Commissioner. And so
23 she has a permanent capacity. That would impact her, of
24 course her workload, and it raises questions, as I mentioned,
25 about, you know, paper trails that she could rely on. But it
26 does not require us to have a permanent presence in the
27 regions, for example, to administer that.

28 **MS. MANI KAKKAR:** I appreciate your answer

1 and testimony on that point. And just to go through these
2 measures in particular, would you say that about all four,
3 including whether existing prohibitions under the *Canada*
4 *Elections Act*, such as undue influence for conduct that is
5 inherently criminal should apply to nomination and leadership
6 contests? Would your office have any role?

7 **MR. STÉPHANE PERRAULT:** It would mainly be
8 for the Commissioner to enforce these rules. So it would not
9 impact my office as much as it would impact her office.

10 **MS. MANI KAKKAR:** I appreciate your
11 testimony. Thank you. Moving to a different point, I wanted
12 to take you to Section 282.4, which Mr. Sheppard addressed
13 with you, as well as my friend, Mr. Jarmyn. I appreciate you
14 have this, it seems, down to memory, but if you'd like, I can
15 put the section up for you.

16 **MR. STÉPHANE PERRAULT:** I would, please.

17 **MS. MANI KAKKAR:** Okay. Not a problem. Can
18 I ask for CEF 302_R to be pulled up?

19 **--- EXHIBIT No. CEF0000302 R:**

20 Memo for CCE_Summary 2022-0925

21 **MS. MANI KAKKAR:** And, Commissioner, I seek
22 your leave before doing so. This was a document not on my
23 list, but I'm only doing so for the purposes of having the
24 excerpt of this section.

25 **MS. ERIN DANN:** Sorry, Mr. Court Operator, I
26 believe that permission was granted. You can pull up the
27 document.

28 **MS. MANI KAKKAR:** Thank you, Ms. Dann. And

1 it's just page 4. There's a small footnote there. If you
2 want to expand or zoom in, Mr. Perrault, you'll be able to
3 see it excerpts ---

4 **MR. STÉPHANE PERRAULT:** Yeah.

5 **MS. MANI KAKKAR:** --- part of, at least, the
6 provision on undue influence.

7 **MR. STÉPHANE PERRAULT:** Correct.

8 **MS. MANI KAKKAR:** And there seem to be three
9 key components, which you summarized quite well. One, that
10 you influence an elector or unduly influence an elector to
11 vote or refrain from voting, whether it's for a particular
12 candidate, or registered party, or at all; that you knowingly
13 incur an expense to directly promote or oppose a candidate,
14 registered party, or leader of a registered party; and that
15 you -- that the conduct may be an offence under a law or
16 regulation, whether federally or provincially.

17 **MR. STÉPHANE PERRAULT:** So A and B are
18 alternatives; right? It's not ---

19 **MS. MANI KAKKAR:** That's correct. It's not
20 an A and a B situation. Either you incur the expense, and
21 you could be unduly influencing, or, B, you could violate a
22 law or a regulation. Can I get your thoughts on why you
23 think these parameters are in place to limit what would
24 otherwise be undue influence?

25 **MR. STÉPHANE PERRAULT:** This came out of Bill
26 C-76, so this was not one of my recommendations, so I cannot
27 speak to the policy analysis that went beyond that.
28 Certainly, it must be read in conjunction with another

1 provision that's in the vicinity, which provides
2 extraterritorial jurisdiction to the Commissioner, and so if,
3 in the case of clause B, it would allow her, if there are
4 violations of other Acts, to also include that in her
5 investigation. But, obviously, what I can tell you, I can
6 tell you simply from reading the provision itself, so I'm not
7 sure I can add much value there.

8 **MS. MANI KAKKAR:** Would you mind if I took
9 you through just a hypothetical? And just to get your
10 thoughts, not to necessarily get a legal opinion of any kind,
11 but we've seen in this Commission ways in which foreign
12 actors engage in interference. For example, they may be
13 influential community organisations or an FI actor that enter
14 into a free campaign, whether it's through WeChat, in person,
15 in small events, whatever it may be, let's assume for the
16 purposes of this hypothetical that it has no cost. That a
17 particular candidate, if elected, is going to -- is anti-
18 Chinese or going to cause the retaliation of the Chinese
19 government and cause them to perhaps take retributive
20 measures. And let's say, again, that there's no cost to
21 that, and that doesn't presumptively violate any law or
22 regulation. It's my understanding that this provision would
23 not apply to that.

24 **MR. STÉPHANE PERRAULT:** It would not. Now
25 I'll put two caveats. One is, I mean, the kind of conduct
26 you're describing is, to a certain degree, an inherent
27 challenge in living in an open society, that electors will be
28 subject to all kinds of influences, and it's very hard to

1 differentiate between those that may originate from state
2 actors and those that are not. So that is a challenge, and
3 foreign states can and do take advantage of the open nature
4 of our society, and that's what we have to deal with. I
5 would point to Bill C-70, which is now law, and Section 20.4,
6 which expands the scope of illegal conduct and would be
7 triggered, or would connect, if I can use that term, with
8 paragraph 2B here. So that's a new provision that talks
9 about influencing the political process at federal and
10 provincial levels. It's not before us, so apologies for
11 that. But by deceptive -- I believe language is deceptive
12 and/or surreptitious means, or something of that nature. So
13 there is an element here that could be captured, depending on
14 the fact scenario, by that provision, and through that by
15 paragraph 2B here.

16 **MS. MANI KAKKAR:** I appreciate that, and I do
17 appreciate you bringing it up. Do you think, though, outside
18 of making individual changes to legislation that may make
19 certain Acts -- that may prohibit certain Acts, and,
20 therefore, allow you to act under 282.4, do you think 282.4
21 itself needs any amendment to better capture FI activity?

22 **MR. STÉPHANE PERRAULT:** So I'm presuming here
23 you're referring to, because I don't have it in front of me
24 to -- paragraph 4, are you talking -- sorry, 282.4 as a whole
25 or any particular provision?

26 **MS. MANI KAKKAR:** Let's say that, to be fair,
27 I stick to subsection (2), which is up above.

28 **MR. STÉPHANE PERRAULT:** Yeah, so in my view,

1 this should be expanded in time and to include at all times,
2 and this is what's in Bill C-65. And it should be expanded
3 to cover nomination in the leadership contests.

4 **MS. MANI KAKKAR:** Okay. And no other
5 expansions you feel would be necessary to capture FI
6 activity?

7 **MR. STÉPHANE PERRAULT:** I'm open to
8 suggestions, but not that I can think of.

9 **MS. MANI KAKKAR:** I appreciate that. Thank
10 you very much.

11 **COMMISSIONER HOGUE:** Thank you.

12 Counsel for Michael Chong?

13 **--- CROSS-EXAMINATION BY MR. FRASER HARLAND:**

14 **MR. FRASER HARLAND:** Good afternoon, Mr.
15 Perrault. I'm Fraser Harland, counsel for Michael Chong. I
16 just wanted to ask you a few questions about the social media
17 monitoring that Elections Canada undertakes. So I understand
18 that Elections Canada has a limited role in social media
19 monitoring, focused only on the electoral process, if I can
20 put it that way; is that right?

21 **MR. STÉPHANE PERRAULT:** It is. So it
22 includes information about where and when to vote, and how to
23 vote, but it also may include information that's of interest
24 to Canada -- to Elections Canada, including how people feel
25 about the process, whether they're frustrated, or satisfied,
26 or happy, or whether there are incidents like roadblocks that
27 may affect, you know, the opening of a polling place,
28 whatnot. But the focus is really about participation in the

1 voting process. It is not about partisan opinion.

2 **MR. FRASER HARLAND:** Right. And so I
3 appreciate that distinction, and I wanted to just ask a
4 couple questions about the resourcing that's dedicated to
5 social media monitoring. So are you able to tell me how many
6 people Elections Canada employs to conduct this monitoring
7 during an election?

8 **MR. STÉPHANE PERRAULT:** So the size of the
9 team at the last election, and I'm including here -- I don't
10 have the breakdown between monitoring and doing the daily
11 reports, for example, but the team it was 27 resources. I've
12 approved 41 for the next election. I -- this is a reflection
13 of the fact that our electoral process is increasingly
14 impacted by online conversations, and social media will play
15 in the future an even greater role than it has in the past.

16 **MR. FRASER HARLAND:** And does that team have
17 people who are proficient in foreign languages, or is it only
18 English and French?

19 **MR. STÉPHANE PERRAULT:** No, no, we have
20 people who are proficient. At the last election, it was 15
21 languages. We are -- again, it depends on the recruitment,
22 but we're aiming to have the similar languages, but
23 certainly, it would include, again, Mandarin, Cantonese, and
24 Punjabi, and Russian, and a range of languages.

25 **MR. FRASER HARLAND:** And do you know how many
26 employees for Mandarin and Chinese specifically you would be
27 targeting for the next election?

28 **MR. STÉPHANE PERRAULT:** I'd be -- I would

1 have to come back to the Commission. I don't have that ---

2 **MR. FRASER HARLAND:** Okay. That's fine. And
3 do you know if that person would be monitoring the WeChat
4 platform, or that would be part of ---

5 **MR. STÉPHANE PERRAULT:** Yes, we have been
6 monitoring WeChat since 2019.

7 **MR. FRASER HARLAND:** Okay. Those are all my
8 questions. Thank you very much.

9 **COMMISSIONER HOGUE:** Thank you.
10 Attorney General?

11 **--- CROSS-EXAMINATION BY MR. BARNEY BRUCKER:**

12 **MR. BARNEY BRUCKER:** Good afternoon, Mr.
13 Perrault. Barney Brucker for the AG. I took from reviewing
14 your materials and your evidence a number of impressions, and
15 I just wanted to go through a few of them and see if you
16 agree. It seemed to me that Elections Canada has made
17 considerable effort to promote education and understanding of
18 the electoral process, particularly with respect to diaspora,
19 Indigenous and vulnerable communities. Would you agree with
20 that?

21 **MR. STÉPHANE PERRAULT:** That is correct. In
22 the case of diaspora communities, we are increasing our
23 efforts.

24 **MR. BARNEY BRUCKER:** And insofar as political
25 finance rules are concerned, it is my impression that ours,
26 or Canada's, are among the most comprehensive and strict of
27 any democratic nation, in terms of ability to limit undue
28 influence of money, transparency, and level the playing field

1 for actors in the electoral space. Would you agree with
2 that?

3 **MR. STÉPHANE PERRAULT:** That is my view. You
4 can see aspects of our regime reflected in other
5 jurisdictions, but rarely do you see the combination of roles
6 that we have. As I said, no system is watertight, but I
7 believe we have the -- if not the most robust, one of the
8 most robust in the world.

9 **MR. BARNEY BRUCKER:** And I also got the sense
10 that upgrades are being made or are planned to security
11 measures around Election Canada's IT systems, including its
12 capacity to detect misinformation and disinformation. Is
13 that fair?

14 **MR. STÉPHANE PERRAULT:** So in terms of IT
15 infrastructure, we continually engage with security experts
16 and upgrade our systems and enhance our posture. There is no
17 complete safety in that area.

18 In the case of misinformation or
19 disinformation, we are also -- and that's a different aspect,
20 but we are also enhancing our efforts in that area.

21 **MR. BARNEY BRUCKER:** I think you said the
22 SITE Task Force was stood up for the byelections, the recent
23 byelections in 2023/'24, and that the electoral coordination
24 security system, I've probably got that moniker wrong, but
25 they met regularly -- Elections Security Coordination
26 Committee. How's that?

27 **MR. STÉPHANE PERRAULT:** That's correct.

28 **MR. BARNEY BRUCKER:** Okay. We had a 10-page

1 handout yesterday of acronyms. Well, our friends at the
2 Commission. And I'm still on page one.

3 But my understanding is that Elections Canada
4 is the co-chair of that ECSS? Is that fair?

5 **MR. STÉPHANE PERRAULT:** That's correct.

6 **MR. BARNEY BRUCKER:** Along with PCO?

7 **MR. STÉPHANE PERRAULT:** Correct. So it
8 exists at different levels at the DG, ADM, and DM levels.
9 I'll be quite frank, the DM level meets more rarely. But
10 certainly during byelections, the ADM and DG levels meet
11 regularly.

12 **MR. BARNEY BRUCKER:** And the SITE Task Force
13 or its representatives regularly brief the committee?

14 **MR. STÉPHANE PERRAULT:** That is correct.

15 **MR. BARNEY BRUCKER:** And so you would, as
16 being on the committee, get access to any information they
17 might have that may impact the election integrity?

18 **MR. STÉPHANE PERRAULT:** That is my
19 expectation.

20 **MR. BARNEY BRUCKER:** And you could make
21 whatever use you would be able to do with that?

22 **MR. STÉPHANE PERRAULT:** Absolutely.

23 **MR. BARNEY BRUCKER:** Okay.

24 **MR. STÉPHANE PERRAULT:** Subject to the
25 protection of the classified documents, of course.

26 **MR. BARNEY BRUCKER:** And -- of course. And
27 you know, recent legislation, Bill C-70 and the legislative
28 initiatives that are planned, I understand, in Bill C-65, so

1 that -- these are some that's already passed and some that
2 are planned are -- also enhance the electoral process or the
3 security of electoral process? Is that fair?

4 **MR. STÉPHANE PERRAULT:** They do to a certain
5 degree, and I look forward to appearing before committee. I
6 think Bill C-65 makes a number of improvements. I think it's
7 something that can be built on, and I'm hopeful that it will.

8 **MR. BARNEY BRUCKER:** And as Canada's Chief
9 Electoral Officer, you have overall responsibility for
10 Elections Canada and the administration of federal elections;
11 right?

12 **MR. STÉPHANE PERRAULT:** That's correct.

13 **MR. BARNEY BRUCKER:** All right. Now no
14 system is perfect, and everything can improve with change,
15 but would you agree with me, are you confident that the
16 integrity of our federal electoral processes is being
17 maintained through the efforts of Elections Canada and its
18 partners?

19 **MR. STÉPHANE PERRAULT:** I have a high degree
20 of confidence in the overall integrity of our electoral
21 process in Canada. One of the reasons for that is that it's
22 always open for improvements, and after each election, it's
23 examined and looked at ways to improve the process, and this
24 is partly what's happening here.

25 **MR. BARNEY BRUCKER:** Last week we had a
26 witness who described Canada as a foreign interference
27 playground. From where you sit as Chief Electoral Officer,
28 and in your perspective, confined to elections, do you agree

1 with that statement?

2 **MR. STÉPHANE PERRAULT:** I can't comment on
3 that statement. I believe that the scope of that statement
4 must -- probably expands well beyond my mandate in the
5 administration of the election.

6 **MR. BARNEY BRUCKER:** Yes. And I'm only
7 asking in respect of your mandate. Do you have any comment
8 on that, whether ---

9 **MR. STÉPHANE PERRAULT:** So with respect to my
10 mandate, I do not believe that it is a playground for foreign
11 interference.

12 **MR. BARNEY BRUCKER:** Thank you, sir.

13 **COMMISSIONER HOGUE:** Thank you.

14 Counsel for Elections Canada, do you have any
15 questions?

16 **UNIDENTIFIED SPEAKER:** No questions. Thank
17 you.

18 **COMMISSIONER HOGUE:** No questions.

19 Mr. MacKay or Mr. Sheppard?

20 **MR. DANIEL SHEPPARD:** Thank you,

21 Commissioner. No questions.

22 **COMMISSIONER HOGUE:** No re-examination.

23 So it's over for you.

24 Have a nice evening. We'll see each other
25 tomorrow morning at 9:30.

26 **THE REGISTRAR:** Order, please.

27 This sitting of the Foreign Interference

28 Commission is adjourned until tomorrow, Wednesday, the 24th -

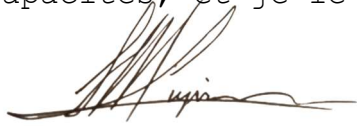
1 - the 25th of September, 2024, at 9:30 a.m.

2 --- Upon adjourning at 5:44 p.m.

3
4 C E R T I F I C A T I O N

5
6 I, Sandrine Marineau-Lupien, a certified court reporter,
7 hereby certify the foregoing pages to be an accurate
8 transcription of my notes/records to the best of my skill and
9 ability, and I so swear.

10
11 Je, Sandrine Marineau-Lupien, une sténographe officielle,
12 certifie que les pages ci-hauts sont une transcription
13 conforme de mes notes/enregistrements au meilleur de mes
14 capacités, et je le jure.

15
16 

17 Sandrine Marineau-Lupien