



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

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 / Procureure en chef de la commission	Shantona Chaudhury
Commission Counsel / Avocat(e)s de la commission	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 / Conseil de la recherche de la commission	Geneviève Cartier Nomi Claire Lazar Lori Turnbull Leah West
Commission Senior Policy Advisors / Conseillers principaux en politiques de la commission	Paul Cavalluzzo Danielle Côté

III

Appearances / Comparutions

Commission Staff / Personnel de la commission	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 Content / Table des matières

	PAGE
MR. DAVID VATCHER, Affirmed/Sous affirmation solennelle	2
MS. JULIE LACROIX, Affirmed/Sous affirmation solennelle	2
Examination in-Chief by/Interrogatoire en-chef par Mr. Gabriel Poliquin	2
Cross-Examination by/Contre-interrogatoire par Mr. Sujit Choudhry	38
Cross-Examination by/Contre-interrogatoire par Mr. Fraser Harland	44
Cross-Examination by/Contre-interrogatoire par Ms. Sara Teich	47
Cross-Examination by/Contre-interrogatoire par Mr. Guillaume Sirois	49
Cross-Examination by/Contre-interrogatoire par Mr. Neil Chantler	53
Cross-Examination by/Contre-interrogatoire par Ms. Ryann Atkins	58
 MR. PATRICK EWEN McDONELL, Affirmed/Sous affirmation solennelle	 65
MR. BENOÎT EUGÈNE DICAIRE, Affirmed/Sous affirmation solennelle	65
Examination in-Chief by/Interrogatoire en-chef par Mr. Hamza Mohamadhossen	65
Examination in-Chief by/Interrogatoire en-chef par Mr. Gabriel Poliquin	84
Cross-Examination by/Contre-interrogatoire par Mr. Fraser Harland	126
Cross-Examination by/Contre-interrogatoire par Mr. Thomas Jarmyn	129
Cross-Examination by/Contre-interrogatoire par Mr. Sujit Choudhry	133
Cross-Examination by/Contre-interrogatoire par Ms. Sarah Teich	140
Cross-Examination by/Contre-interrogatoire par Mr. Gregory Tzemenakis	143
 MR. STÉPHANE PERRAULT, Affirmed/Sous affirmation solennelle	 155
Examination in-Chief by/Interrogatoire en-chef par Mr. Jean-Philippe MacKay	155
Examination in-Chief by/Interrogatoire en-chef par Mr. Daniel Sheppard	188
Cross-Examination by/Contre-interrogatoire par Mr. Neil Chantler	217
Cross-Examination by/Contre-interrogatoire par Mr. Guillaume Sirois	225

VI
Table of Content / Table des matières

	PAGE
Cross-Examination by/Contre-interrogatoire par Ms. Sarah Teich	231
Cross-Examination by/Contre-interrogatoire par Mr. Thomas Jarmyn	232
Cross-Examination by/Contre-interrogatoire par Ms. Mani Kakkar	240
Cross-Examination by/Contre-interrogatoire par Mr. Fraser Harland	248
Cross-Examination by/Contre-interrogatoire par Mr. Barney Brucker	250

VII

Exhibit List / Liste des pièces

No.	DESCRIPTION	PAGE
SEN0000001.EN	Senate of Canada Institutional Report	3
SEN0000001.FR	Rapport institutionnel - Le parlement et le processus législatif	3
WIT0000126.FR	Résumé d'entrevue : Administration du Sénat (David Vatcher, Julie Lacroix et Shaila Anwar)	4
WIT0000126.EN	Interview Summary: Senate Administration (David Vatcher, Julie Lacroix and Shaila Anwar)	4
JKW0000169	Senate Procedure - Chapter 11 Privileges and Immunities	43
WIT0000128.EN	Interview Summary: House of Commons Administration (Patrick McDonell and Benoît Dicaire)	67
WIT0000128.BIL	Interview Summary: House of Commons Administration (Patrick McDonell and Benoît Dicaire)	67
WIT0000128.FR	Résumé d'entrevue : Administration de la Chambre des communes (Patrick McDonell et Benoît Dicaire)	67
WIT0000129.EN	Appendix to Interview Summary: House of Commons Administration (Hedi Touati and Benoît Dicaire)	68
WIT0000129.FR	Complément au résumé d'entrevue: Administration de la Chambre des communes (Hedi Touati and Benoît Dicaire)	69
HOC0000001.EN	Institutional Report of the House of Commons Administration	69
HOC0000001.FR	Rapport institutionnel de l'administration de la Chambre des Communes	70
CAN.SUM.000027	PRC Email Operations Against parliamentarians	107
CAN.SUM.000027.001	Tab A - Chronology of Events: Email Tracking Link Campaign Targeting Canadian parliamentarians	107
COM0000363	Special Report on Foreign Interference in Canada's Democratic Processes and Institutions	127
WIT0000074.EN	Interview Summary - Elections Canada (Stage 2)	155

VIII

Exhibit List / Liste des pièces

No.	DESCRIPTION	PAGE
WIT0000074.FR	Résumé d'entrevue: Élections Canada (Stéphane Perrault, Serge Caron, Josée Villeneuve et Susan Torosian)	155
WIT0000074.001	Affidavit of Jose Villeneuve	156
WIT0000074.002	Affidavit of Serge Caron	156
WIT0000074.003	Affidavit of Susan Torosian	156
ELC.IR.0000002.EN	Elections Canada's Supplementary Institutional Report August 2024	157
ELC.IR.0000002.FR	Rapport institutionnel supplémentaire d'élections Canada	157
CAN004599	Site Status Update and Summary of Foreign Interference Threats to Canadian Democratic Institutions-2023	177
ELC0000054	Meeting New Challenges - Recommendations from the Chief Electoral Officer of Canada following the 43rd and 44th General Elections	200
WIT0000015.EN	Interview Summary: Leona Alleslev	233
CAN011293	China: Domination of Chinese-Language Media in Canada Poses National Security Threats - IM 30/2023	236
CEF0000302_R	Memo for CCE_Summary 2022-0925	244

Ottawa, Ontario

--- L'audience débute le mardi 24 septembre 2024 à 9 h 32

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

LE GREFFIER: Order, please. À l'ordre, s'il vous plaît.

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

Cette séance de la Commission sur l'ingérence étrangère est en cours. La commissaire Hogue préside.

The time is 9:32 a.m. Il est 9 h 32.

COMMISSAIRE HOGUE: Alors, bonjour tout le monde. J'espère que vous avez tous eu un bon weekend.

Alors, c'est vous, Maitre Poliquin, ce matin qui menez l'interrogatoire?

Me GABRIEL POLIQUIN: Bonjour, Madame la Commissaire.

COMMISSAIRE HOGUE: Alors, good morning et bonjour. Je pense que c'est les...

Me GABRIEL POLIQUIN: Oui. Bonjour.

Si on pouvait procéder à l'affirmation solennelle des témoins, s'il vous plaît?

LE GREFFIER: Donc, Monsieur Vatcher, pourriez-vous, s'il vous plaît, indiquer votre nom complet et épeler votre nom de famille pour la transcription sténographique.

M. DAVID VATCHER: Bon matin. David Vatcher -

1 V-A-T-C-H-E-R.

2 LE GREFFIER: Merci beaucoup. Et maintenant,
3 pour la déclaration solennelle.

4 --- M. DAVID VATCHER, Affirmed/Sous affirmation solennelle:

5 LE GREFFIER: Et maintenant, pour Madame
6 Lacroix. Pourriez-vous, s'il vous plaît, indiquer votre nom
7 complet et épeler votre nom de famille pour la transcription
8 sténographique.

9 Mme JULIE LACROIX: Julie Lacroix - L-A-C-R-O-
10 I-X.

11 LE GREFFIER: Merci beaucoup. Et maintenant,
12 pour la déclaration solennelle.

13 --- Mme JULIE LACROIX, Affirmed/Sous affirmation solennelle:

14 LE GREFFIER: Merci.

15 Maitre, vous pouvez procéder.

16 Me GABRIEL POLIQUIN: Merci beaucoup.

17 --- EXAMINATION IN-CHIEF BY/INTERROGATOIRE EN CHEF PAR

18 Me GABRIEL POLIQUIN:

19 Me GABRIEL POLIQUIN: Alors, je demanderais à
20 l'opérateur judiciaire d'afficher le rapport institutionnel
21 du Sénat du Canada, document qui porte le numéro SEN1.FR.

22 Me GABRIEL POLIQUIN: Parfait. Merci.

23 Donc, Madame et Monsieur les témoins, le
24 Sénat du Canada a préparé un rapport institutionnel à la
25 demande des avocats de la Commission. C'est exact?

26 Mme JULIE LACROIX: Oui.

27 Me GABRIEL POLIQUIN: Et puis vous avez eu
28 l'occasion de revoir le rapport institutionnel du Sénat?

1 M. DAVID VATCHER: Absolument.

2 Mme JULIE LACROIX: Oui.

3 Me GABRIEL POLIQUIN: Donc, vous adoptez le
4 rapport comme élément de preuve aux fins de l'enquête de la
5 Commission?

6 Mme JULIE LACROIX: Oui.

7 Me GABRIEL POLIQUIN: Donc, le rapport est
8 soumis en preuve. La version anglaise du rapport porte le
9 numéro SEN1.EN. Inutile de l'afficher, mais je veux
10 simplement dire aux fins du procès-verbal que ce document-là
11 est également déposé en preuve.

12 --- EXHIBIT No./PIÈCE No. SEN0000001.EN:

13 Senate of Canada Institutional Report

14 --- EXHIBIT No./PIÈCE No. SEN0000001.FR:

15 Rapport institutionnel - Le Parlement
16 et le processus législatif

17 Me GABRIEL POLIQUIN: Alors, je demanderais
18 maintenant à l'opérateur d'afficher le résumé d'entrevue des
19 témoins du Sénat, document qui porte le numéro WIT126.FR.

20 Donc, vous vous rappelez, Madame et Monsieur
21 les témoins, que vous avez été interrogés par les avocats de
22 la Commission le jeudi 12 septembre 2024. C'est exact?

23 M. DAVID VATCHER: Oui.

24 Mme JULIE LACROIX: Exact.

25 Me GABRIEL POLIQUIN: OK. Et puis les avocats
26 de la Commission ont ensuite préparé un résumé d'entrevue qui
27 vous a été communiqué, ainsi qu'au légiste du Canada. Vous
28 vous rappelez de ça?

1 M. DAVID VATCHER: Exact.

2 Mme JULIE LACROIX: Oui.

3 Me GABRIEL POLIQUIN: Puis vous avez eu
4 l'occasion de vérifier les informations contenues dans le
5 rapport... dans le résumé?

6 Mme JULIE LACROIX: Oui.

7 Me GABRIEL POLIQUIN: Vous êtes d'accord que
8 le résumé d'entrevue est un compte rendu exact des réponses
9 que vous avez données à l'entrevue?

10 M. DAVID VATCHER: Oui.

11 Mme JULIE LACROIX: Oui.

12 Me GABRIEL POLIQUIN: Donc, le résumé est donc
13 déposé en preuve. Inutile d'afficher la version anglaise qui
14 porte le numéro WIT125.EN, cette version va également être
15 déposée en preuve.

16 --- EXHIBIT No./PIÈCE No. WIT0000126.FR:

17 Résumé d'entrevue : Administration du
18 Sénat (David Vatcher, Julie Lacroix
19 et Shaila Anwar

20 --- EXHIBIT No./PIÈCE No. WIT0000126.EN:

21 Interview Summary: Senate
22 Administration (David Vatcher, Julie
23 Lacroix and Shaila Anwar)

24 Me GABRIEL POLIQUIN: Donc, mes questions pour
25 vous aujourd'hui seront en français largement, mais sentez-
26 vous libres de répondre dans la langue officielle de votre
27 choix.

28 Alors, dans un premier temps, je veux

1 simplement aborder, pour mettre la table, vos fonctions, vos
2 rôles et responsabilités au sein de l'administration du
3 Sénat.

4 Donc, à commencer par vous, Madame Lacroix,
5 quelles sont vos fonctions actuelles?

6 **Mme JULIE LACROIX:** Je suis la directrice de
7 la Sécurité institutionnelle du Sénat et je m'occupe de toute
8 matière de sécurité du Sénat, à l'exception des opérations de
9 la sécurité physique, dont ceux-ci relèvent du Service de
10 protection parlementaire.

11 **Me GABRIEL POLIQUIN:** D'accord. Puis quels
12 sont les rôles et responsabilités... vous pouvez peut-être
13 étendre sur votre réponse, mais la direction de la Sécurité
14 institutionnelle, est-ce qu'elle s'occupe d'autres choses?

15 **Mme JULIE LACROIX:** Oui. Dans le fond, dans
16 mes fonctions, j'agis aussi en tant que conseillère
17 principale en matière de sécurité à la présidente du Sénat,
18 la greffière du Sénat, et la régie interne. Je m'occupe... il y
19 plusieurs divisions qui composent ma direction, dont
20 l'accréditation de sécurité, la gestion de risque, les
21 enquêtes, tout l'aspect de sécurité en enceinte, les
22 déplacements à l'étranger, à travers le pays, la gestion de
23 la prévention des incendies, le stationnement, les événements
24 de sécurité, la gestion de projets de sécurité aussi, les
25 opérations techniques de sécurité et la sensibilisation à la
26 sécurité, pour ne nommer que quelques divisions.

27 **Me GABRIEL POLIQUIN:** OK. Puis on va aborder
28 la sensibilisation à la sécurité dans mes questions un peu

1 plus tard.

2 Je pense que je ne vous ai pas posé la
3 question, mais depuis quand occupez-vous vos fonctions?

4 **Mme JULIE LACROIX:** J'occupe mes fonctions
5 depuis 2018.

6 **Me GABRIEL POLIQUIN:** D'accord. Puis combien
7 de membres du personnel compte la direction à peu près?

8 **Mme JULIE LACROIX:** Quarante-deux (42).

9 **Me GABRIEL POLIQUIN:** OK. Et puis dans cette
10 direction-là, qui détient une cote de sécurité? Pas les noms
11 là, mais quelques proches.

12 **Mme JULIE LACROIX:** Ah, les 42 employés.

13 **Me GABRIEL POLIQUIN:** D'accord. À quel niveau?

14 **Mme JULIE LACROIX:** Top secret.

15 **Me GABRIEL POLIQUIN:** D'accord. Puis au sein
16 de votre unité, au sein de votre direction, est-ce qu'il y a
17 une personne spécifique qui s'occupe de questions relatives à
18 l'ingérence étrangère ou est-ce que c'est une responsabilité
19 partagée?

20 **Mme JULIE LACROIX:** C'est une responsabilité
21 partagée.

22 **Me GABRIEL POLIQUIN:** D'accord. Puis on va
23 entrer dans plus de détails plus tard dans quel genre de
24 questions auxquelles vous faites face.

25 Monsieur Vatcher, à votre tour, j'ai des
26 questions semblables pour vous.

27 Quelles sont vos fonctions actuelles?

28 **M. DAVID VATCHER:** Bon matin, Maitre. Donc,

1 David Vatcher, je suis directeur des Services d'information
2 au Sénat, et puis notre direction, une cinquantaine
3 d'employés, est chargée de la gestion de l'information, donc
4 le traitement des archives du Sénat, archives du Parlement,
5 mais et aussi tout ce qui est TI, donc du service à la
6 clientèle jusqu'à la gestion d'infrastructures. Et également,
7 on a une équipe qui fait du développement applicatif et de
8 l'intégration de systèmes.

9 **Me GABRIEL POLIQUIN:** D'accord. Puis par
10 développement applicatif, intégration de systèmes, nous
11 expliquer un peu qu'est-ce que ça voudrait dire.

12 **M. DAVID VATCHER:** Donc, le Sénat, c'est une
13 institution unique au Canada, bien sûr, et puis on a des
14 applications qui sont faites « *in house* » pour répondre
15 exactement aux besoins précis de la Chambre, par exemple.

16 **Me GABRIEL POLIQUIN:** D'accord. Des
17 applications, donc des logiciels qui sont développés.

18 **M. DAVID VATCHER:** Exactement.

19 **Me GABRIEL POLIQUIN:** D'accord. Parfait. Puis
20 depuis quand occupez-vous vos fonctions?

21 **M. DAVID VATCHER:** Depuis février 2018.

22 **Me GABRIEL POLIQUIN:** D'accord. Donc, même
23 question pour vous : qui détient au sein de votre unité une
24 cote de sécurité?

25 **M. DAVID VATCHER:** L'ensemble des employés de
26 ma direction détient une cote de sécurité « secret ».

27 **Me GABRIEL POLIQUIN:** Parfait. Merci. Puis
28 donc, est-ce qu'il existe une personne spécifique qui

1 s'occupe d'ingérence étrangère au sein de l'unité ou est-ce
2 que c'est une responsabilité partagée?

3 **M. DAVID VATCHER:** Ce n'est pas... non, il n'y a
4 pas une personne qui s'occupe spécifiquement de l'ingérence
5 étrangère.

6 **Me GABRIEL POLIQUIN:** Parfait. Merci.

7 Je vais aborder maintenant les relations du
8 Sénat avec des partenaires externes, en matière de sécurité
9 plus généralement, mais aussi, si ça englobe l'ingérence
10 étrangère, nous le faire savoir.

11 Donc je vais commencer par vous, Madame
12 Lacroix.

13 Si vous pouviez décrire de manière générale
14 quelles sont vos relations avec des partenaires externes,
15 puis par ça j'entends les agences de sécurité et de
16 renseignement, mais aussi des services de police, des
17 services d'application de la loi.

18 **Mme JULIE LACROIX:** Donc, nous avons de très
19 bonnes relations et collaborations avec le Service de
20 renseignements, la police locale, divers services de police,
21 la GRC, et nos partenaires à la sécurité à travers le fédéral
22 et la Colline du Parlement.

23 **Me GABRIEL POLIQUIN:** Puis quand vous parlez
24 de collaboration, on parle de quoi? D'échanges de
25 renseignements? De...

26 **Mme JULIE LACROIX:** Échanges, réunions
27 informelles, réunions quotidiennes, conseils au niveau de
28 préparatifs de documents de breffage, et cetera.

1 **Me GABRIEL POLIQUIN:** D'accord. Puis, outre la
2 préparation de documents de breffage, est-ce qu'il y a
3 d'autres objectifs dans l'échange de cette information-là?

4 **Mme JULIE LACROIX:** Ben, je pense qu'on
5 travaille tous dans le but commun d'assurer la sécurité de
6 tous ceux qu'on dessert.

7 **Me GABRIEL POLIQUIN:** D'accord. En parlant de
8 différents forums d'échanges, au paragraphe 38 du résumé
9 d'entrevue, vous mentionnez l'organisme Intersec. Pouvez-vous
10 nous expliquer c'est quoi Intersec puis quelle est la
11 participation du Sénat?

12 **Mme JULIE LACROIX:** C'est un forum d'échanges
13 de divers participants qui jouent un rôle de sûreté et de
14 sécurité, dont le Sénat y participe.

15 **Me GABRIEL POLIQUIN:** Merci. Puis de manière
16 générale, pour tout autre forum d'échanges comme ça, est-ce
17 que vous décririez ces échanges-là comme étant proactifs en
18 matière de prévention, en matière de sécurité, ou est-ce que
19 c'est réactif? Un peu des deux?

20 **Mme JULIE LACROIX:** Un peu des deux.

21 **Me GABRIEL POLIQUIN:** D'accord. Puis quand
22 c'est proactif, est-ce que l'ingérence étrangère
23 spécifiquement est une question qui est souvent à l'ordre du
24 jour?

25 **Mme JULIE LACROIX:** Ça pourrait.

26 **Me GABRIEL POLIQUIN:** Donc, ça... est-ce que ça
27 intervient souvent ou...

28 **Mme JULIE LACROIX:** Pardon?

1 **Me GABRIEL POLIQUIN:** Est-ce que c'est quelque
2 chose qui est soulevé de manière fréquente ou...

3 **Mme JULIE LACROIX:** Je pense que ça dépend des
4 échanges et ça dépend du contexte, mais c'est parfois
5 discuté.

6 **Me GABRIEL POLIQUIN:** D'accord. Est-ce que le
7 Sénat détient des ententes formelles avec ces agences-là en
8 matière de sécurité physique?

9 **Mme JULIE LACROIX:** En matière de sécurité
10 physique, le Sénat et la Chambre des communes, dont les deux
11 présidents, ont une entente formelle avec la Sécurité
12 publique et la GRC quant à la gestion du service de
13 protection parlementaire.

14 **Me GABRIEL POLIQUIN:** Le service de protection
15 parlementaire, si je comprends bien, ne relève pas de votre
16 direction.

17 **Mme JULIE LACROIX:** Non, et il se rapporte aux
18 deux présidents.

19 **Me GABRIEL POLIQUIN:** D'accord. C'est compris.
20 Vous nous avez parlé tout à l'heure d'accréditation. Qu'est-
21 ce que ça veut dire, « accréditation »?

22 **Mme JULIE LACROIX:** L'accréditation, dans le
23 fond, c'est le point de filtrage et de contrôle de sécurité,
24 dont le *background check* de tous les employés. Donc, c'est
25 une vérification des antécédents et de la loyauté.

26 **Me GABRIEL POLIQUIN:** D'accord. Puis en
27 matière d'accréditation, est-ce que ça arrive que vous faites
28 face à des questions d'ingérence étrangère?

1 **Mme JULIE LACROIX:** Ça pourrait arriver, oui.

2 **Me GABRIEL POLIQUIN:** Est-ce que c'est arrivé?

3 Sans entrer dans les détails là.

4 **Mme JULIE LACROIX:** Oui.

5 **Me GABRIEL POLIQUIN:** OK. Merci.

6 Monsieur Vatcher...

7 **COMMISSAIRE HOGUE:** Attendez, juste une

8 question...

9 **Me GABRIEL POLIQUIN:** Oui, allez-y.

10 **COMMISSAIRE HOGUE:** ...Maitre Poliquin.

11 Vous indiquez que ce sont les vérifications

12 de sécurité des employés. Est-ce que je dois comprendre que

13 les sénateurs, par ailleurs, en sont exclus du champ de...

14 **Mme JULIE LACROIX:** Exact. Donc...

15 **COMMISSAIRE HOGUE:** ...de ces vérifications?

16 **Mme JULIE LACROIX:** La politique

17 d'accréditation du Sénat ne s'applique pas aux sénateurs.

18 **COMMISSAIRE HOGUE:** D'accord.

19 **Me GABRIEL POLIQUIN:** D'accord. Puis une fois

20 qu'une personne est accréditée, ça leur donne quels droits?

21 **Mme JULIE LACROIX:** Ça leur donne le droit

22 d'accéder à de l'information dont ils ont besoin, ça leur

23 donne le droit d'accéder les lieux, c'est une condition

24 d'emploi.

25 **Me GABRIEL POLIQUIN:** D'accord. Mais si je

26 comprends bien, pour faire suite à la question de Madame la

27 Commissaire...

28 **Mme JULIE LACROIX:** Oui.

1 **Me GABRIEL POLIQUIN:** ...lorsqu'un sénateur est
2 nommé, une sénatrice est nommée, est-ce que c'est automatique
3 qu'ils ont accès à tous ces services-là – les lieux, les
4 logiciels, et cetera?

5 **Mme JULIE LACROIX:** Un sénateur ou on parle
6 d'un employé?

7 **Me GABRIEL POLIQUIN:** Un sénateur.

8 **Mme JULIE LACROIX:** Un sénateur, dès qu'il est
9 nommé et entre en ses fonctions, a accès à l'enceinte
10 parlementaire, oui.

11 **Me GABRIEL POLIQUIN:** D'accord.

12 **Mme JULIE LACROIX:** Et à l'information dont il
13 a besoin pour exécuter ses fonctions parlementaires.

14 **Me GABRIEL POLIQUIN:** Parfait. Donc, juste
15 pour faire un suivi sur ça, donc, s'il y a une matière de..
16 s'il est question de vérifier les antécédents d'un sénateur
17 ou d'une sénatrice avant sa nomination, ça ne relève pas de
18 votre service.

19 **Mme JULIE LACROIX:** Ça relèverait du Bureau du
20 Conseil privé.

21 **Me GABRIEL POLIQUIN:** C'est compris. Parfait.

22 Monsieur Vatcher, maintenant, donc, de votre
23 côté, du côté de la sécurité de l'information des TI, quelles
24 sont, de manière générale, vos relations avec les partenaires
25 externes?

26 **M. DAVID VATCHER:** Nos relations... je
27 qualifierais qu'on a une relation de très positive, une très
28 bonne communication qui a lieu entre mon équipe et les

1 équipes de différents sites gouvernementaux, et puis, donc,
2 lorsque quelque chose vient à leur attention qui pourrait
3 nous intéresser où un sénateur ou un employé du Sénat
4 pourrait être une cible spécifique d'une cyberattaque, on est
5 averti et puis on pose les actions nécessaires.

6 **Me GABRIEL POLIQUIN:** D'accord. Puis on va
7 avoir plus de questions pour ça, à ce sujet-là plus tard,
8 mais pour faire un suivi, donc, lorsque... il y a une règle
9 spécifique, vous êtes avertis. Est-ce que vous détectez aussi
10 des attaques sur la base de vos propres capacités, c'est-à-
11 dire sans collabor...

12 **M. DAVID VATCHER:** Quotidiennement.

13 **Me GABRIEL POLIQUIN:** Quotidiennement.
14 D'accord. Puis dans quelles circonstances est-ce que vous
15 seriez alertés par un partenaire externe?

16 **M. DAVID VATCHER:** S'il s'agissait d'une
17 attaque qui venait à leur attention par un de leurs moyens et
18 qui pourrait impacter un de nos parlementaires ou un de nos
19 employés, il nous en ferait part tout simplement.

20 **Me GABRIEL POLIQUIN:** D'accord. Puis on aura
21 l'occasion d'explorer ce sujet-là en parlant d'un incident en
22 particulier.

23 Donc, quelle est la fréquence de vos échanges
24 avec les partenaires externes?

25 **M. DAVID VATCHER:** Nos échanges sont
26 réguliers, mais sont... c'est selon le besoin. Nous n'avons pas
27 de forums mensuels ou quoi que ce soit où nous nous
28 rencontrons pour discuter de différents trucs...

1 **Me GABRIEL POLIQUIN:** OK.

2 **M. DAVID VATCHER:** ...mais mon équipe est
3 toujours à l'écoute de ces agences-là pour... justement pour
4 être à l'affut de potentiels problèmes.

5 **Me GABRIEL POLIQUIN:** D'accord. De potentiels
6 problèmes, mais aussi en matière d'échanges de bonnes
7 pratiques, est-ce qu'il y a des rencontres... je sais pas,
8 régulières qui portent sur ça, pour l'éducation finalement de
9 l'administration du Sénat?

10 **M. DAVID VATCHER:** Donc, ces instances-là,
11 dans certains cas émettent des bonnes pratiques justement, et
12 le Sénat, à travers son... a un programme de cybersécurité et à
13 travers ce programme-là a mis de l'avant l'ensemble des
14 meilleures pratiques de l'industrie et telles qu'elles se
15 représentent pour un institut gouvernemental, donc en étroite
16 collaboration avec eux là, si on a des questions, on peut
17 leur poser, mais nous mettons de l'avant les meilleures
18 pratiques de l'industrie.

19 **Me GABRIEL POLIQUIN:** OK. Mais si je comprends
20 bien, c'est un peu de l'initiative du Sénat de rechercher,
21 d'être à l'affut de ces mêmes pratiques-là qui sont
22 développées par les agences, c'est ça?

23 **M. DAVID VATCHER:** Absolument.

24 **Me GABRIEL POLIQUIN:** D'accord. Donc, si je
25 comprends bien, donc, y'a pas de forums, des rencontres
26 régulières pour échanger les bonnes...

27 **M. DAVID VATCHER:** Exactement.

28 **Me GABRIEL POLIQUIN:** D'accord. Donc, dans vos

1 échanges qui, comme vous l'avez dit, sont sur une base... sur
2 la base du besoin, de nécessité, est-ce que des questions...
3 vous faites face à des questions d'ingérence étrangère?

4 **M. DAVID VATCHER:** Nous faisons face à des
5 questions de cybersécurité, de cybermenaces...

6 **Me GABRIEL POLIQUIN:** Oui.

7 **M. DAVID VATCHER:** ...qui, lors de leur
8 apparition, ne sont pas nécessairement reliées à une
9 ingérence étrangère et elles sont toutes prises au sérieux,
10 bien entendu, puis c'est parfois plus tard qu'on découvre que
11 c'était l'œuvre d'un malfaiteur étranger.

12 **Me GABRIEL POLIQUIN:** D'accord. Puis cette
13 information-là qu'une cyberattaque est l'œuvre d'un
14 malfaiteur étranger, est-ce que ça fait une différence dans
15 vos pratiques par rapport à la prévention ou à la réaction
16 contre une cyberattaque?

17 **M. DAVID VATCHER:** Euh... je vous dirais que
18 non. L'ensemble des menaces est affronté par mon équipe de
19 manière à l'éliminer le plus rapidement possible, puis comme
20 je vous dis, puisqu'on ne sait pas qu'il s'agit d'un État
21 ailleurs qui nous menace ou qui nous attaque, on... c'est pas
22 dans cette optique-là que nous réglons le problème, mais bien
23 dans l'optique de prévenir que de potentiels dommages soient
24 plus grands qu'on l'aimerait.

25 **Me GABRIEL POLIQUIN:** D'accord. Puis j'aurai
26 d'autres questions à ce sujet-là dans quelques minutes.

27 Donc, j'aimerais passer maintenant au sujet
28 de la formation des sénateurs puis des membres du personnel,

1 puis quand je vais parler de membres du personnel, j'entends
2 à la fois le personnel des sénateurs et aussi le personnel de
3 l'administration du Sénat. Je comprends qu'il y a des
4 différences au niveau des ressources humaines, mais en
5 matière de formation, je ne ferai pas la différence, mais
6 s'il y en a une, s'il vous plait me l'indiquer.

7 Donc, pour vous, Madame Lacroix, si vous
8 pouvez me décrire quelles sont les formations que votre unité
9 donne aux sénateurs et aux membres du personnel?

10 **Mme JULIE LACROIX:** Oui. Donc, dès la
11 nomination et l'appointement du sénateur, on fait ce qu'on
12 appelle un *on-boarding* et une orientation. C'est une
13 formation de sensibilisation à la sécurité, des multiples
14 facettes de la sécurité, et on fait la même chose avec le
15 personnel de l'administration et des bureaux de sénateurs.

16 **Me GABRIEL POLIQUIN:** Est-ce que c'est la même
17 formation pour les sénateurs et pour le personnel?

18 **Mme JULIE LACROIX:** Non. Pour les sénateurs,
19 ça peut comprendre des composantes un peu plus différentes
20 quant à la sécurité personnelle et physique des sénateurs,
21 surtout lors de leurs déplacements, etc.

22 **Me GABRIEL POLIQUIN:** D'accord. Et nous, ce
23 qui nous intéresse évidemment ici, c'est l'ingérence
24 étrangère.

25 **Mme JULIE LACROIX:** Oui.

26 **Me GABRIEL POLIQUIN:** Est-ce qu'il y a une
27 différence sur cette question-là? Est-ce que les sénateurs
28 ont une formation en matière d'ingérence étrangère qui est

1 différente?

2 **Mme JULIE LACROIX:** Oui, absolument, puisque...
3 surtout dans le contexte des déplacements à l'étranger,
4 lorsqu'ils reçoivent aussi des invités ou des délégations de
5 l'étranger. Donc, oui, il y a une composante un peu plus
6 différente entre les sénateurs et le personnel. Cependant, on
7 y touche quand même le sujet avec le personnel des sénateurs.

8 **Me GABRIEL POLIQUIN:** D'accord. Puis cette
9 formation-là d'ingérence étrangère, elle est intégrée au
10 processus d'accueil, ce qu'on appelle le « *on-boarding* »,
11 depuis quand environ?

12 **Mme JULIE LACROIX:** Avant mon arrivée.

13 **Me GABRIEL POLIQUIN:** D'accord. D'accord.
14 Et puis, si vous pouvez nous décrire peut-être un peu plus en
15 détail, quand vous parlez d'une formation en matière
16 d'ingérence étrangère, pour les sénateurs ou pour le
17 personnel, c'est quel genre de choses qu'on leur a dit?

18 **Mme JULIE LACROIX:** Je ne voudrais pas trop
19 entrer dans le détail pour nuire à notre posture de sécurité
20 et à nos mesures d'atténuation.

21 **Me GABRIEL POLIQUIN:** D'accord. Puis dans
22 quelle mesure est-ce que votre direction collabore avec
23 d'autres agences pour le développement de ces formations-là?

24 **Mme JULIE LACROIX:** Oui, nous collaborons
25 avec d'autres partenaires. Et parfois dans nos échanges avec
26 le service de renseignement, ils nous fournissent des
27 ressources qu'on trouve utiles et on peut... on donne
28 justement, lors de la formation.

1 **Me GABRIEL POLIQUIN:** D'accord. Puis est-ce
2 que les agences de sécurité et de renseignement offrent,
3 elles, des formations directement, soit aux sénateurs, soit
4 au personnel?

5 **Mme JULIE LACROIX:** C'est quelque chose
6 qu'ils offrent sur demande.

7 **Me GABRIEL POLIQUIN:** Que les agences de
8 sécurité offrent sur demande aux sénateurs?

9 **Mme JULIE LACROIX:** Oui.

10 **Me GABRIEL POLIQUIN:** D'accord. Et au
11 personnel. Donc, juste de manière générale, en matière de
12 sécurité... puis encore là, entrez pas dans les détails
13 nécessairement, mais c'est quoi les ressources disponibles?
14 Qui est-ce que les sénateurs peuvent contacter, par exemple,
15 s'ils font face à une menace de sécurité?

16 **Mme JULIE LACROIX:** Ils peuvent nous
17 contacter, contacter la police locale de leur région. Aussi,
18 on peut faciliter des réunions avec le service de
19 renseignement, GRC ou autre, dépendamment du sujet.

20 **Me GABRIEL POLIQUIN:** D'accord. Puis qu'en
21 est-il s'ils sont à l'étranger?

22 **Mme JULIE LACROIX:** Pardon?

23 **Me GABRIEL POLIQUIN:**

24 **Mme JULIE LACROIX:** Qu'en est-il s'ils sont à
25 l'étranger? Même chose?

26 **Me GABRIEL POLIQUIN:** S'ils sont à
27 l'étranger, nous avons un framework de sécurité qui les
28 accompagne. Donc, ça pourrait être du personnel ressources

1 sur place. Sinon, on les équipe avec les ressources à
2 l'étranger et un point de contact, etcetera.

3 **Mme JULIE LACROIX:** D'accord. Merci.

4 **Me GABRIEL POLIQUIN:** De votre côté, Monsieur
5 Vatcher, comme on est sur la question des voyages, on peut
6 commencer par là. Lorsqu'un sénateur ou un membre du
7 personnel du Sénat voyage à l'étranger, c'est quoi les
8 préparatifs de votre côté? Qu'est-ce que vous faites pour
9 équiper le sénateur ou le personnel?

10 **M. DAVID VATCHER:** Donc, avant un voyage,
11 nous demandons au sénateur voyageur de nous indiquer là où il
12 ou elle se rendra et la raison pour laquelle, sans rentrer
13 trop dans les détails, afin de déterminer le niveau de risque
14 associé à ce voyage-là. Au besoin, des dispositions seront
15 prises pour sécuriser davantage ou non les équipements du
16 sénateur ou de la sénatrice qui voyage.

17 **Me GABRIEL POLIQUIN:** D'accord.
18 L'équipement, on parle d'ordinateur, de téléphone, c'est ça?

19 **M. DAVID VATCHER:** On parle essentiellement
20 d'appareils mobiles, donc téléphone cellulaire et ordinateur
21 au besoin.

22 **Me GABRIEL POLIQUIN:** D'accord. De manière
23 plus générale, c'est quoi les formations qui sont données au
24 sénateur ou au personnel en matière de protection de
25 l'information, de TI?

26 **M. DAVID VATCHER:** Donc, pour ce qui est de
27 mon groupe, deux formations obligatoires existent pour
28 l'ensemble des employés et des sénateurs. La première, c'est

1 une formation sur la gestion de l'information, où on explique
2 très bien le traitement qu'une information doit avoir du
3 berceau jusqu'à la fin de sa vie utile.

4 Et puis, à l'intérieur de notre programme de
5 protection et de cybersécurité, il y a une formation toujours
6 obligatoire, qui est de sensibilisation à la cybersécurité,
7 qui est donnée à tous. On demande aux nouveaux employés,
8 comme aux nouveaux sénateurs, de compléter cette formation-là
9 dans les deux semaines à leur arrivée au Sénat.

10 Les sénateurs peuvent aussi... ben, je
11 rencontre chaque nouveau sénateur, moi ou un de mes
12 gestionnaires, si je suis absent cette journée-là, afin de
13 leur parler des risques reliés à la cybersécurité et aux
14 cybermenaces à lesquelles ils font face en tant que
15 sénateurs.

16 **Me GABRIEL POLIQUIN:** D'accord. Donc, ça
17 fait partie du processus d'accueil, si je comprends bien.
18 Est-ce qu'il y a des formations qui sont données de manière
19 régulière par après?

20 **M. DAVID VATCHER:** Certaines formations
21 peuvent être données suite à des échecs, par exemple, à des
22 simulations d'hameçonnage que nous pourrions faire.
23 Quelqu'un qui mord à l'hameçon, disons, pourrait se voir
24 contraint de suivre une seconde formation afin de rappeler
25 les dangers, mais aussi comment repérer ces risques-là.

26 **Me GABRIEL POLIQUIN:** D'accord. Donc, si je
27 comprends bien, c'est un genre de test...

28 **M. DAVID VATCHER:** Absolument.

Me GABRIEL POLIQUIN: ... que vous faites aux

M. DAVID VATCHER: Absolument.

Me GABRIEL POLIQUIN: ... à quoi vous faites

M. DAVID VATCHER: Absolument.

Me GABRIEL POLIQUIN: Puis quelle est la

M. DAVID VATCHER: Elle n'a pas été incluse

Me GABRIEL POLIQUIN: D'accord. Merci.

Les formations que vous donnez en matière de

Mme JULIE LACROIX: Non.

Me GABRIEL POLIQUIN: Donc, le processus

Mme JULIE LACROIX: Non.

Me GABRIEL POLIQUIN: Et c'est pas

obligatoire pour les sénateurs pis c'est pas obligatoire pour le personnel non plus? Je vous ai vu hocher de la tête.

Mme JULIE LACROIX: Non.

Me GABRIEL POLIQUIN: Merci. Parfait.

Passons plus précisément au sujet de cyberattaque. Donc, je vais faire appel à vous, Monsieur Vatcher, surtout.

C'est mentionné au paragraphe 57 et suivant du résumé d'entrevue. On n'est pas obligé de se tourner vers le document, mais simplement pour la référence.

Pour ce qui est des cyberattaques en général, si vous pouviez, sans rentrer dans le détail, décrire la nature du genre de cyberattaque auquel le Sénat fait face?

M. DAVID VATCHER: Notre institution fait face à l'ensemble des cybermenaces qui existent et de manière continue. On sait que, de par nos outils, on sait... en partie, parce qu'il y a souvent, par exemple, des courriels d'hameçonnage qui rentrent, mais qu'on n'est pas au courant, mais que le sénateur ou l'employé va effacer directement.

Donc, je pourrais pas vous donner de chiffres précis, mais on sait qu'on fait face à l'ensemble des types d'attaques possibles, étant donné que nous répondons aux quatre types de malfaiteurs, si vous voulez.

Me GABRIEL POLIQUIN: C'est quoi les quatre types de malfaiteurs?

M. DAVID VATCHER: Le premier est l'opportuniste, qui découvre une faille en quelque part et il tente de l'exploiter. Le deuxième est l'activiste, qui a une cause en tête. Le troisième, c'est... il est... je vais dire

1 financier. Donc, lui ou elle, ces groupes-là veulent obtenir
2 de l'argent et, par exemple, les rançongiciels sont souvent
3 donc dans cette catégorie-là. Et finalement, il y a les
4 états qui peuvent tenter d'obtenir de l'information ou de
5 nuire aux opérations de l'institution.

6 Donc, plus on monte dans ces quatre niveaux-
7 là, plus ces malfaiteurs-là ont du temps et de l'argent à
8 investir dans ces attaques-là.

9 **Me GABRIEL POLIQUIN:** D'accord. Puis est-ce
10 que, de façon correspondante, ça change votre approche
11 opérationnelle pour l'un ou l'autre?

12 **M. DAVID VATCHER:** Il est certain qu'une
13 réponse à une attaque va être basée sur le type d'attaque,
14 mais toutes les attaques sont prises au sérieux et traitées
15 dès que possible.

16 **Me GABRIEL POLIQUIN:** Si vous voulez
17 éclaircir quelque chose pour moi, parce que tout à l'heure,
18 on disait, bon, est-ce que l'information à savoir si un
19 acteur étatique est derrière une attaque, si j'ai bien
20 compris votre réponse, d'un point de vue opérationnel, c'est
21 un peu pareil, si je comprends bien.

22 **M. DAVID VATCHER:** Dans un premier temps,
23 c'est de faire échouer cette tentative.

24 **Me GABRIEL POLIQUIN:** D'accord.

25 **M. DAVID VATCHER:** Ensuite, on pourra faire
26 des exercices de vérification d'où venait... quelle était la
27 provenance. Pis à ce moment-là, on pourrait, comme on
28 parlait tout à l'heure, parler avec nos collègues de

1 différentes agences de sécurité canadiennes sur trouver la
2 provenance et sur faire les *forensics*, comme on dit en
3 anglais.

4 **Me GABRIEL POLIQUIN:** D'accord. Au
5 paragraphe 58 de votre résumé d'entrevue, vous parlez
6 spécifiquement d'un des risques, je ne sais pas si c'est une
7 vulnérabilité, mais un des risques auxquels le Sénat fait
8 face, entre autres parmi d'autres institutions là, ce sont
9 les attaques secondaires. Pouvez-vous me parler de c'est
10 quoi une attaque secondaire? Pis si vous voulez vous mettre
11 en contexte, on peut afficher le résumé d'entrevue.

12 **M. DAVID VATCHER:** Pas nécessaire. Une
13 attaque secondaire consiste... c'est une attaque qui a été
14 menée dans un premier temps vers une firme avec laquelle... une
15 firme de confiance avec laquelle nous faisons affaire et que
16 possiblement que cette firme-là, c'est à leur insu, même. Et
17 qu'ensuite, le malfaiteur utilise cette voie pour attaquer
18 notre institution.

19 Donc, si je reçois un courriel d'une firme
20 avec laquelle je fais affaire qui me demande un paiement, je
21 dois forcément faire attention, mais dans la façon que c'est
22 fait, parce que, bien entendu, nous recourons à différents
23 services pour les opérations du Sénat et on veut s'assurer
24 que les gens avec qui on fait affaire sont vraiment surs.

25 **COMMISSAIRE HOGUE:** Fait que ce que vous
26 voulez dire par... je donne un exemple tout à fait
27 hypothétique... le Sénat fait affaire avec une firme de
28 comptable.

1 **M. DAVID VATCHER:** Absolument.

2 **COMMISSAIRE HOGUE:** Qui fournit des services
3 comptables. Une attaque secondaire, c'est qu'un acteur
4 quelconque commencerait par s'ingérer dans le système de la
5 firme comptable?

6 **M. DAVID VATCHER:** Voilà.

7 **COMMISSAIRE HOGUE:** Et par cette voie-là,
8 puisque la firme comptable a des liens, on imagine,
9 informatiques là avec le Sénat, utiliserait cette voie-là
10 pour tenter de pénétrer votre système?

11 **M. DAVID VATCHER:** En fait, exactement ou
12 presque. En fait, ce qu'ils feraient, c'est qu'ils
13 tenteraient d'usurper l'identité de cette firme-là pour
14 entrer en communications en nous... avec nous pour nous jouer
15 de vilains tours là.

16 **COMMISSAIRE HOGUE:** D'accord.

17 **M. DAVID VATCHER:** Donc, nous, on doit
18 s'assurer avec les firmes qu'on fait affaire qu'il y ait
19 donc... on leur demande si jamais il y a un problème
20 quelconque, qu'ils croient être attaqués, qu'ils nous en
21 fassent part, au moins pour qu'on puisse faire la part des
22 choses et savoir ce qui se passe.

23 **COMMISSAIRE HOGUE:** D'accord. Alors, il n'y
24 a pas nécessairement d'intrusion dans le système du tiers,
25 c'est simplement d'usurper l'identité pour avoir accès...

26 **M. DAVID VATCHER:** Exactement.

27 **COMMISSAIRE HOGUE:** ... au vôtre? D'accord.

28 **Me GABRIEL POLIQUIN:** D'accord. Merci.

1 Pour venir à des cyberattaques qui viennent
2 d'acteurs étatiques étrangers, si vous le savez à l'interne,
3 mettons, que ça provient d'un acteur étatique étranger, c'est
4 quoi la collaboration que vous avez avec les autres agences
5 de renseignement, ou les agences de renseignement de
6 sécurité? Est-ce que c'est une collaboration accrue dans ces
7 circonstances-là ou qu'est-ce qui se passe?

8 **M. DAVID VATCHER:** Oui, absolument. Donc,
9 les campagnes... par exemple, les campagnes d'hameçonnage sont
10 presque quotidiennes, mais certaines campagnes par des états
11 vont être plus sophistiquées, étant donné le temps et
12 l'argent qu'ils ont à mettre là-dedans. Et puis, vont être
13 beaucoup plus ciblées.

14 Donc, à ce moment-là, nous, quand on détecte
15 qu'il s'agit en effet d'une puissance étrangère qui voudrait
16 nuire à nos opérations ou nous soutirer de l'information
17 quelconque, on agit avec... on rentre en communication avec nos
18 collègues, bien sûr, sur la colline parlementaire, mais aussi
19 des agences du service canadien.

20 **Me GABRIEL POLIQUIN:** Et d'une manière
21 générale, est-ce que vous êtes satisfait de l'information que
22 vous obtenez des agences pour faire votre travail en matière
23 de cybersécurité?

24 **M. DAVID VATCHER:** Absolument. Ces agences-
25 là ont le bien-être de notre appareil à cœur, donc vont
26 communiquer les bonnes informations au bon moment pour nous
27 aider à éviter les dégâts.

28 **Me GABRIEL POLIQUIN:** D'accord. Merci. On

1 va se tourner maintenant vers un incident spécifique qui est
2 un peu pour la Commission, un cas d'étude, si on veut, d'une
3 cyberattaque qui a fait l'objet d'une couverture médiatique.
4 On parle de l'incident APT31. Je vais donc aborder ce sujet-
5 là. C'est une attaque qui a eu lieu, comme on le sait, en
6 janvier 2021. Vous étiez en poste à cette époque-là?

7 **M. DAVID VATCHER:** Oui.

8 **Me GABRIEL POLIQUIN:** Donc, il est indiqué
9 aux paragraphes 27 et 28 du résumé d'entrevue. On l'a ici,
10 donc, vous pouvez y tourner, tant qu'à faire. Simplement
11 pour nous mettre en contexte. Donc, c'est la direction des
12 services... si vous voulez décrire vous-même l'incident APT31,
13 qu'est-ce qui s'est passé?

14 **M. DAVID VATCHER:** Donc, à la fin janvier
15 2021, on a été mis au courant par nos collègues de la Chambre
16 des communes qu'une tentative d'harponnage était en cours.
17 Ce qu'il faut comprendre, c'est que, comme je disais tout à
18 l'heure, l'hameçonnage, on en voit tous les jours.
19 L'harponnage est moins fréquent parce que l'harponnage est
20 plus ciblé.

21 **Me GABRIEL POLIQUIN:** Mais pourriez-vous
22 décrire la différence entre hameçonnage pis harponnage, juste
23 pour qu'on comprenne?

24 **M. DAVID VATCHER:** L'hameçonnage... ben, on va
25 utiliser les termes de pêche. Donc, l'hameçonnage, c'est
26 vraiment, je lance plusieurs lignes à l'eau et j'espère qu'un
27 poisson va mordre.

28 **Me GABRIEL POLIQUIN:** OK.

1 **M. DAVID VATCHER:** Ça, c'est l'hameçonnage.
2 Et puis, le but de l'hameçonnage, c'est rediriger une
3 personne pour que soit elle installe un maliciel sur son
4 poste ou qu'elle saisisse ses informations personnelles, ses
5 accès sur un site de mon choix. Ça, c'est l'hameçonnage, qui
6 utilise souvent l'usurpation d'identité. Un transporteur de
7 colis qui vous dit que votre colis est en retard, par
8 exemple, c'est de l'hameçonnage. C'est envoyé à des
9 centaines, peut-être des milliers de personnes.

10 L'harponnage est différent. Harponnage, en
11 anglais, *spear fishing*, c'est qu'on vise vraiment quelqu'un.
12 Et puis cette personne-là, on va écrire un message avec des
13 informations qui ont été obtenues ailleurs pour aller tenter,
14 une fois de plus, d'aller chercher de l'information ou, une
15 fois de plus, installer un maliciel. Mais, c'est vraiment
16 plus ciblé. Je n'envoie pas des messages d'harponnage à tout
17 le monde, je l'envoie à ces trois personnes, huit personnes
18 que je vise.

19 **Me GABRIEL POLIQUIN:** D'accord. Puis, APT31,
20 c'était une attaque d'hameçonnage?

21 **M. DAVID VATCHER:** Pardon?

22 **Me GABRIEL POLIQUIN:** APT31, c'était une
23 attaque de quel genre?

24 **M. DAVID VATCHER:** Harponnage.

25 **Me GABRIEL POLIQUIN:** Harponnage, OK. Donc,
26 plus ciblé.

27 **M. DAVID VATCHER:** Plus ciblé.

28 **Me GABRIEL POLIQUIN:** D'accord. Donc, en

1 janvier 2021, on se replace là, que saviez-vous de cette
2 attaque-là, à ce moment-là?

3 **M. DAVID VATCHER:** Tout ce qu'on savait,
4 c'est qu'il y avait des drôles de courriels qui rentraient.
5 Et puis que certains de nos parlementaires pourraient être
6 visés ou ciblés par une tentative d'harponnage.

7 **Me GABRIEL POLIQUIN:** Est-ce que c'est une
8 attaque que vous aviez déjà détectée ou est-ce que c'est le
9 message du centre de cybersécurité qui vous a alerté?

10 **M. DAVID VATCHER:** Nos collègues de la
11 Chambre des communes nous ont alertés.

12 **Me GABRIEL POLIQUIN:** Ah.

13 **M. DAVID VATCHER:** Et puis, nous, nos outils
14 avaient déjà détecté certains des courriels de la campagne et
15 les avait mis de côté. Et puis nous, ce qu'on a fait, c'est
16 qu'on est entrés directement et immédiatement en contact avec
17 les bureaux de sénateurs qui étaient ciblés pour nous assurer
18 que l'ensemble des messages soient détruits.

19 **Me GABRIEL POLIQUIN:** Donc, en janvier 2021...

20 **COMMISSAIRE HOGUE:** J'ai juste une question.

21 **Me GABRIEL POLIQUIN:** Oui.

22 **COMMISSAIRE HOGUE:** Quand vous dites que vous
23 les avez mis de côté, je comprends que c'est mis en
24 quarantaine quand on est avisé qu'un courriel est en
25 quarantaine, on a un certain délai pour aller voir si c'est...
26 c'est ça que vous avez fait? Donc, ça ne se rend pas, en
27 principe, ça ne se rend pas dans la boîte de réception
28 lorsqu'ils sont mis de côté de la personne à qui c'est

1 destiné, à laquelle c'est destiné?

2 **M. DAVID VATCHER:** Exactement. Donc, dans
3 certains cas, l'outil le fait par lui-même. L'outil va
4 détecter que, à cause de différentes caractéristiques, ce
5 message-là est du... soit du *spam* ou, plus sérieusement, est
6 potentiellement dangereux, donc, va le mettre de côté.

7 Notre politique interne au Sénat est de faire
8 en sorte que nous ne détruisons aucun courriel adressé à un
9 sénateur. On les met de côté. Après ça, on peut les appeler
10 et leur dire : il y a ce courriel-là qu'on a mis là pour
11 vous. On veut vous aviser que c'est potentiellement une
12 attaque. Puis on souhaiterait l'effacer avec votre
13 permission.

14 **COMMISSAIRE HOGUE:** D'accord.

15 **Me GABRIEL POLIQUIN:** Puis pour faire un lien
16 avec la réponse à cette question-là, vous avez mentionné tout
17 à l'heure que le hameçonnage, l'harponnage, c'est des choses
18 qui arrivent tous les jours. Donc, est-ce que pour chacun
19 des courriels que vous recevez de cette nature-là, vous
20 avisez le sénateur en question?

21 **M. DAVID VATCHER:** Non. L'hameçonnage est
22 presque quotidien. L'harponnage est plus rare.

23 **Me GABRIEL POLIQUIN:** OK.

24 **M. DAVID VATCHER:** Ce qui demande plus
25 d'efforts.

26 **Me GABRIEL POLIQUIN:** Donc, même question,
27 mais par rapport au hameçonnage. Donc, vous recevez des
28 courriels de hameçonnage, est-ce que vous alertez les

1 sénateurs?

2 **M. DAVID VATCHER:** Nous allons aviser le
3 sénateur - si ça vient à nos oreilles bien entendu là - nous
4 allons aviser les sénateurs visés de cette campagne de
5 l'hameçonnage-là.

6 **Me GABRIEL POLIQUIN:** D'accord. Et...

7 **COMMISSAIRE HOGUE:** Lorsque c'est de
8 l'hameçonnage, j'imagine que vous pouvez faire un avis
9 général...

10 **M. DAVID VATCHER:** Absolument.

11 **COMMISSAIRE HOGUE:** ... à l'ensemble des
12 sénateurs?

13 **M. DAVID VATCHER:** Absolument.

14 **COMMISSAIRE HOGUE:** Disant « Tel type de
15 courriel circule. Ne l'ouvrez pas », bon, blablabla. Alors
16 que quand c'est de l'harponnage, vous allez communiquer avec
17 les sénateurs sur une base individuelle parce qu'ils sont
18 spécifiquement visés?

19 **M. DAVID VATCHER:** Absolument.

20 **COMMISSAIRE HOGUE:** D'accord.

21 **Me GABRIEL POLIQUIN:** D'accord. Donc, pour
22 venir au fait de l'APT 31, je crois comprendre de votre
23 résumé d'entrevue que certains messages auraient
24 effectivement abouti dans les boîtes de réception des
25 sénateurs, c'est exact?

26 **M. DAVID VATCHER:** Oui. Oui.

27 **Me GABRIEL POLIQUIN:** D'accord. Puis
28 d'autres auraient pas abouti, c'est ça?

1 **M. DAVID VATCHER:** Exact.

2 **Me GABRIEL POLIQUIN:** Ils auraient été captés
3 par ce qu'on appelle des pare-feu, c'est ça?

4 **M. DAVID VATCHER:** Par des outils de... oui.

5 **Me GABRIEL POLIQUIN:** J'ai peut-être pas le
6 bon vocabulaire.

7 **M. DAVID VATCHER:** De protection. Non, c'est
8 pas grave. C'est beau.

9 **Me GABRIEL POLIQUIN:** Donc, des outils de
10 protection généralisés.

11 **M. DAVID VATCHER:** Voilà.

12 **Me GABRIEL POLIQUIN:** D'accord. Puis... donc,
13 est-ce que des messages ont été envoyés aux sénateurs peu
14 importe si le courriel avait été capté par les outils de
15 protection? Ou vous avez contacté seulement les sénateurs
16 qui ont reçu bel et bien le courriel?

17 **M. DAVID VATCHER:** Nous avons contacté tous
18 les sénateurs qui avaient été ciblés.

19 **Me GABRIEL POLIQUIN:** D'accord.

20 **M. DAVID VATCHER:** Parce qu'une attaque
21 d'harponnage pourrait arriver en deux vagues, en trois
22 vagues. Donc, on... la sensibilisation de nos clients est
23 notre meilleur outil de protection au Sénat. Donc, quand un
24 sénateur ou une sénatrice sait qu'il ou elle est la cible
25 d'une attaque, donc, sa réaction est d'autant plus méfiante
26 envers, bien entendu. Et puis, c'est vraiment notre meilleur
27 outil là, la sensibilisation.

28 **Me GABRIEL POLIQUIN:** D'accord. Pis ça, vous

1 saviez à cette époque-là... ben, vous saviez en janvier ou
2 février 2021 que des sénateurs avaient été... avaient reçu ces
3 courriels-là?

4 **M. DAVID VATCHER:** Nous savions que certains
5 sénateurs avaient été la cible d'une campagne d'harponnage.

6 **Me GABRIEL POLIQUIN:** D'accord. Puis est-ce
7 que vous saviez à ce moment-là - encore là, janvier-février
8 2021 - que c'était un acteur étatique qui était derrière
9 cette campagne-là?

10 **M. DAVID VATCHER:** Non.

11 **Me GABRIEL POLIQUIN:** Non. Quand est-ce que
12 vous l'avez su?

13 **M. DAVID VATCHER:** Je l'ai su, je vous dirais
14 avril ou mai de cette année lorsque ça a été publié dans les
15 journaux.

16 **Me GABRIEL POLIQUIN:** Vous l'avez su par les
17 journaux?

18 **M. DAVID VATCHER:** Je l'ai su par... oui. Par
19 des... oui.

20 **Me GABRIEL POLIQUIN:** Puis est-ce que, encore
21 là, cette information-là aurait été utile à savoir en
22 janvier-février 2021?

23 **M. DAVID VATCHER:** Pas vraiment, parce que
24 comme je vous expliquais plus tôt, la menace, peu importe qui
25 fait la menace, la menace va être traitée directement et de
26 manière immédiate, une fois que ça vient à nos oreilles, bien
27 entendu. Qu'elle vienne d'un groupe de malfaiteurs qui
28 tentent de subtiliser de l'argent ou d'un état quelconque, on

1 veut vraiment éliminer la menace.

2 COMISSAIRE HOGUE: Fait que votre réaction à
3 vous, c'est la même?

4 M. DAVID VATCHER: Oui. Éliminer la menace.

5 COMISSAIRE HOGUE: Il y a pas de distinction
6 selon l'identité de l'acteur qui est derrière cette attaque-
7 là?

8 M. DAVID VATCHER: Aucune. Nous, ce qu'on
9 fait, c'est qu'il y a une menace, on s'occupe de la menace.
10 Après, peut-être qu'on fera des... on aura des communications
11 avec des collègues de sécurité pour déterminer d'où venait la
12 menace. On leur fournira les informations dont eux ont
13 besoin pour les aider à identifier ça, parce qu'on est des
14 collaborateurs dans ce sens-là, parce qu'on veut la
15 protection non seulement du Sénat, mais aussi de la Chambre
16 des communes et de tout l'appareil gouvernemental canadien.
17 Donc, nous, on est des bons collaborateurs dans ce sens-là.

18 COMISSAIRE HOGUE: Est-ce que les échanges
19 ont eu lieu? Parce qu'on voit que l'attaque a eu lieu en
20 janvier 2021, pis vous dites c'est cette année en... je pense
21 vous avez dit avril ou mai là.

22 M. DAVID VATCHER: Oui.

23 COMISSAIRE HOGUE: Donc, 2024 que vous
24 apprenez qui est derrière cette attaque-là. Est-ce que par
25 ailleurs, entre 2021 et 2024, il y a eu ce type d'échange-là
26 pour essayer de comprendre d'où cette attaque-là était venue
27 ou c'était tellement une parmi d'autres qu'il n'y avait pas
28 de...

1 **M. DAVID VATCHER:** C'était une parmi
2 d'autres, et nous n'avons pas eu de suivi quant à l'attaque
3 précise au Sénat. On n'a pas eu de suivi ni de nos collègues
4 de la Chambre, ni d'une instance gouvernementale quelconque.
5 C'est vraiment au moins d'avril-mai de cette année que
6 l'affaire est devenue plus publique et qu'un lien avec le
7 groupe APT31 a été fait.

8 **COMMISSAIRE HOGUE:** Et ça, même si c'était de
9 l'harponnage par opposition à de l'hameçonnage,

10 **M. DAVID VATCHER:** Oui.

11 **COMMISSAIRE HOGUE:** ... parce que vous avez dit
12 il y a moins souvent de l'harponnage...

13 **M. DAVID VATCHER:** Oui.

14 **COMMISSAIRE HOGUE:** ... ça change rien au fait
15 que c'était quand même une parmi... une tentative d'harponnage
16 parmi plusieurs?

17 **M. DAVID VATCHER:** Comme d'autres, oui.

18 **COMMISSAIRE HOGUE:** C'est ça, il y en a
19 d'autres.

20 **M. DAVID VATCHER:** Souvent, l'harponnage, ce
21 n'est pas un état, mais un groupe bien organisé qui veut
22 tenter de nous subtiliser de l'argent, souvent de manière
23 très maladroite là.

24 **COMMISSAIRE HOGUE:** Ceux qui se trompent dans
25 la façon d'épeler les mots qui apparaissent sur les
26 courriels?

27 **M. DAVID VATCHER:** Entre autres. Il y a des
28 choses qui sautent aux yeux des fois, heureusement. Mais les

1 attaques sont de plus en plus sophistiquées et de bonne
2 qualité, je dirais. Donc, la sensibilisation pis la
3 formation de nos parlementaires, entre autres, mais aussi de
4 nos employés au Sénat est notre première ligne de défense.

5 **Me GABRIEL POLIQUIN:** D'accord. Puis depuis
6 l'attaque APT31... depuis que vous savez que c'était un acteur
7 étatique, est-ce qu'il y a des mesures additionnelles ou des
8 mesures différentes qui auraient été prises pour faire face à
9 ce genre d'attaque-là dans le futur?

10 **M. DAVID VATCHER:** Non. Il est certain que
11 nous, on a des communications, comme je disais, avec des
12 partenaires externes. Et puis, étant donné que... qu'on veut
13 tous la même chose, on s'assure de rester à l'affut si jamais
14 il y avait d'autres menaces là.

15 **COMMISSAIRE HOGUE:** Et une fois que vous avez
16 su que c'était APT31 qui était derrière cette attaque-là,
17 est-ce que vous avez, vous, communiqué avec les sénateurs qui
18 avaient fait l'objet d'harponnage pour les informer de ça?
19 Ben, probablement qu'ils l'ont su aussi en lisant les
20 journaux, mais avez-vous communiqué avec eux pour en discuter
21 ou il y a pas eu de suivi non plus à cet égard?

22 **M. DAVID VATCHER:** Je n'ai pas communiqué
23 avec eux. Par contre, j'ai répondu à un des sénateurs qui
24 m'a posé des questions sur comment ça avait été traité. J'ai
25 répondu qu'on avait éliminé le risque pis qu'il n'y avait
26 aucune brèche d'information, aucune... il y avait eu aucun
27 succès relié à cette attaque-là. Puis, c'est la fin de cette
28 attaque-là pour nous.

1 **COMMISSAIRE HOGUE:** D'accord.

2 **Me GABRIEL POLIQUIN:** Je suis à court de
3 temps, mais je vais vous laisser l'opportunité. Est-ce qu'il
4 y a d'autres choses que vous voudriez... dont vous voudriez
5 informer la Commission au sujet de l'ingérence étrangère dans
6 vos disciplines particulières au Sénat?

7 **Mme JULIE LACROIX:** Non.

8 **COMMISSAIRE HOGUE:** Moi, j'ai une question et
9 si vous ne pouvez pas y répondre, je vous invite à me le
10 dire. Sentez-vous pas mal à l'aise parce que c'est moi qui
11 pose la question là.

12 Sur la base de ce que vous pouvez voir comme
13 information, est-ce que vous diriez que les attaques
14 auxquelles le Sénat fait face proviennent fréquemment
15 d'acteurs étrangers? Et j'entends des états ou des agents
16 qui agissent pour l'état, ou est-ce que c'est quelque chose
17 qui demeure marginal et peu fréquent? Où est-ce qu'on se
18 situe? Autrement dit, dans le nombre d'attaques, je
19 comprends que vous en avez un grand nombre quotidiennement,
20 il y a des attaques, des cyberattaques, est-ce que la
21 présence d'états étrangers est un phénomène important?

22 **M. DAVID VATCHER:** Merci de votre question.
23 En termes de quantité, les attaques d'acteurs étrangers, ou
24 qui représentent ou qui sont sympathiques à un gouvernement
25 étranger, augmentent mais représentent une minorité des
26 attaques auxquelles on fait face. Parce que ce sont souvent
27 les tentatives de rançongiciel et ainsi de suite, parce qu'il
28 y a de l'argent à faire que les gens s'essaient plus. Il y a

1 des firmes qui existent dans d'autres pays qui font
2 uniquement que ça.

3 Par contre, je crois qu'on est... nous vivons
4 dans un climat géopolitique... je veux pas aller trop loin,
5 mais on vit dans un climat géopolitique tendu, et puis il
6 serait fou de ne pas croire que ces attaques-là vont
7 continuer d'augmenter en nombre et en sophistication.

8 **COMMISSAIRE HOGUE:** Alors, est-ce que ça
9 serait exact de dire, actuellement - chez vous, on parle
10 simplement du Sénat - il y a pas péril en la demeure là, en
11 ce sens que ça demeure quelque chose qui est relativement
12 modeste et contrôlé, mais que vous assistez à une montée de
13 ces attaques-là de la part d'états étrangers ou d'agents
14 d'états étrangers? Vous constatez une augmentation?

15 **M. DAVID VATCHER:** Je suis pas sûr que je
16 veux répondre à ça.

17 **COMMISSAIRE HOGUE:** Parfait. J'arrête. Vous
18 avez rien à ajouter, Madame Lacroix?

19 **Mme JULIE LACROIX:** Non.

20 **COMMISSAIRE HOGUE:** Merci.

21 **Me GABRIEL POLIQUIN:** Merci. Ce sont mes
22 questions. Merci aux témoins.

23 **COMMISSAIRE HOGUE:** Alors, contre-
24 interrogatoire laissez-moi juste trouver ma feuille. Voilà.
25 Alors, le premier, ça sera Maitre Choudhry pour... qui
26 représente Jenny Kwan.

27 **--- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR**

28 **MR. SUJIT CHOUDHRY:**

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

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

4 **MR. SUJIT CHOUDHRY:** Not a problem. Okay.
5 Great. Thanks. So I'd like to just ask you -- for the
6 record, I'm -- my name is Sujit Choudhry and I represent
7 Jenny Kwan, member of Parliament.

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

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

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

15 « Quoi qu'il en soit le fait de
16 connaitre la source de l'attaque plus
17 tôt n'aurait pas changé la réponse
18 rapide de la Direction des services
19 d'information. »

20 And so that's your evidence; correct?

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

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

1 **MR. DAVID VATCHER:** Right.

2 **MR. SUJIT CHOUDHRY:** So suppose when you
3 became aware of the attack back in January 2021, at that
4 time, you had also become aware that the attack was from
5 APT31. I know you didn't learn that until June 2024, but
6 let's imagine you learned at that time or soon thereafter.
7 And so the question I have is this, in addition to informing
8 the offices of the relevant senators that there had been an
9 attack, would you also have informed them that the attack had
10 come from APT31?

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

13 **MR. SUJIT CHOUDHRY:** Sure.

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

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

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

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

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

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

28 **MR. DAVID VATCHER:** I think I would first

1 have raised it to my superiors, and, ultimately, that
2 decision to warn senators, or to mention it to senators would
3 have been taken by our CIBA steering members.

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

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

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

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

16 **MR. DAVID VATCHER:** Correct.

17 **MR. SUJIT CHOUDHRY:** Who then would have been
18 able to decide whether to disclose. Ms. Lacroix, did you
19 want to -- you're nodding. Did you want to add something to
20 that?

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

27 **MR. SUJIT CHOUDHRY:** So that's helpful. So
28 maybe I'll just want to -- Madam Commissioner, how much more

1 time do I have?

2 **COMMISSIONER HOGUE:** You have another five
3 minutes.

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

7 **COMMISSIONER HOGUE:** Thanks.

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

27 **MS. JULIE LACROIX:** Correct. Our job is to
28 ensure the safety and security of the senate and senators as

1 a whole, and to balance any mitigation measures we have with
2 their requirements and need to -- needs in order to execute
3 their parliamentary functions.

4 MR. DAVID VATCHER: I ---

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

6 MR. DAVID VATCHER: --- I would add that I am
7 not an expert on ---

8 MR. SUJIT CHOUDHRY: Sure

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

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

25 --- EXHIBIT No./PIÈCE No. JKW0000169:

26 Senate Procedure - Chapter 11

27 Privileges and Immunities

28 MR. SUJIT CHOUDHRY: Anyway, thank you for

1 your time. Have a good day.

2 COMMISSIONER HOGUE: Thank you.

3 Mr. Harland for Michael Chong.

4 --- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR

5 MR. FRASER HARLAND:

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

13 « La Direction des services
14 d'information savait seulement que
15 les logiciels avaient été envoyés par
16 courriel. »

17 No, paragraph 30, sorry.

18 « La Direction des services
19 d'information a appris en juin 2024
20 de l'équipe de sécurité des TI de la
21 Chambre des communes que l'attaque
22 avait été menée par APT31. »

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

25 MR. DAVID VATCHER: Correct.

26 MR. FRASER HARLAND: And were you informed by
27 CSIS or by any other government department that APT31 was
28 responsible for ---

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

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

7 **MR. DAVID VATCHER:** Correct. So in May or
8 June of this year, I did not reach out to the senators who
9 were targeted by the attack in January 2021; however, I did
10 respond to questions from one of the senators to their
11 satisfaction.

12 **MR. FRASER HARLAND:** Okay. And Mr. Choudhry
13 mentioned MP MacKay and MP Genius, who were very clear that
14 they want to be informed of incidents like this. Would it be
15 fair to say that that would also be true for senators?

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

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

21 **MR. DAVID VATCHER:** I think that senators
22 always want to be informed, and at the same times, I think
23 that senators receive a lot of information, and there's -- I
24 mean, I'm completely transparent, and when asked by senators
25 to provide more information, I always do. And if that -- if
26 there was a ruling by CIBA steering to that effect, I would,
27 of course, comply. I'm not trying to hide anything from
28 anybody. I'm just -- this was -- this attack happened two-

1 and-a-half years ago. It was thwarted. There was no damage.
2 So I would leave it to senators to ask me if they wish to
3 have any more information. I mean, I have no issue with
4 that.

5 **MR. FRASER HARLAND:** Understood. That's very
6 helpful. So do I understand that there's not a policy or
7 directive in place from that steering committee to inform
8 senators of attacks like the APT31 incident?

9 **MR. DAVID VATCHER:** For a spearfishing attack
10 like that, I do not have -- that only attacked a small
11 minority of senators. I do not have that requirement.
12 However, that attack was made available in our quarterly
13 reports on cyber security, which are internal documents.

14 **MR. FRASER HARLAND:** But in that -- so what
15 we and the Commission are most interested in is that this was
16 an attack from a foreign state. So that's the part -- was
17 that known in that -- made known in that document? Or just
18 that it was a spearfishing attack?

19 **MR. DAVID VATCHER:** In 2021 it was made known
20 that it was a spearfishing attack. And recently, we updated,
21 of course, accordingly with the knowledge that we gained.

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

26 **MR. DAVID VATCHER:** What I will say is that
27 should the events occur once more, the result would be the
28 same.

1 **MR. FRASER HARLAND:** Okay. Those are my
2 questions. Thank you, Commissioner.

3 **COMMISSIONER HOGUE:** Thank you.

4 Ms. Teich for the Human Rights Coalition.

5 **--- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR**

6 **MS. SARAH TEICH:**

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

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

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

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

24 **MR. DAVID VATCHER:** There are a lot of ifs in
25 your question.

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

27 **MR. DAVID VATCHER:** I'm not sure what to
28 reply to your question because in fact, it was an

1 unsuccessful attack against a handful of senators. We made
2 sure that all of their devices were not compromised as part
3 of our routine verifications. And so your question is --
4 calls for me to speculate, and I don't think I should.

5 **MS. SARAH TEICH:** Okay. I appreciate that.
6 I'm not asking particularly about the APT31 attack. I'm
7 speaking generally, just, you know, using your expertise.
8 But I appreciate that your focus is on senators.

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

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

19 **MS. SARAH TEICH:** Why not?

20 **MR. DAVID VATCHER:** The Senate is an
21 independent institution and I do not believe that external
22 government entities should manage security for our devices.

23 **MS. SARAH TEICH:** Okay. If not the Senate
24 administration, would it be valuable for another agency to
25 offer that kind of support?

26 **MR. DAVID VATCHER:** I don't see why. Why
27 would it be -- I'm sorry.

28 **MS. SARAH TEICH:** Sorry, maybe I'm not being

1 clear. Not to senators, but to potentially the contacts of
2 senators, who may have their devices compromised as a result
3 of the attack on senators?

4 **MR. DAVID VATCHER:** I'm -- I don't know what
5 to answer to that.

6 **MS. SARAH TEICH:** Okay. Those are my
7 questions. Thank you.

8 **COMMISSIONER HOGUE:** Thank you.

9 Next one is Maitre Sirois for the RCDA.

10 **--- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR**

11 **Me GUILLAUME SIROIS :**

12 **Me GUILLAUME SIROIS:** Bonjour. Guillaume
13 Sirois, avocat de l'Alliance démocratique des Canadiens
14 russes.

15 J'aimerais qu'on montre WIT 126, la version
16 française, s'il vous plait. Le paragraphe 24.

17 J'aimerais juste parler brièvement de
18 l'attaque de déni de service distribuée qu'il y a eu lieu...
19 qui a été attribué à des sympathisants de la Russie.
20 J'aimerais comprendre davantage les circonstances entourant
21 cette attaque. Quand avez-vous été mis au courant que le
22 site Internet du Sénat avait été attaqué par des
23 sympathisants russes?

24 **M. DAVID VATCHER:** Il y a eu plus d'une
25 instance de ce type d'attaque là de déni de service sur notre
26 site externe. À chaque fois, nous... on a des outils, bien
27 entendu, qui surveillent le nombre de connexions à nos sites
28 externes. Et puis lorsqu'il y a une anomalie, ça m'est

1 rapporté et nous prenons les actions nécessaires pour contrer
2 l'attaque. Donc, c'est... je vous dirais que c'est
3 presque immédiatement que c'est porté à mon attention, je n'ai
4 pas de date à vous donner puisque ça arrive régulièrement ou
5 de temps en temps.

6 **Me GUILLAUME SIROIS:** Avez-vous l'année, le
7 mois?

8 **M. DAVID VATCHER:** Pas avec moi, je suis
9 désolé. J'ai pas le...

10 **Me GUILLAUME SIROIS:** Et une fois que vous
11 avez été mis presque immédiatement au courant de cette
12 attaque-là, c'est quand que vous avez appris que ça avait été
13 mené par des sympathisants russes particulièrement?

14 **M. DAVID VATCHER:** La façon dont les attaques
15 sont perpétrées, il y a des composantes technologiques... des
16 spécificités qui nous aident à identifier la source de
17 l'attaque, mais aussi, les groupes... certains groupes sont
18 très vocals sur les réseaux sociaux et se vantent et
19 confirment un peu... se vantent de ces attaques-là.

20 **Me GUILLAUME SIROIS:** Pis en termes de délai,
21 comme... c'est un peu ce que j'ai vu dans votre résumé
22 d'entrevue, mais plutôt en termes de délai, c'est quoi...
23 combien de temps que ça a pris entre le moment que vous avez
24 été informé que le site Internet du Sénat avait été attaqué,
25 qui était fermé, et le moment que vous avez appris... que ce
26 soit pas les médias sociaux ou par des informations
27 technologiques que cette attaque-là avait été menée par des
28 sympathisants de la Russie. Est-ce qu'il y avait un délai

1 entre les deux?

2 **M. DAVID VATCHER:** C'est très... il y a pas
3 grand temps. Il y a pas grande différence entre les deux.
4 Donc, on sait qu'il y a une attaque qui est en cours. On
5 sait si ça ressemble beaucoup à l'attaque précédente qui a
6 des caractéristiques que nous connaissons qui sont techniques
7 et dans lesquelles je n'entrerai pas. Et puis ces
8 caractéristiques-là nous portent à croire qu'il s'agit d'un
9 groupe précis. C'est presque immédiatement, dans le fond.

10 **Me GUILLAUME SIROIS:** Et la réponse du Sénat
11 dans ce contexte-là, l'administration du Sénat dans ce
12 contexte-là est la même quand on apprend presque immédiatement
13 que c'est des sympathisants de la Russie qui sont derrière...
14 ou d'un état étranger qui sont derrière une attaque que si on
15 a aucune indication qu'un état étranger est derrière une
16 attaque. C'est la même réponse de la part du Sénat, c'est
17 ça?

18 **M. DAVID VATCHER:** Absolument.

19 **Me GUILLAUME SIROIS:** Et je comprends que de
20 contacter les partenaires en sécurité et renseignement, c'est
21 pas nécessairement utile pour le Sénat lui-même. Mais
22 pensez-vous que de les contacter, les informer que vous êtes
23 au courant de ce genre d'attaque-là pourrait être utile pour
24 leur travail à eux?

25 **M. DAVID VATCHER:** Eux le savent déjà.

26 **Me GUILLAUME SIROIS:** Comment vous savez
27 qu'ils le savent si vous êtes pas en contact avec eux à ce
28 moment-là?

1 **M. DAVID VATCHER:** Les attaques contre des
2 institutions du gouvernement canadien sont publiques, dans le
3 fond. Dans le sens où ces ressortissants-là s'en vantent et
4 puis on s'en cache pas. Donc, nous, on sait quand elles
5 surviennent, mais vous avez raison, je crois qu'ils le
6 savent. Je n'en ai pas la preuve. Vous avez raison là-
7 dessus.

8 **Me GUILLAUME SIROIS:** Et juste pour finir,
9 pensez-vous que certaines informations que vous avez en votre
10 possession, parce que vous êtes la victime de l'attaque en
11 tant que tel, qu'une certaine information pourrait être utile
12 pour eux pour continuer leur enquête et essayer de peut-être
13 mettre des mesures de représailles ou quoi que ce soit.

14 **M. DAVID VATCHER:** Absolument. Et puis je
15 voudrais pas faire croire que nous ne discutons pas de ces
16 attaques-là avec eux. Des membres de mon équipe travaillent
17 avec ces entités externes et puis je ne serais pas surpris
18 que ces attaques-là aient été mentionnées, cependant, lors de
19 l'attaque, je ne suis pas certain... je ne crois pas que nous
20 communiquons avec eux pour leur dire « Attention, tel groupe
21 nous attaque aujourd'hui ».

22 **Me GABRIEL POLIQUIN:** D'accord. Merci. Mon
23 temps est terminé, mais je vous remercie pour votre temps
24 aujourd'hui.

25 **COMMISSAIRE HOGUE:** Merci.

26 J'ai juste une question. Quand vous dites
27 qu'ils... les groupes qui attaquent comme ça vont généralement
28 s'en vanter sur les réseaux sociaux, est-ce qu'il y a des

1 revendications d'attaques proprement dites?

2 M. DAVID VATCHER: Absolument.

3 COMMISSAIRE HOGUE: Alors, les groupes vont
4 revendiquer que ce sont eux qui ont mené une attaque donnée?

5 M. DAVID VATCHER: Absolument.

6 COMMISSAIRE HOGUE: OK. Merci.

7 Alors, the Concern Group. Mr. Chantler.

8 --- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR

9 MR. NEIL CHANTLER:

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

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

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

23 And you're aware, and you describe at
24 paragraph 67 of your interview summary, that this motion was
25 introduced last spring following the release of the Special
26 Report on Foreign Interference released by the National
27 Security and Intelligence Committee of parliamentarians,
28 NSICOP. You're aware of that and you've stated it in your

1 interview summaries; correct?

2 MR. DAVID VATCHER: I'm sorry, ---

3 MS. JULIE LACROIX: We're aware in general
4 terms. Correct.

5 MR. DAVID VATCHER: Yes.

6 MR. NEIL CHANTLER: Okay. And that report
7 reported on intelligence that suggests there are
8 parliamentarians who are witting participants in efforts of
9 foreign states to interfere with our democracy. You're aware
10 of that general finding? Either of you.

11 COMMISSIONER HOGUE: Are you?

12 MS. JULIE LACROIX: No, I think for specifics
13 on this motion, you would need to direct the questions to
14 either the Standing Committee on Ethics and Conflicts of
15 Interest or Senator Sainte-Germain.

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

18 MR. DAVID VATCHER: I'm ---

19 MS. JULIE LACROIX: I'm not aware.

20 MR. DAVID VATCHER: I'm sorry. I'm not
21 aware.

22 MR. NEIL CHANTLER: You're not aware that
23 that committee found there are witting participants among
24 parliamentarians in assisting foreign states?

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

26 MR. NEIL CHANTLER: And you're not aware of
27 news reports that have reported on these very significant
28 allegations?

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

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

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

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

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

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

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

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

25 **MR. DAVID VATCHER:** Yeah.

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

28 **MR. NEIL CHANTLER:** Well you both undergo --

1 or I apologize, the CSD undergoes a process of risk
2 assessment, ---

3 MS. JULIE LACROIX: Yes.

4 MR. NEIL CHANTLER: --- you help to educate a
5 senator prior to travel on the risks of that foreign country,
6 you provide information about how to be safe in the foreign
7 country, you give advice on best practices, on how to use
8 electronic devices, and so on. And you'd both agree that
9 those are critically important -- that's critically important
10 information for a senator to have before ---

11 MS. JULIE LACROIX: Yes.

12 MR. NEIL CHANTLER: --- undergoing a trip
13 like that?

14 MS. JULIE LACROIX: Yeah.

15 MR. NEIL CHANTLER: And when a senator
16 accepts sponsored foreign travel, often it's the foreign
17 state or a foreign interest group that is paying for that
18 travel and making the arrangements for the senator? Is that
19 correct?

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

21 MR. NEIL CHANTLER: I mean, by its very
22 nature, the sponsored travel is being paid for by a foreign
23 entity?

24 MR. DAVID VATCHER: That would be the
25 definition of a sponsored trip.

26 MR. NEIL CHANTLER: Right. And in
27 circumstances like that, would you agree that there's a
28 heightened risk to the safety and security of the travelling

1 senator, perhaps heightened risks of espionage, entrapment,
2 and other forms of foreign interference?

3 **MS. JULIE LACROIX:** I would agree in general
4 terms that throughout the assessment, those are all
5 considerations that will form part of the assessment and
6 mitigation measures put in place.

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

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

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

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

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

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

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

23 **MS. JULIE LACROIX:** No.

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

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

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

28 **COMMISSIONER HOGUE:** Thank you.

1 AG.

2 **--- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR**

3 **MS. RYANN ATKINS:**

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

6 You note in your witness statement that the
7 senate administration collaborates quite closely with the
8 sergeant-at-arms of the House of Commons. Is that right?

9 **MS. JULIE LACROIX:** Correct.

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

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

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

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

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

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

23 **MS. RYANN ATKINS:** And you share information
24 about cyber attacks?

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

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

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

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

4 **MR. DAVID VATCHER:** Correct.

5 **MS. RYANN ATKINS:** And the relationship
6 between the Senate and the House of Commons is such that you
7 would expect that if the House of Commons received
8 information that was relevant to your IT systems or the
9 protection of senators, that they would share that
10 information with you?

11 **MR. DAVID VATCHER:** Absolutely.

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

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

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

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

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

23 **MS. JULIE LACROIX:** Correct.

24 **MS. RYANN ATKINS:** Okay. I want to talk to
25 you about the cyber incident in January 2021 by the threat
26 actor known as APT31. And you noted in your testimony that
27 this incident was not successful, the attack was thwarted.
28 Correct?

1 **MR. DAVID VATCHER:** Correct.

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

4 **MR. DAVID VATCHER:** Yes.

5 **MS. RYANN ATKINS:** And am I correct that your
6 team would have been responsible for linking the IP addresses
7 of the systems that were attacked to the specific Senators
8 that were being targeted?

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

10 **MS. RYANN ATKINS:** Okay. And so to put it
11 another way, the security agencies may have had the IP
12 addresses, but it was your team who would have identified the
13 specific Senators.

14 **MR. DAVID VATCHER:** Correct.

15 **MS. RYANN ATKINS:** And did you receive
16 consent from the Senators to share their names with CSE or
17 any other government agency?

18 **MR. DAVID VATCHER:** At that point, we were
19 informed that -- we were informed which parliamentarians were
20 already targeted, so we didn't share that information; that
21 information was given to us.

22 **MS. RYANN ATKINS:** By the House of Commons?

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

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

27 **MR. DAVID VATCHER:** No, but once again, it
28 was shared with us. We didn't share it; it was shared with

1 us.

2 **MS. RYANN ATKINS:** Okay. But sitting here
3 today you don't know if the House of Commons shared that
4 information with government agencies?

5 **MR. DAVID VATCHER:** I do not.

6 **MS. RYANN ATKINS:** Okay. And the Cyber
7 Centre -- you note in your summary that the Cyber Centre
8 didn't provide any information to the Senate Administration
9 about who might have been behind the attacks. Did the House
10 of Commons relay that information to you?

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

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

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

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

24 **MR. DAVID VATCHER:** No.

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

28 **MR. DAVID VATCHER:** Please let me rephrase;

1 nobody from my Directorate attended that meeting. I don't
2 know, I can't speak for other Directorates.

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

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

6 **MS. RYANN ATKINS:** Okay. And following that
7 meeting, did anyone from the House of Commons share with you
8 the information that was relayed at that meeting?

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

10 **MS. RYANN ATKINS:** Okay. The House of
11 Commons -- I anticipate we're going to hear that the House of
12 Commons relayed to the security agencies that some of its
13 members, members of Parliament, may have received similar
14 messages on their personal email addresses. Did the House of
15 Commons deliver that same message to the Senate?

16 **MR. DAVID VATCHER:** I don't remember that
17 they did.

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

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

23 **MS. RYANN ATKINS:** Okay.

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

27 **MS. RYANN ATKINS:** Is that part of the
28 general advice and training on cyber security that Senators

1 receive?

2 **MR. DAVID VATCHER:** Yes.

3 **MS. RYANN ATKINS:** Thank you. Those are my
4 questions.

5 **COMMISSIONER HOGUE:** Thank you.

6 For the Senate it's Maître Roy and Maître
7 Clair, avez-vous des questions?

8 **Me MARC-ANDRÉ ROY:** Non, Madame la
9 commissaire.

10 **COMMISSAIRE HOGUE:** Pas de questions?

11 We'll resume ---

12 Réinterrogatoire, Maitre Poliquin?

13 **Me GABRIEL POLIQUIN:** Madame la Commissaire,
14 j'ai pas de questions en réinterrogatoire; cependant, je veux
15 juste préciser que Me Choudhry avait identifié un décalage
16 dans les paragraphes...

17 **COMMISSAIRE HOGUE:** Oui.

18 **Me GABRIEL POLIQUIN:** ...du résumé d'entrevue.
19 En fait, c'est... y'a pas d'erreurs substantielles là, c'est
20 juste que dans la version anglaise, le paragraphe 26 n'a pas
21 son numéro, ce qui explique le décalage des... dans la
22 numérotation des paragraphes, mais pas dans la substance.

23 **COMMISSAIRE HOGUE:** Alors, l'ensemble de
24 l'information est là.

25 **Me GABRIEL POLIQUIN:** C'est ça.

26 **COMMISSAIRE HOGUE:** Merci beaucoup.

27 **Me GABRIEL POLIQUIN:** Merci.

28 **COMMISSAIRE HOGUE:** Bonne journée. Vous êtes

1 libres de quitter.

2 **COMMISSAIRE HOGUE:** Merci.

3 Alors, on va prendre la pause 20 minutes.

4 Alors, we'll resume at 11:15.

5 **THE REGISTRAR:** Order, please. À l'ordre,
6 s'il vous plaît.

7 The sitting of the Commission is now in
8 recess until 11:15 a.m. Cette séance de la commission est
9 maintenant suspendue jusqu'à 11 h 15.

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

11 --- La séance est suspendue à 10 h 55

12 --- Upon resuming at 11:18 a.m./

13 --- La séance est reprise à 11 h 18

14 **THE REGISTRAR:** Order, please. À l'ordre,
15 s'il vous plaît.

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 11:18 a.m. Il est 11 h 18.

21 **COMMISSIONER HOGUE:** Bonjour.

22 **MR. HAMZA MOHAMADHOSSEN:** Commissioner.

23 For the record, it's Hamza Mohamadhossen for
24 the Commission.

25 Commissioner, the witnesses before you are
26 representatives from the House of Commons, Mr. Patrick
27 McDonnell and Me Benoît Dicaire.

28 Mr. Registrar, I would ask that both

1 witnesses please be sworn.

2 **THE REGISTRAR:** We'll start with Mr.
3 McDonald. Could you please state your full name and then
4 please spell your last name for the record?

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

7 **--- MR. PATRICK EWEN McDONELL, Affirmed/Sous affirmation**
8 **solennelle:**

9 **THE REGISTRAR:** Thank you.
10 Now, I'll proceed with Mr. Dicaire. Could
11 you please state your full name and spell your last name for
12 the record?

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

15 **--- MR. BENOÎT EUGÈNE DICAIRE, Affirmed/Sous affirmation**
16 **solennelle:**

17 **THE REGISTRAR:** Thank you, Mr. Dicaire.
18 Counsel, you may proceed.

19 **--- EXAMINATION IN-CHIEF BY/INTERROGATOIRE EN-CHEF**

20 **MR. HAMZA MOHAMADHOSSEN:**

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

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

25 **MR. HAMZA MOHAMADHOSSEN:** And a summary was
26 generated following that interview?

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

28 **MR. HAMZA MOHAMADHOSSEN:** Court Operator,

1 could we please pull up document WIT128.BIL, please? And the
2 document on screen is the summary that was generated from
3 your interview?

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

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

7 **MR. PATRICK McDONELL:** I had that opportunity
8 to review it, yes.

9 **MR. HAMZA MOHAMADHOSSEN:** And do you have any
10 corrections, additions, or any other modifications to make
11 today?

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

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

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

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

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

21 **MR. BENOÎT DICAIRE:** Twenty twenty-four
22 (2024)?

23 **MR. HAMZA MOHAMADHOSSEN:** Twenty Twenty-four
24 (2024).

25 **MR. BENOÎT DICAIRE:** Yes, I do.

26 **MR. HAMZA MOHAMADHOSSEN:** And the document on
27 screen is the summary that was generated from your interview
28 with Commission counsel?

1 MR. BENOÎT DICAIRE: Yeah.

2 MR. HAMZA MOHAMADHOSSEN: And you've reviewed
3 the summary for accuracy?

4 MR. BENOÎT DICAIRE: I did.

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

7 MR. BENOÎT DICAIRE: I don't.

8 MR. HAMZA MOHAMADHOSSEN: And do you adopt
9 the contents of the witness summary as part of your evidence
10 before the Commission?

11 MR. BENOÎT DICAIRE: I do.

12 MR. HAMZA MOHAMADHOSSEN: Thank you.

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

19 **--- EXHIBIT No./PIÈCE No. WIT0000128.EN:**

20 Interview Summary: House of Commons
21 Administration (Patrick McDonell and
22 Benoît Dicaire)

23 **--- EXHIBIT No./PIÈCE No. WIT0000128.BIL:**

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

27 **--- EXHIBIT No./PIÈCE No. WIT0000128.FR:**

28 Résumé d'entrevue : Administration de

1 la Chambre des communes (Patrick
2 McDonnell et Benoît Dicaire)

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

6 **MR. BENOÎT DICAIRE:** Correct.

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

9 **MR. BENOÎT DICAIRE:** Correct.

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

13 **MR. BENOÎT DICAIRE:** I did.

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

17 **MR. BENOÎT DICAIRE:** No.

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

21 **MR. BENOÎT DICAIRE:** Yes.

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

23 For the record, the French version of this
24 summary is at WIT129.FR, and both versions will be entered
25 into evidence as the next two exhibits.

26 **--- EXHIBIT No./PIÈCE No. WIT0000129.EN:**

27 Appendix to Interview Summary: House
28 of Commons Administration (Hedi

Touati and Benoît Dicaire)

--- EXHIBIT No./PIÈCE No. WIT0000129.FR:

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

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

MR. BENOÎT DICAIRE: Correct.

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

MR. BENOÎT DICAIRE: Correct.

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

MR. BENOÎT DICAIRE: Yes.

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

MR. BENOÎT DICAIRE: We do.

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

--- EXHIBIT No./PIÈCE No. HOC0000001.EN:

1 Institutional Report of the House of
2 Commons Administration

3 --- EXHIBIT No./PIÈCE No. HOC0000001.FR:

4 Rapport institutionnel de
5 l'administration de la Chambre des
6 Communes

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

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

17 **MR. PATRICK McDONELL:** I'm the Sergeant-at-
18 Arms at the House of Commons, and also oversee corporate
19 security.

20 **MR. HAMZA MOHAMADHOSSEN:** Can you please
21 describe the responsibilities associated with those two
22 roles?

23 **MR. PATRICK McDONELL:** Sergeant-at-Arms role
24 is for the most part ceremonial. And the Corporate Security,
25 we oversee the safety and security of members of Parliament
26 off the hill.

27 **MR. HAMZA MOHAMADHOSSEN:** Okay. Before you
28 joined the House of Commons, can you provide us with a brief

1 overview of your professional experiences?

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

12 **MR. HAMZA MOHAMADHOSSEN:** Right. In your
13 interview summary you referenced the Parliamentary Protective
14 Services. Can you explain how the responsibilities of the
15 Parliamentary Protective Service differs from your
16 responsibilities when it comes to ensuring the safety of MPs?

17 **MR. PATRICK McDONELL:** Parliamentary
18 Protective Service is responsible for the security of MPs,
19 staff, employees, contractors, volunteers, anyone who comes
20 into the Parliamentary precinct, they are responsible for
21 their physical security.

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

24 **MR. PATRICK McDONELL:** Basically, beyond the
25 Wellington Wall and out in the communities. So I provide
26 residential security, constituency security, mobile duress
27 alarms, open source -- we do open-source intelligence,
28 technical surveillance countermeasures.

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

4 **MR. PATRICK McDONELL:** The Director of the
5 PPC is a Chief Superintendent in the Royal Canadian Mounted
6 Police.

7 **MR. HAMZA MOHAMADHOSSEN:** Perfect. Thank
8 you.

9 Mr. Dicaire, what is your current role at the
10 House of Commons?

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

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

15 **MR. BENOÎT DICAIRE:** So I oversee a team
16 that's responsible for the IT infrastructure, the
17 applications, the broadcasts, webcast infrastructure, and
18 also our real property group and facilities group.

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

22 **MR. BENOÎT DICAIRE:** I've been an employee of
23 the House of Commons since October 2000, so 24 years. And
24 I've been responsible for various roles throughout this
25 tenure, namely as a DG of applications and also as a Director
26 of IT Infrastructure before.

27 **MR. HAMZA MOHAMADHOSSEN:** Okay. Thank you.
28 I'd like to focus in a bit on physical

1 security. So most of these questions will be directed to
2 you, Mr. McDonnell.

3 Are there any teams under your supervision
4 that are either dedicated or engage with foreign interference
5 issues?

6 **MR. PATRICK McDONELL:** Yes. There would be
7 the RMI, Risk Management Investigators. They work hand in
8 hand with CSIS and the RCMP. There is my Technical
9 Surveillance Countermeasures team.

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

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

13 **MR. HAMZA MOHAMADHOSSEN:** Right. Can you
14 describe a little bit about the open-source monitoring
15 program?

16 **MR. PATRICK McDONELL:** The open-source
17 monitoring program is a team of analysts that scan the
18 internet using various software for threats against --
19 threats and harassment of members of Parliament.

20 **MR. HAMZA MOHAMADHOSSEN:** Right. Do they
21 receive support or information from other teams internal to
22 the House of Commons?

23 **MR. PATRICK McDONELL:** Yes, they do. From
24 the Risk Management Investigators.

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

27 **MR. PATRICK McDONELL:** The Risk Management
28 Investigative team works hand in hand with CSIS. They

1 regularly meet once a month.

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

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

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

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

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

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

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

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

27 **MR. PATRICK McDONELL:** --- through an email
28 or Facebook, people using their image fraudulently. But we

1 converse with the MP in question ---

2 MR. HAMZA MOHAMADHOSSEN: Right.

3 MR. PATRICK McDONELL: --- and the Whip's
4 Office also.

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

7 MR. PATRICK McDONELL: In most cases, yes.

8 MR. HAMZA MOHAMADHOSSEN: Okay. And does
9 that also include the House Leader? The MP's House Leader?

10 MR. PATRICK McDONELL: No, we'll go to the
11 respective Whips.

12 MR. HAMZA MOHAMADHOSSEN: Okay.

13 MR. PATRICK McDONELL: Yeah.

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

17 MR. PATRICK McDONELL: Daily.

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

22 MR. PATRICK McDONELL: Okay. As I mentioned
23 earlier, we have a residential security program, both for
24 their primary and secondary residence.

25 MR. HAMZA MOHAMADHOSSEN: By secondary
26 residence, you're referring to what, exactly?

27 MR. PATRICK McDONELL: Their secondary
28 residence would be here in Ottawa. It doesn't cover a

1 cottage or anything. It's -- when they travel to Ottawa,
2 many stay in apartments. Some stay in hotels.

3 MR. HAMZA MOHAMADHOSSEN: M'hm.

4 MR. PATRICK McDONELL: I don't know if any
5 own a house in Ottawa, ---

6 MR. HAMZA MOHAMADHOSSEN: Right.

7 MR. PATRICK McDONELL: --- but the secondary
8 residence refers to the geographical area of Ottawa and
9 Gatineau.

10 MR. HAMZA MOHAMADHOSSEN: Great.

11 MR. PATRICK McDONELL: Constituency office
12 security. Some MPs have more than one constituency office.

13 MR. HAMZA MOHAMADHOSSEN: M'hm.

14 MR. PATRICK McDONELL: We provide members of
15 Parliament with mobile duress alarms, ---

16 MR. HAMZA MOHAMADHOSSEN: M'hm.

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

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

26 MR. HAMZA MOHAMADHOSSEN: M'hm.

27 MR. PATRICK McDONELL: If the MP wants to be
28 escorted to their place of residence in the Ottawa area.

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

2 **MR. PATRICK McDONELL:** --- PPS will provide
3 that.

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

6 **MR. PATRICK McDONELL:** No, that's entirely
7 PPS.

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

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

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

12 **MR. PATRICK McDONELL:** And we also provide
13 event security if an MP is attending an event and requests
14 security at an event in relation to their parliamentary
15 duties, we'll provide security at that event and their
16 constituency.

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

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

21 **MR. HAMZA MOHAMADHOSSEN:** Okay.

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

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

26 You indicate at paragraph 49 of your summary,
27 and I'm not going to bring it up, but if it's helpful, let me
28 know and I will call it. You indicate that your office is

1 responsible for conducting security screening of House of
2 Commons personnel and staff. When you're referring to House
3 of Commons personnel and staff, can you describe who would be
4 captured by that security screening?

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

9 **MR. HAMZA MOHAMADHOSSEN:** So those working in
10 the offices of MPs? Is that what you mean by political
11 staff?

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

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

16 **MR. PATRICK McDONELL:** They're -- no, they're
17 MP employees.

18 **MR. HAMZA MOHAMADHOSSEN:** They're MP
19 employees.

20 **MR. PATRICK McDONELL:** They're hired by the
21 MP.

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

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

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

1 **MR. PATRICK McDONELL:** Security screening
2 looks like a criminal background check ---

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

4 **MR. PATRICK McDONELL:** --- and loyalty to
5 Canada check.

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

7 **MR. PATRICK McDONELL:** So the criminal
8 background check is done through the Royal Canadian Mounted
9 Police ---

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

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

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

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

21 **MR. HAMZA MOHAMADHOSSEN:** And that's handled
22 entirely by CSIS?

23 **MR. PATRICK McDONELL:** CSIS handles it.
24 Sometimes -- yeah, it's handled by CSIS and then there's --
25 it goes into CSIS often because the person has spent some
26 period of time within the last five years outside of Canada,
27 ---

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

1 **MR. PATRICK McDONELL:** --- it could be
2 someone new to Canada, or a Canadian citizen, so CSIS will
3 investigate that period of time.

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

5 **MR. PATRICK McDONELL:** CSIS may interview the
6 individual. CSIS may come back to us and say it's -- they
7 haven't reached a conclusion and they recommend that we
8 interview the person on a resolution of doubt interview.

9 **MR. HAMZA MOHAMADHOSSEN:** Okay. And can you
10 explain a little bit what that resolution of doubt interview
11 ---

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

18 **MR. HAMZA MOHAMADHOSSEN:** Okay. I think you
19 mentioned that you were originally appointed sergeant-at-arms
20 back in 2019?

21 **MR. PATRICK McDONELL:** Yes.

22 **MR. HAMZA MOHAMADHOSSEN:** How has the use of
23 resolution of doubt interviews changed over time?

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

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

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

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

1 **MR. PATRICK McDONELL:** Yeah, thank you. It's
2 increased significantly. I believe in 2019 we did --
3 conducted 10 resolution of doubt interviews. And in 2023,
4 128, ---

5 **MR. HAMZA MOHAMADHOSSEN:** Okay.

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

7 **MR. HAMZA MOHAMADHOSSEN:** Yeah. And these
8 interviews, is there a threshold for conducting the
9 interviews, or is it only when CSIS indicates there's a need
10 for an interview?

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

18 **MR. HAMZA MOHAMADHOSSEN:** Okay. And at the
19 end of this process, what is the output -- what is the
20 outcome?

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

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

24 **MR. PATRICK McDONELL:** --- whether to move
25 forward and give the applicant access and accreditation, ---

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

27 **MR. PATRICK McDONELL:** --- or to refuse.

28 **MR. HAMZA MOHAMADHOSSEN:** And when you say

1 access, that's access to what exactly?

2 MR. PATRICK McDONELL: That would be access
3 to our buildings and our network.

4 MR. HAMZA MOHAMADHOSSEN: Okay. Let's say
5 there's -- let's say that you decide not to grant
6 accreditation.

7 MR. PATRICK McDONELL: M'hm.

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

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

12 MR. HAMZA MOHAMADHOSSEN: By they, you are
13 referring to who?

14 MR. PATRICK McDONELL: The applicant.

15 MR. HAMZA MOHAMADHOSSEN: The applicant.
16 Okay.

17 MR. PATRICK McDONELL: Yeah. If I refuse.
18 Yeah.

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

21 MR. PATRICK McDONELL: I meet with them, yes,
22 ---

23 MR. HAMZA MOHAMADHOSSEN: Okay.

24 MR. PATRICK McDONELL: --- and discuss it.

25 MR. HAMZA MOHAMADHOSSEN: Okay. Referring
26 generally to the screening process, where does your team
27 obtain the information required to conduct the screenings?

28 MR. PATRICK McDONELL: Overall, if we're

1 going into a resolution of doubt interview, we'll take the
2 information either received from the Royal Canadian Mounted
3 Police and/or CSIS ---

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

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

7 **MR. HAMZA MOHAMADHOSSEN:** Okay. And does the
8 process of security screening, including the loyalty to
9 Canada investigation, the resolution interview, does that
10 entire process capture foreign interference concerns?

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

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

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

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

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

23 **MR. HAMZA MOHAMADHOSSEN:** --- threat
24 themselves.

25 **MR. PATRICK McDONELL:** --- we'd make them
26 aware.

27 **MR. HAMZA MOHAMADHOSSEN:** And in some
28 instances the Party whips ---

1 **MR. PATRICK McDONELL:** Yes.

2 **MR. HAMZA MOHAMADHOSSEN:** --- also the RCMP.

3 In the event that there are security concerns relating to
4 staffers, to political staffers in an MP's office, who would
5 you notify regarding these concerns?

6 **MR. PATRICK McDONELL:** Well, the staffer and
7 the MP and the whip. And that has happened, and we've had,
8 you know, meetings, the staffer, the whip, the MP, myself,
9 and discussed the way forward.

10 **MR. HAMZA MOHAMADHOSSEN:** Okay. And would
11 you ever communicate your concerns to external agencies?

12 **MR. PATRICK McDONELL:** Only agencies that
13 could assist in the investigation of the possible offence.

14 **MR. HAMZA MOHAMADHOSSEN:** Thank you. These
15 are my questions. Mtre. Poliquin will carry on with the rest
16 of the examination.

17 **COMMISSIONER HOGUE:** Thank you.

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

19 **--- EXAMINATION IN-CHIEF/EXAMINATION EN-CHEF PAR**

20 **MR. GABRIEL POLIQUIN:**

21 **MR. GABRIEL POLIQUIN:** Just I'll get set up
22 here. Turns out I had water.

23 Good morning. Just for the record, Gabriel
24 Poliquin for the Commission. So I'll take over from Mr.
25 Mohamadhossen on the relationships with government entities.
26 We've talked a little bit about it already in terms of
27 specific examples when you collaborate with the RCMP or with
28 CSE and so on, but I'd like to take it to a more formal level

1 and talk about formal agreements that the House of Commons
2 has with various security and intelligence agencies. And
3 I'll start with you, Mr. McDonell. I understand from
4 paragraph 24 of the witness summary -- we could actually pull
5 that up, Mr. Court Operator, just so we have it before us,
6 paragraph 24.

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

10 **MR. PATRICK McDONELL:** The MOU with CSIS and
11 the RCMP, the purpose of both of those MOUs is the sharing of
12 information.

13 **MR. GABRIEL POLIQUIN:** Okay. And does that
14 MOU provide for anything about foreign interference
15 specifically?

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

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

22 **MR. PATRICK McDONELL:** --- foreign
23 interference.

24 **MR. GABRIEL POLIQUIN:** Very well. And then
25 at paragraph 24 it's also mentioned that there's an MOU with
26 Privy Council, if you could elaborate on that, please?

27 **MR. PATRICK McDONELL:** Yeah, so I have an MOU
28 with Privy Council and that has to do with technical

1 surveillance countermeasures. We assist them in the
2 provision of those service -- and those services for caucus
3 meetings and possibly other meetings where they require that
4 service.

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

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

10 **MR. GABRIEL POLIQUIN:** Okay.

11 **MR. PATRICK McDONELL:** And the monitoring of
12 signals, cell phones in a room, Bluetooth, watches, whatever
13 may emit a signal.

14 **MR. GABRIEL POLIQUIN:** Right.

15 **MR. PATRICK McDONELL:** We'll monitor the
16 room.

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

22 **MR. PATRICK McDONELL:** CSIS, the RMI section,
23 which I had mentioned earlier, Risk Management Investigators,
24 they meet with CSIS once a month and discuss files of
25 interest, investigative techniques, latest trends, and then
26 operational files as they come forward. The RCMP, pretty
27 well talk to the RCMP every day.

28 **MR. GABRIEL POLIQUIN:** Okay. And this is

1 what you were referring to earlier, the exchanging
2 information about open-source intelligence, is that what
3 you're referring to?

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

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

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

24 **MR. GABRIEL POLIQUIN:** Okay. And you also
25 touch on the Deputy Minister Protection Committee. What's
26 that and what's ---

27 **MR. PATRICK McDONELL:** So the DM Protection
28 Committee is headed up by the NSIA, National Security

1 Intelligence Advisor to the Prime Minister, and it's a
2 community made up of DMs, Deputy Ministers, where the
3 protection of Ministers and parliamentarians is discussed.

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

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

17 **MR. GABRIEL POLIQUIN:** Okay.

18 **MR. BENOÎT DICAIRE:** So if there's an
19 incident.

20 **MR. GABRIEL POLIQUIN:** Very well. And what
21 about Shared Services Canada? That's touched on at paragraph
22 26 at the ---

23 **MR. BENOÎT DICAIRE:** Well, we have
24 independence from, we're not subject to Treasury Boards, so
25 we're not subject to Shared Services Canada, but we do
26 consume some services with them, so as a client, not as a
27 partner department. And I'm invited to some informal or
28 formal forum, communities of practice, CIO sharing, some of

1 their offerings, these types of scenarios.

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

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

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

16 **MR. BENOÎT DICAIRE:** Yeah, we manage our own
17 infrastructure for the -- and we also manage the
18 infrastructure for parliamentary partners.

19 **MR. GABRIEL POLIQUIN:** Okay. And who are
20 those parliamentary partners?

21 **MR. BENOÎT DICAIRE:** Well, the senate, the
22 library, the Ethics Commissioner, the PPS, officers of
23 parliament mostly.

24 **MR. GABRIEL POLIQUIN:** Okay. And if you
25 could explain for us laypersons, when you -- you manage the -
26 - I might not have the right term, but you manage the
27 network, what does that mean exactly?

28 **MR. BENOÎT DICAIRE:** Well, it's a common

1 infrastructure for the parliamentary partners that the House
2 supports. They are all independent. They own -- in the case
3 of the senate, they own their portion, but we manage it. And
4 in case of the rest of the institution, we manage pretty much
5 the perimeter and the network itself.

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

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

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

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

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

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

27 **MR. GABRIEL POLIQUIN:** Okay. And then to
28 what extent do you share that information that you receive

1 with Parliamentary partners? Does it happen at all?

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

6 **MR. GABRIEL POLIQUIN:** Okay. And so you
7 would relay that information received to the Senate, for
8 instance?

9 **MR. BENOÎT DICAIRE:** Yes.

10 **MR. GABRIEL POLIQUIN:** Okay. What happens if
11 that information is classified?

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

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

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

26 **MR. GABRIEL POLIQUIN:** Okay. Understood.
27 And again, we'll talk about that in more detail later on.

28 So when you -- so while we're on the topic,

1 talking specifically about information that you receive from
2 CSE, and again, just speaking very generally, if you could --
3 and again, not saying what that information is, but how is it
4 packaged? Like, what do you receive from CSE?

5 **MR. BENOÎT DICAIRE:** It's mostly technical
6 bulletins.

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

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

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

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

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

28 **MR. BENOÎT DICAIRE:** Yes, no, I think that we

1 have a strong collaboration with the Cyber Centre. It's
2 evolving over the years, as you know, as the cyber landscape
3 is evolving quite a bit. So there is definitely more
4 collaboration, more willingness to share, but again, around
5 the caveats assigned to, you know, our mandate, specifically.
6 So my specific mandate is to protect the infrastructure, and
7 protect members, and the continuity of Parliament. So they
8 have different mandates tied to intelligence and protecting
9 the Government of Canada and other types that are beyond my
10 mandate. So they share content based on what my mandate --
11 what they can share based on my mandate.

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

15 **MR. BENOÎT DICAIRE:** That's ---

16 **MR. GABRIEL POLIQUIN:** --- the House of
17 Commons ---

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

19 **MR. GABRIEL POLIQUIN:** --- infrastructure;
20 correct?

21 **MR. BENOÎT DICAIRE:** Correct.

22 **MR. GABRIEL POLIQUIN:** Okay. But in that
23 context, where they provide information that help you do your
24 job, to what extent does foreign interference come up? Do
25 you ever know, let's say, an attack is perpetrated by a
26 foreign actor?

27 **MR. BENOÎT DICAIRE:** Attacks are happening
28 very frequently and as you know, Parliament is a prime

1 target. So you can suspect that foreign actors are also
2 targeting the cyber infrastructure.

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

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

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

25 **MR. GABRIEL POLIQUIN:** Okay. And would you
26 say that when you do know that a threat is associated with a
27 foreign actor, is there -- you know, are -- is your posture
28 different, operationally?

1 **MR. BENOÎT DICAIRE:** It's very similar to --
2 yes, our posture would be different in those kinds of
3 scenarios because it depends on the risk level and it would
4 be very similar to when I'm treating a throne from the speech
5 -- a speech from the Throne, or a budget speech, these types
6 of scenarios where we -- the infrastructure is being taxed by
7 having more people consume, you know, these types of
8 services. So a spike in services might not be related
9 necessarily to a cyber attack, but might be related to an
10 important event happening at Parliament. So the same
11 resiliency concepts are applying. So monitoring, more
12 capacity management, these types of scenarios from an IT
13 infrastructure, with the objective of ensuring that the
14 infrastructure is resilient.

15 **MR. GABRIEL POLIQUIN:** Okay. So what I'm
16 hearing is that it is helpful to have that information. I
17 guess what I'm wondering is who determines when it's going to
18 be helpful? You know, like you say you have a spike in
19 activity, that's something that would change your operational
20 posture, foreign interference maybe as well. Can -- do you
21 have a mechanism for alerting the Cyber Centre, "Look, I need
22 to know whether this is a foreign actor because I'm seeing
23 something a little bit different"?

24 **MR. BENOÎT DICAIRE:** Yeah, so our
25 collaboration, I mean, they don't always know the scenario.
26 The collaboration is really broad. But at the same point in
27 time, the important factor is, you know, the continuity of
28 Parliament. And again, I'm kind of overstating the same

1 comment, but that's the reality here, is really my mandate is
2 really not to do intelligence gathering or these types of
3 scenarios. I'm really focused on continuity of Parliament
4 and allowing members to sit.

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

11 **MR. GABRIEL POLIQUIN:** Okay.

12 **MR. BENOÎT DICAIRE:** --- they couldn't share
13 it with us.

14 **MR. GABRIEL POLIQUIN:** Okay. Understood.
15 And while we're on that topic, so who in your unit has the
16 classification to what level?

17 **MR. BENOÎT DICAIRE:** A variety of staff have
18 the -- have different levels of clearances, depending on
19 their roles.

20 **MR. GABRIEL POLIQUIN:** Okay. So not all ---

21 **MR. BENOÎT DICAIRE:** It's really -- no, not
22 all of them, because it's really on a need-to-know basis
23 around that scenario.

24 **MR. GABRIEL POLIQUIN:** Okay. And before I
25 forget, Mr. McDonell, in your unit, who has -- what kind of
26 employees have security clearances, and what level?

27 **MR. PATRICK McDONELL:** Technical Surveillance
28 Countermeasures Team would be top secret. RMI, Risk

1 Management Investigations, top secret. And open-source
2 intelligence, top secret.

3 **MR. GABRIEL POLIQUIN:** Okay. That's helpful.

4 So going back to the topic of cyber attacks
5 and operational posture on that, I just want to make sure we
6 address that topic. And here I just want to give you an
7 opportunity to comment. We heard from members of Parliament
8 last week, Mr. MacKay and Mr. Genuis, who mentioned, you
9 know, their take on cyberattacks and one event in particular,
10 APT31, that we're going to cover in a minute. Mr. Genuis
11 mentioned that it would be useful in his view, to get
12 notification of cyberattacks when they've happened or if they
13 are about to happen. Just notification of cyberattacks, so
14 that MPs can better protect themselves. I just want to give
15 you an opportunity to comment. Is that -- from a practical
16 standpoint, what's your take on that?

17 **MR. BENOÎT DICAIRE:** Well, the scale of
18 things, as again, parliament is a prime target, we're dealing
19 in hundreds of millions of attack attempts in a year. So the
20 practicality of briefing everyone at every instance would
21 create a serious operational burden. And most of those are
22 thwarted by either controls in place, or by, you know,
23 infrastructures in place.

24 That being said, we take every attack
25 seriously, every attack attempt seriously, and should there
26 be any risk to members of Parliament, specifically their data
27 or their devices, we would and have, you know, communicated
28 with them.

1 **MR. GABRIEL POLIQUIN:** And so ---

2 **COMMISSIONER HOGUE:** And just a question, who
3 is making the decision to advise or not the MPs?

4 **MR. BENOÎT DICAIRE:** It depends on criteria.
5 I would say, you know, depending on the risk. Like, is the
6 threat dealt with? Is it still active? Is there a risk of
7 further contamination, or if there's a risk of further risks,
8 those things would escalate through our cyber security
9 program and the cyber -- the person responsible for cyber
10 security or Chief Information Security Officer and ultimately
11 would come to me, you know, around that.

12 But there's parameters that don't require
13 escalation. So if there's an imminent threat, or if there's
14 a threat that's ongoing, the protocol is to advise right away
15 and to action, because we're trying to contain the risk, and
16 trying to remedy the situation. So then the cyber team
17 directly from the ground up are dealing with the member's
18 office directly at that point.

19 **MR. GABRIEL POLIQUIN:** Okay. So just to sum
20 up, like, what's the threshold where you would advise an MP
21 that, you know, a cyber attack has occurred?

22 **MR. BENOÎT DICAIRE:** Every time there's an
23 impact on their -- on their information, or there's an impact
24 on their devices.

25 **MR. GABRIEL POLIQUIN:** Okay. And by impact,
26 what could that be?

27 **MR. BENOÎT DICAIRE:** Well, an attack has
28 succeeded or the mechanisms -- there's a risk, there's a

1 vulnerability that needs to be addressed, or there's a usage
2 pattern, there's been a user or someone in their office has
3 clicked something that have generated an action that, you
4 know, potentially puts the infrastructure at risk, or puts
5 their information at risk. These type of scenarios. Or so -
6 --

7 **MR. GABRIEL POLIQUIN:** Okay. And I want to
8 just understand it as a layperson, I'm sure as we all do.
9 But say an email is received by an MP or their staff, and
10 somebody's clicked on it and then thereby heightened their
11 risk. Do you know about that, like, do you know they've
12 clicked?

13 **MR. BENOÎT DICAIRE:** There's two or three
14 ways that we would know. One is through monitoring, so we --
15 if you've clicked on a malicious email then it would start
16 generating abnormal patterns. We would see that through our
17 monitoring approach. The second is we've implemented a
18 phishing button, so they can report a suspicious email to IT
19 security directly. And third, is some members or their staff
20 report directly to our IT service centre, so 24/7 they can
21 call and report that this email is suspicious, can you look
22 at it, can you -- so these are the three most common
23 scenarios where we're flagged.

24 **MR. GABRIEL POLIQUIN:** Okay. And are cyber
25 attacks sometimes flagged by external partners?

26 **MR. BENOÎT DICAIRE:** Yes, it could be if some
27 pattern would be seen. It depends on the visibility, again,
28 because the complexity of our infrastructure is that those

1 visibility points are not necessarily -- because of the
2 architecture, they don't see everything.

3 MR. GABRIEL POLIQUIN: Okay.

4 MR. BENOÎT DICAIRE: So they would see
5 abnormal patterns that are leaving the parliamentary network
6 or entering the parliamentary network. But when it comes to
7 the parliamentary network themselves, they don't have
8 visibility.

9 MR. GABRIEL POLIQUIN: Right.

10 MR. BENOÎT DICAIRE: So they work with our
11 cyber team.

12 MR. GABRIEL POLIQUIN: So to make sure I
13 understand, your unit sees what's going on within the House
14 of Commons framework, but an external partner such as CSE may
15 not. Is that correct?

16 MR. BENOÎT DICAIRE: Yes. If you -- I'm not
17 wanting to go very technical here but ---

18 MR. GABRIEL POLIQUIN: Sure. No, we don't.

19 MR. BENOÎT DICAIRE: You know, the reality is
20 what is displayed outside our network and what happens inside
21 our network, we have thousands of IP addresses that are not
22 necessarily exposed to outside world. So what they see, or
23 what somebody could see outside doesn't necessarily correlate
24 to the inside. So what we need to do is now make that
25 correlation between external data and internal data to really
26 understand the threat.

27 MR. GABRIEL POLIQUIN: Okay. And speaking of
28 visibility, while we're on that topic, it's my understanding

1 that MPs are provided with parliamentary phones and
2 computers, but that they may have their own as well. And in
3 terms of visibility, how do you -- can you know what's going
4 on on an MP's personal device?

5 **MR. BENOÎT DICAIRE:** So we have policies in
6 place, an IT security policy and acceptable use policies that
7 prevent them from conducting parliamentary business on
8 personal devices. So that's the one first thing, scenario.
9 So it's all HOC managed devices. So parliamentary business
10 is done on House of Commons ---

11 **MR. GABRIEL POLIQUIN:** I'm sorry, hot, HOC?

12 **MR. BENOÎT DICAIRE:** House of Commons.

13 **MR. GABRIEL POLIQUIN:** House of Commons,
14 sorry.

15 **MR. BENOÎT DICAIRE:** House of Commons devices
16 that are managed through our infrastructure to my team. So
17 that's the scenario around that. We do allow some guests'
18 devices if you want, so personal laptop would connect to a
19 different architecture, so it's a guest Wi-Fi architecture
20 that's secured. But we don't manage those devices, and we
21 don't monitor those devices. To connect to the
22 infrastructure, you need to have a house managed device.

23 **MR. GABRIEL POLIQUIN:** Okay. And so what
24 happens in a scenario where a personal device may have been
25 used for parliamentary business or not, is compromised.
26 What's your jurisdiction, so to speak?

27 **MR. BENOÎT DICAIRE:** Well, the infrastructure
28 supporting guests' connectivity, we still monitor that

1 portion. So if we see an abnormal pattern we would
2 interject, you know around that, potentially cut the access
3 and to remedy the impact potentially. But there's
4 segregation between, you know, our parliamentary network and
5 our guest network.

6 So there is these scenarios that there is
7 these controls in place in place to prevent, you know,
8 impacts, or mitigating impacts around some of those
9 scenarios. But if we have the visibility, if it's connected
10 -- if it's not connected to our guest network then I have
11 zero visibility.

12 **MR. GABRIEL POLIQUIN:** Okay.

13 **MR. BENOÎT DICAIRE:** If it's connected to our
14 guest network, then we have a possibility to see some
15 activity.

16 **MR. GABRIEL POLIQUIN:** Right. So if my
17 understanding is correct, say I bring my phone and it's not a
18 parliamentary phone, and I'm on the guest Wi-Fi at House of
19 Commons, and it's compromised by a phishing email or
20 something. Can that person come to your service and say,
21 "Look, what can I do about this?"

22 **MR. BENOÎT DICAIRE:** That would be -- we
23 wouldn't see that type of compromise because then you
24 wouldn't be on our email infrastructure. So to see a
25 phishing email it would have to go through the email
26 infrastructure we have.

27 So if you have a phone that's personal,
28 that's on Gmail, and there's a phishing email on Gmail, I

1 wouldn't have that visibility. I would see if the device is
2 exhibiting, you know, a pattern of trying to call out to a
3 malicious site, or a home base that is malicious, I would see
4 some of the traffic around that. But I wouldn't necessarily
5 see what the source of the issue is compared to a managed
6 system where we have more visibility.

7 **MR. GABRIEL POLIQUIN:** Right. And say we
8 accept you don't have visibility on a personal device, but as
9 an MP I know it's been compromised somehow and you know, I'm
10 having trouble with this. Can you help that person, can you
11 help that MP?

12 **MR. BENOÎT DICAIRE:** We would do best effort.
13 Our mandate is really tied to house managed devices, and
14 house information, and house infrastructure. So we truly
15 don't have a mandate for personal devices.

16 **MR. GABRIEL POLIQUIN:** Okay. So again, this
17 ties to points that were brought up by Mr. Genuis and Mr.
18 MacKay, you know, that sometimes, the difference between
19 Parliamentary work, electoral work, and personal matters,
20 sometimes gets blurry. So I know that there's a policy in
21 place that says, well, you know, your jurisdiction and your
22 visibility, your physical visibility anyway is limited to
23 your system.

24 But that, you know, that distinction gets
25 blurred, and can you do anything to help them if something
26 happens? Say an MP receives an email on their parliamentary
27 phone -- or on their personal phone from a constituent, it's
28 about an electoral matter, but the conversation is also about

1 a parliamentary matter.

2 MR. BENOÎT DICAIRE: Okay.

3 MR. GABRIEL POLIQUIN: Does that change
4 anything?

5 MR. BENOÎT DICAIRE: No, really the records
6 of visibility is -- where we have eyes, is the managed
7 devices.

8 MR. GABRIEL POLIQUIN: Yeah.

9 MR. BENOÎT DICAIRE: That's the
10 responsibility we have and that's the mandate we have. The
11 Acceptable Use Policy does provision that, you know, there
12 could be certain personal, you know, checking an email,
13 checking your bank system, or these types of scenarios, using
14 parliamentary devices, but the opposite doesn't really apply.
15 I don't have visibility on something that's a personal
16 device.

17 MR. GABRIEL POLIQUIN: Right.

18 MR. BENOÎT DICAIRE: In a scenario like Mr.
19 Genuis, I wouldn't have seen anything.

20 MR. GABRIEL POLIQUIN: Okay. Now I take it
21 some MPs have two different phones for two different
22 purposes. MPs might have just one phone that they do
23 everything on, maybe it's separate accounts, but it's on the
24 same phone. From a practical standpoint, you know, does
25 having two phones help your job? Having the same phone, does
26 that impede your job? Does it make any difference?

27 MR. BENOÎT DICAIRE: Well the bylaws are
28 pretty specific today and I'm not the right person to ---

1 **MR. GABRIEL POLIQUIN:** Right. And I'm not
2 asking you about the bylaws. I know that you can't comment
3 on, you know, the application of the policy, but, you know,
4 as a person who is responsible for ensuring the security, is
5 having just one phone, does that create an extra technical
6 vulnerability?

7 **MR. BENOÎT DICAIRE:** Like I said, our mandate
8 is really through the House managed devices, so whether
9 there's a personal phone or not in the equation, if somebody
10 has a different phone, ---

11 **MR. GABRIEL POLIQUIN:** Right.

12 **MR. BENOÎT DICAIRE:** --- it really doesn't
13 change my mandate. If they start using ---

14 **MR. GABRIEL POLIQUIN:** Okay. Say they do
15 everything from their parliamentary phone, ---

16 **MR. BENOÎT DICAIRE:** Yes.

17 **MR. GABRIEL POLIQUIN:** --- does that make any
18 difference? Does that ---

19 **MR. BENOÎT DICAIRE:** Well we would see more.
20 We would see -- but again, we -- the parliamentary phones are
21 there for parliamentary business.

22 **MR. GABRIEL POLIQUIN:** Okay.

23 **MR. BENOÎT DICAIRE:** That's the scope.

24 **MR. GABRIEL POLIQUIN:** Okay. I'll turn now
25 to a specific event that we all know now as the event
26 attributed to APT31. So that happened in January 2021. And
27 if you could remind us, Mr. Dicaire, how long you've been in
28 your role?

1 **MR. BENOÎT DICAIRE:** I started my position in
2 October 2023.

3 **MR. GABRIEL POLIQUIN:** Twenty twenty-three
4 (2023). Okay. So you weren't in that role when this attack
5 happened. But perhaps you can help us anyway in terms of
6 institutional response. The event came to light to the
7 public in June 2024, I believe. So what was your role in
8 respect to the response to that, institutional response of
9 the House of Commons to that?

10 **MR. BENOÎT DICAIRE:** So the cyber security
11 team would have -- so the knowledge I have from the gathering
12 that we've done and the extensive search that we've done, and
13 the interviews, and internally is indeed we collaborated with
14 the Cyber Centre in January 2021.

15 **MR. GABRIEL POLIQUIN:** M'hm. Okay.
16 Specifically to ---

17 **MR. BENOÎT DICAIRE:** Specific to an
18 information collecting campaign at the time. That was the
19 way it was earmarked.

20 **MR. GABRIEL POLIQUIN:** So you're saying that
21 the attack was an information collection campaign? Is that
22 your ---

23 **MR. BENOÎT DICAIRE:** That's the way it was
24 portrayed in 2021.

25 **MR. GABRIEL POLIQUIN:** Okay. And what else
26 can you tell us about that event and its repercussions from
27 the point of view of the House of Commons, you know, in as
28 much as you know about it from the information gathering

1 you've done?

2 **MR. BENOÎT DICAIRE:** At the time, you know,
3 from -- this was a very common attack vector, these types of
4 scenarios, and some of the information that was shared at the
5 time from the bulletins is that, you know, it was information
6 collecting. But it wasn't -- it was specifically said that
7 it wasn't malicious, or likely not malicious, I should say.

8 So again, when we have protocols in place,
9 when there's a bulletin that's provided to us, and there's
10 been several in that period of time in the first four or five
11 months of January to April, we collaborate, we collaborate
12 and provide as much information and -- but our mandate is
13 really, at this point in time, to always protect
14 parliamentarians and protect the infrastructure.

15 **MR. GABRIEL POLIQUIN:** Okay. If we could
16 pull a document, CAN.SUM27.1, please? Thank you.

17 So this is an annex to a topical summary
18 prepared by Government of Canada, being CAN.SUM27, which we
19 may refer to later on.

20 **--- EXHIBIT No./PIÈCE No. CAN.SUM.000027:**

21 PRC Email Operations Against
22 parliamentarians

23 **--- EXHIBIT No./PIÈCE No. CAN.SUM.000027.001:**

24 Tab A - Chronology of Events: Email
25 Tracking Link Campaign Targeting
26 Canadian parliamentarians

27 **MR. GABRIEL POLIQUIN:** This is a chronology
28 of events that relates to APT31. I know that this isn't your

1 document, but I have just some specific terminological
2 questions in association with that, just to help us
3 understand it.

4 If you could scroll down to February 3rd,
5 2021? Oh, February 3rd. Sorry. There we are. There we
6 are.

7 So just to summarize, the first few points
8 are about information that your unit has received from the
9 Cyber Centre. Is that correct?

10 **MR. BENOÎT DICAIRE:** Yeah.

11 **MR. GABRIEL POLIQUIN:** You're familiar with
12 this document?

13 **MR. BENOÎT DICAIRE:** Yeah. I'm familiar with
14 the document.

15 **MR. GABRIEL POLIQUIN:** Right. And so at
16 February 3rd, it says:

17 "The Cyber Centre Incident Handler
18 follows up to request feedback on
19 January 22nd report."

20 And says:

21 "The HoC Senior IT Security Analyst..."
22 So that person would be within your unit;
23 correct?

24 **MR. BENOÎT DICAIRE:** Yes.

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

26 "...responded to the Cyber Center
27 Incident Handler and indicated that
28 the issue was handled internally."

1 Now, again, I know you weren't there at the
2 time, but can you comment more generally, when we say
3 "handled internally", what does that mean?

4 **MR. BENOÎT DICAIRE:** Okay. So the current
5 protocol, and it's tied to our mandate, is the risk to
6 Parliament infrastructure, risk to parliamentary information,
7 or parliamentary devices. So if information is shared about
8 a possible attack, or possible attack vector, then our first
9 lens at this is really around how do we protect ourselves and
10 are we, you know, are we -- have we been breached or have we
11 been -- do we have to invoke our incident management
12 protocol?

13 So in this particular case, as we've
14 discussed in the past, you know, the investigation or the
15 lens that brought us there to say that it was handled
16 internally is that there was no more threat to -- there was
17 no threat. It was a combination of the investigation and the
18 assessment of the security analyst was that there was no
19 threat to the IT infrastructure.

20 **MR. GABRIEL POLIQUIN:** And when you say no
21 threat, does that mean no breach or is that something
22 different?

23 **MR. BENOÎT DICAIRE:** No breach at this point
24 in time, because in particular -- in this particular case,
25 with the parameters that were shared in the bulletin, they
26 were specifically asking for technical information based on a
27 very specific date range, from the 18th of January to the 21st
28 of January. So upon investigation with this information, we

1 noticed that the emails that were associated with those IP
2 addresses and the technical information never reached members
3 of Parliament. They were quarantined.

4 **MR. GABRIEL POLIQUIN:** Okay. I see.

5 So and just to confirm, if we could scroll
6 down a little bit to February 17th? I believe there are two
7 February 17th dates. Hold on. just scroll up, please.
8 Okay.

9 So just making sure that I have the right
10 reference.

11 Oh, if you could, yeah, scroll down to the
12 next 17th of February one?

13 Right. So the second paragraph there the:

14 "HoC director, IT Security, provided
15 the Cyber Centre's Incident
16 Management team with a printed
17 document containing a sample
18 malicious email and the names of
19 eight MPs who were intended
20 recipients of malicious emails."

21 So I've got a couple of questions about that.
22 You said earlier that the information you had was that it was
23 likely not malicious.

24 **MR. BENOÎT DICAIRE:** That's what the bulletin
25 indicated at the time.

26 **MR. GABRIEL POLIQUIN:** Okay. And so did that
27 change by February 17th?

28 **MR. BENOÎT DICAIRE:** No.

1 **MR. GABRIEL POLIQUIN:** Okay. And so of
2 course this may be a question for the folks who prepared this
3 document, but do you know why it says "malicious email" here?
4 And you may not.

5 **MR. BENOÎT DICAIRE:** Well the attack tactic
6 that was being advertised and wasn't necessarily said at that
7 point in time, but multiple -- you know, a year after the
8 bulletin, there was a bulletin in June 2022 that was way more
9 specific based on, you know, a year of information, but at
10 the time, we knew of the pattern that they were looking at in
11 this particular email, which was a method through a pixel
12 type of threat, meaning that through an embedded image, they
13 would trigger a collection of data that would be sent back to
14 this malicious ---

15 **MR. GABRIEL POLIQUIN:** And I guess that's
16 known as a pixel reconnaissance?

17 **MR. BENOÎT DICAIRE:** That's it.

18 **MR. GABRIEL POLIQUIN:** Something -- okay.

19 **MR. BENOÎT DICAIRE:** But in this case of the
20 House of Commons, we have protections at multiple levels. As
21 you know, our SITE cyber security program has proactive
22 measures and reactive measures, and one of those proactive
23 measures is disabling of downloading of images in email. So
24 they're not downloaded by default, they're prevented from
25 being opened. So specifically a user or a recipient would
26 have to go click to download that email. So by default that
27 that's not happening.

28 So -- but the fact that these emails never

1 reach -- that were part of that date range never reached the
2 MPs, you know, that's basically -- that's basically -- that's
3 an area. But the malicious email part, that was part of the
4 bulletin, it wasn't coming from us; a bulletin that indicated
5 likely not malicious, that's their documentation, our
6 partners.

7 **MR. GABRIEL POLIQUIN:** Okay. And maybe a
8 later assessment, but that's a question for them.

9 **MR. BENOÎT DICAIRE:** Yeah.

10 **MR. GABRIEL POLIQUIN:** Okay. I had two
11 questions, now I actually have three.

12 My second-to-last about that point, you
13 mentioned how when you see the email you'd have to click for
14 it -- for the malicious effects to kick in. So is that due
15 to a measure that's taken at the network level that, you
16 know, images aren't downloaded automatically?

17 **MR. BENOÎT DICAIRE:** It's a configuration
18 that we have through our email infrastructure, an email
19 security posture, if you want to call it. Email is one of
20 the biggest vector of threats, so we have a configuration
21 that is restricted that prevents those -- the likelihood of
22 those types of attacks being successful. It doesn't
23 eliminate them because I don't control the users.

24 **MR. GABRIEL POLIQUIN:** Somebody might click?

25 **MR. BENOÎT DICAIRE:** Some people might click.
26 So that's the scenario.

27 **MR. GABRIEL POLIQUIN:** Okay. And so that
28 measure of protection, is that something that users can opt

1 in and out of?

2 MR. BENOÎT DICAIRE: No.

3 MR. GABRIEL POLIQUIN: So it's a blanket
4 protection.

5 MR. BENOÎT DICAIRE: It is a protection
6 mechanism ---

7 MR. GABRIEL POLIQUIN: Okay.

8 MR. BENOÎT DICAIRE: --- built in for the
9 parliamentary email system.

10 MR. GABRIEL POLIQUIN: Okay. Taking a step
11 back before I get to my last question on that, so I don't
12 forget it, so does the House of Commons have -- and we'll get
13 to more detail on that in a minute, but do they have
14 briefings to MPs and other users on best practices for their
15 personal devices as well?

16 MR. BENOÎT DICAIRE: For the personal? So in
17 general as part of our IT security program we have an
18 awareness filler. So -- and it is a very effective mechanism
19 in terms of a defence tactic, right? So awareness around
20 users and behaviours in these types of scenarios. So over
21 the years so we send multiple bulletins; we call them Cyber
22 Vigilance Bulletin, and we do briefings at Caucus, and these
23 types of scenarios around best practices and different threat
24 factors, phishing, spear phishing, you know, ransomware, all
25 of these types of scenarios.

26 Some of our bulletins are actually
27 specifically talking about personal devices in some cases,
28 but they're in the spirit of parliamentary information. So

1 in 2023, you know, we change and approach it, if you're
2 trying to consume -- one of the bulletins specifically was
3 we've implemented multifactor identification, so if you're
4 trying to consume something on a parliamentary infrastructure
5 from outside as exposed to the internet, but with a personal
6 device and not your HOC device, then you would be challenged
7 for that second factor identification.

8 These are parameters that we put in place
9 here to protect parliamentary information that is accessible
10 outside of the privy of a parliamentary device.

11 **MR. GABRIEL POLIQUIN:** Right, okay.
12 Understood. And so this may be too specific of a question,
13 then, but just following up on that, as part of those
14 bulletins, do you include, you know, toggling on this
15 protection device of, you know, not downloading automatically
16 images that come through email; is that a piece of advice
17 that's transmitted in your bulletins?

18 **MR. BENOÎT DICAIRE:** I wouldn't have the
19 specific information about that particular case because
20 they're configurations -- there're some configurations that
21 are not behavioural based, such as that. It's -- but we do
22 have multiple parameters as part of our awareness campaign;
23 "Don't click on links," you know, "Assume that it's a
24 verified sender, somebody you would know," these type
25 scenarios are all best practice, so on prior to clicking.
26 And when in doubt, you now, use the phishing email, phishing
27 button to report it so we can verify it, or call us and we
28 can do that verification with you before you click.

1 So there's the best practices around
2 influencing that cyber safety, if you want, or safe
3 behaviours.

4 **MR. GABRIEL POLIQUIN:** Okay. And so turning
5 to my last question on this point, which I haven't forgotten,
6 it says here that there were eight MPS who were intended
7 recipients of malicious emails. And so if my understanding
8 is correct, those MPs did not receive -- like, let's put it
9 this way, those eight MPs, those emails did not end up in
10 their inboxes; is that correct?

11 **MR. BENOÎT DICAIRE:** That is correct. Our IT
12 security team reached out, though, to those eight MPs prior
13 to understanding -- this is happening very fast. So before
14 even confirming that those emails were quarantined, the cyber
15 team reached out to those eight MPs to see if they had
16 received anything in regards to that. So two members
17 acknowledged that they didn't receive anything, but they were
18 asking if -- should we need to -- we'll look out for it, type
19 of scenarios. But then it was easily determined, you know,
20 very rapidly afterwards that those emails were quarantined
21 and never reached for those particular date range.

22 **MR. GABRIEL POLIQUIN:** Okay. But you reached
23 out to them anyway.

24 **MR. BENOÎT DICAIRE:** We had reached out to
25 them, so there was an email that was sent the same day by the
26 security to the Members' mailbox.

27 **MR. GABRIEL POLIQUIN:** Okay. Thank you for
28 that.

1 Let's turn now briefly to the witness
2 summary, so WIT128, please. Okay, if you could scroll down
3 to paragraph 70, please? Seventy (70); seven zero, please.

4 So it's the third sentence from that
5 paragraph. Again, this paragraph pertains to February 17th,
6 which we've just discussed. The third sentence is:

7 "The original information they
8 received [that] related to MP IP
9 addresses, which they assessed had
10 not been compromised."

11 And we're talking about the -- just to be
12 clear, your unit.

13 **MR. BENOÎT DICAIRE:** M'hm.

14 **MR. GABRIEL POLIQUIN:** Right. So "He" being
15 you:

16 "He indicated that no contextual
17 information was shared in the report
18 received by CCCS, so they had no way
19 of knowing whether this was a state-
20 sponsored attack or otherwise."

21 And correct me if I'm wrong but this is at
22 the time of February 17th.

23 **MR. BENOÎT DICAIRE:** Correct.

24 **MR. GABRIEL POLIQUIN:** So when you say there
25 was no information in the report received by CCCS, just to
26 clarify, what report is that?

27 **MR. BENOÎT DICAIRE:** So this is the first
28 report that we received on January 22nd, 2021.

1 **MR. GABRIEL POLIQUIN:** And is that what you
2 referred to earlier as technical bulletins?

3 **MR. BENOÎT DICAIRE:** Yeah, it is -- I don't
4 know, it's called a Cyber Event Report.

5 **MR. GABRIEL POLIQUIN:** Okay. And just
6 speaking from, again, your general experience in this role, I
7 know you weren't there at the time, but is the knowledge that
8 an attack was state sponsored, does that make a difference in
9 your operational posture?

10 **MR. BENOÎT DICAIRE:** At the time it wouldn't
11 have because, again, the scenario is the same, right? Our
12 mandate is protecting the IT infrastructure and ensuring
13 that, you know, continuity of Parliament. So in that sense,
14 no. But, you know, in our renewed, you know, mandate and MOU
15 with -- that is just recently signed, you know, we're
16 focusing a lot more on the information-sharing aspect.

17 But, again, there's an evolution that needs
18 to happen because, again, there's clearances tied to access
19 to specific information. But there is a renewed
20 collaboration with our partners to ensure that, you know,
21 recommendations as far as bulletins are more accurate, or
22 contextual information would be given so that, you know, we
23 -- and it's mostly around how we work so that we can
24 collaborate more extensively on that -- on providing more
25 information, you know, while staying within our mandate.
26 Again, my team's mandate is not, you know, national security
27 and not necessarily intelligence. So we are happy to be good
28 collaborative partners, but there is an extent to which our

1 mandate, you know, takes us. But there is definitely, as
2 part of our MOU and as part of our organizations, both
3 organization, a willingness to provide more contextual
4 information based on, you know, the evolution of their own
5 mandate and the ministerial directives that they have to
6 abide to in helping them in their own mandate.

7 **MR. GABRIEL POLIQUIN:** Okay.

8 **COMMISSIONER HOGUE:** And is it useful for you
9 to get more information if we place ourselves as of today?

10 **MR. BENOÎT DICAIRE:** Well, it's always useful
11 to have more context. It's not always possible to have
12 because there's a lot of recognizance activity at the time.
13 It's like piecing -- trying to piece a puzzle together. They
14 might have three pieces of that puzzle, but it doesn't paint
15 that full picture yet. So as you saw in the evolution of
16 some of those bulletins, there's an evolution of that
17 situation that brought us from 2021 to 2024. So there is
18 lessons learned that are tied to how we collaborate and how
19 we can share information and contribute to both our mandates.
20 So, in some cases, the -- it's what's useful for me is in the
21 discourse of my own mandate in protecting parliament.

22 **COMMISSIONER HOGUE:** Thank you.

23 **MR. GABRIEL POLIQUIN:** Okay. And so this is
24 an MOU you've recently finalized with ---

25 **MR. BENOÎT DICAIRE:** Yes.

26 **MR. GABRIEL POLIQUIN:** --- the Cyber Centre;
27 correct?

28 **MR. BENOÎT DICAIRE:** Yeah, it's finally --

1 it's -- I think it was signed last week ---

2 MR. GABRIEL POLIQUIN: Okay.

3 MR. BENOÎT DICAIRE: --- the MOU, and we are
4 still in negotiation on -- we're still finalizing the
5 associated documents that are really the methodology of how
6 we are working as per the MOU.

7 MR. GABRIEL POLIQUIN: Okay. When you say
8 associated documents, what do you mean?

9 MR. BENOÎT DICAIRE: So CONOPS, so a way that
10 we engage, the formalized protocol for engagement.

11 MR. GABRIEL POLIQUIN: Okay. And are you
12 satisfied with this new MOU that your unit will be getting
13 the ---

14 MR. BENOÎT DICAIRE: Yes.

15 MR. GABRIEL POLIQUIN: --- the right
16 information?

17 MR. BENOÎT DICAIRE: Yes.

18 MR. GABRIEL POLIQUIN: Okay. If we could
19 turn now to WIT128 while still on the interview summary,
20 please? And if you could scroll down to paragraph 79,
21 please? Okay. So let's start with the first sentence here.
22 So,

23 "The targeted MPs were not informed
24 by the HOC administration in 2022
25 because the threat activity never
26 reached them."

27 So I'm just trying to reconcile that with
28 what you said earlier that they were notified. I just don't

1 understand.

2 **MR. BENOÎT DICAIRE:** So they weren't -- there
3 was a -- on the January 22nd bulletin 2021, as part of our
4 investigation, we did send an email to those 8 members, once
5 we correlated the IP address to the member's email, to see if
6 they had reached the email, but, clearly, as part of the
7 investigation, we also found out that our email system hadn't
8 done its job in quarantine. So that was the only time that
9 was notified around those scenarios. So ---

10 **MR. GABRIEL POLIQUIN:** Okay. Okay. Now
11 going back to an earlier topic, this is the third sentence,
12 "Had HoC IT known that it was a
13 state-sponsored campaign, they may
14 have looked at it with a heightened
15 sense of awareness for monitoring and
16 business continuity purposes."

17 Is this what you were referring to earlier?

18 **MR. BENOÎT DICAIRE:** Yes. Just like we --
19 when we have a special event at the House, not necessarily
20 cyber, but that is of public interest where it would generate
21 more interest and would potentially, you know, risk the
22 infrastructure because there's too many people consuming
23 those services, then we have the same heightened sense of
24 monitoring and awareness to ensure that, you know, we can
25 ensure that those important events are happening unhindered
26 from technical failures.

27 **MR. GABRIEL POLIQUIN:** Okay. Understood. If
28 we could turn now to another document, so CANSUM27, please?

1 So we'll stick on this page for now, that paragraph in
2 italics. Just to summarize, this is a document that's
3 prepared by the Government of Canada that summarizes some
4 intelligence that it received. So, of course, the document
5 is based on intelligence and not evidence, and the document -
6 - this document here does not contain the caveats and
7 limitations that are on the original information, but, of
8 course, you know, it applies as well.

9 If we could turn to paragraph 9 of that
10 document, please? And again, we're on that famous February
11 17th date of 2021. It says,

12 "...CSE delivered a SECRET-level
13 briefing to the HoC's IT Security
14 officials, including the Director IT
15 Security. CSE's brief was delivered
16 by CSE subject matter experts with
17 CSIS officials also in attendance.
18 [And] the brief focused on the threat
19 actor designated as APT31. Country
20 tactics, and classes of targets that
21 have historically been of interest to
22 the threat actor, such as U.S. and
23 Canadian politicians, were explicitly
24 shared."

25 And so -- and I realize you weren't there at
26 the time. You were not at this meeting; correct? Okay.

27 **MR. BENOÎT DICAIRE:** Correct.

28 **MR. GABRIEL POLIQUIN:** And so I just want to

1 understand, it seems that there was some information that was
2 delivered to the HoC IT's security officials about the fact
3 that this was a foreign threat; correct?

4 **MR. BENOÎT DICAIRE:** Correct.

5 **MR. GABRIEL POLIQUIN:** Okay. And so I just
6 want to reconcile that with what was said earlier in the
7 interview summary that, you know, it would have been nice to
8 have that information at the time. Just help us just
9 understand.

10 **MR. BENOÎT DICAIRE:** Well, it's not that
11 abnormal when information comes to light on some things, but
12 at this point in time, the keyword here is "suspected". I
13 mean, I think that that was -- it's very preliminary in the
14 timeline around, you know, confirmation and these types of --
15 so I think the key word here is, you know, the -- suspected
16 to come from the following, you know, but they were asking
17 also for our help in trying to piece that puzzle together.
18 So as part of the same meeting, we also shared some relevant
19 metadata, so not actual emails from MPs, but actual
20 information that we've gathered from based on their bulletins
21 to help them in their recognizance efforts and in their
22 intelligence-gathering efforts. So, yes, there was some -- a
23 classified briefing that we -- one of our directors was shown
24 and couldn't -- you know, needed to -- that classified
25 briefing was happening in a secure facility, and that
26 document was not provided to him. So there is definitely
27 caveats around ---

28 **MR. GABRIEL POLIQUIN:** Sure.

1 **MR. BENOÎT DICAIRE:** --- handling that type
2 of information.

3 **MR. GABRIEL POLIQUIN:** Sure. And I'll have a
4 question about that in a second, but while we're on here, I
5 just want to -- what we're interested in is making sure that,
6 you know -- or knowing whether your unit has the information
7 that it needs. And so what I'm understanding is that, yes,
8 it can be useful to have information about whether or not an
9 operation is by a foreign actor. Did your unit have the
10 information it needed at the time? And I know you weren't
11 there, but, you know, from an institutional standpoint, if an
12 IT director under your purview receives information like
13 that, are you satisfied that you have the information you
14 need to change your operational stance or not?

15 **MR. BENOÎT DICAIRE:** If I can meet my
16 mandate, which is, you know, assess and that the
17 parliamentary infrastructure wasn't breached, or there's no
18 risk from a cyber perspective to the parliamentary, or the
19 parliamentary infrastructure, or the continuity of
20 parliament, then it satisfies my needs, because I am not a
21 national intelligence agency.

22 **MR. GABRIEL POLIQUIN:** Okay. So I'm almost
23 close to the end of my time. Yeah, I had just one more
24 question on this document at paragraph 11. So at paragraph
25 11 it makes reference to,

26 "The 2021 APT31 cyber event
27 highlighted three "lessons learned"
28 within CSE regarding the response to

1 the ongoing threat..."

2 So, again, this isn't your document, but we
3 talk about here at paragraph 2, so (ii) -- oh, sorry, (iii),
4 so, "CSE officials..." -- this is part of their lessons
5 learned, but,

6 "CSE officials also worked with [the]
7 HoC teams to ensure that the HoC
8 adopted the full range of measures
9 offered by CSE's cyber security
10 program to better defend and respond
11 to cyber threats."

12 And you may or may not be able to comment on
13 what those measures are, but have they been implemented?

14 **MR. BENOÎT DICAIRE:** I can't comment on the
15 measures that we implemented. I can tell you that we have a
16 strong relationship with CSE and Cyber Centre, and that they
17 offer different -- a various amount of services.

18 **MR. GABRIEL POLIQUIN:** Okay. But are those
19 measures mentioned in the MOU, the new MOU, at all, or?

20 **MR. BENOÎT DICAIRE:** We have access to the
21 full range of their services.

22 **MR. GABRIEL POLIQUIN:** Okay. Okay. I have
23 one last question that may not be able to answer, but you can
24 maybe help us out. One of the questions that comes up in
25 this Commission is, well who is responsible for what? Who is
26 responsible for informing MPs? Here MPs seem to have been
27 informed at some point that they were targeted by an attack.
28 Suppose you have another incident a little bit like this one,

1 where this is investigated by you internally, but also
2 external partners are aware this is going on. Do you have a
3 view on who should be responsible for informing MPs?

4 **MR. BENOÎT DICAIRE:** I think it depends on
5 what the question, and what the situation is, and what the
6 mandate is, and those criteria have to be -- so if it's
7 something that has to do with a cyber risk around
8 infrastructure and continuity of Parliament, definitely we
9 are there. And then if it's something that has to do with
10 under the privy of national security agencies, then, you
11 know, we would work in collaboration through my partner here,
12 the sergeant-at-arms, you know, around those. So it's
13 definitely there's an opportunity to evolve our collaboration
14 while respecting our individual mandates.

15 **MR. GABRIEL POLIQUIN:** Okay. Those are my
16 questions, Mme Commissaire.

17 **COMMISSIONER HOGUE:** Thank you. You're right
18 on.

19 So we'll come back at 2:00 o'clock sharp,
20 because we have a long day today, so if we want to make sure
21 to be able to go until the end. Be back at 2:00 and we'll do
22 the same.

23 Thank you. Bon appétit, tous monde.

24 **THE REGISTRAR:** Order, please. À l'ordre,
25 s'il vous plait.

26 The sitting of the Commission is now in
27 recess until 2:00 p.m. Cette séance de la Commission est
28 maintenant suspendue jusqu'à 14 h.

1 --- Upon recessing at 12:40 p.m./

2 --- La séance est suspendue à 12 h 40

3 --- Upon resuming at 2:02 p.m./

4 --- La séance est reprise à 14 h 02

5 **THE REGISTRAR:** Order, please. À l'ordre,
6 s'il vous plait.

7 This sitting of the Foreign Interference
8 Commission is now back in session. Cette séance de la
9 Commission sur l'ingérence étrangère est de retour en
10 session. The time is 2:02 p.m. Il est 14 h 02.

11 **COMMISSIONER HOGUE:** Alors, contre-
12 interrogatoire. First one is counsel for Michael Chong.

13 **--- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR**

14 **MR. FRASER HARLAND:**

15 **MR. FRASER HARLAND:** Good afternoon,
16 Commissioner.

17 I'd like to start with some questions on
18 security briefings.

19 And if we could, Mr. Court Operator, bring up
20 WIT128.EN, please? And if we could go to paragraph 61?

21 It's a question for you, Mr. McDonell. At
22 paragraph 61 there, it says that you note that you had been
23 advocating in favour of these types of briefings, which are
24 security briefings to members of Parliament, prior to the
25 recommendations made in the Procedure and House Affairs
26 Committee. So my question is, how long had you been
27 advocating for those briefings? I just want to understand
28 your views on that matter.

1 **MR. PATRICK McDONELL:** I first started
2 advocating for those briefings in 2019.

3 **MR. FRASER HARLAND:** In 2019? Okay.

4 And Madam Commissioner, I'm going to ask for
5 your leave to take the witness to the NSICOP report. I did
6 not put it in my list of documents, so if there's an
7 objection, I understand, but it's a well-known document at
8 this point, so.

9 **COMMISSIONER HOGUE:** It's fine if they can
10 answer your question. If they cannot answer your question,
11 they will let you know.

12 **MR. FRASER HARLAND:** Absolutely. So that is
13 at COM363.

14 **--- EXHIBIT No./PIÈCE No. COM0000363:**

15 Special Report on Foreign

16 Interference in Canada's Democratic

17 Processes and Institutions

18 **MR. FRASER HARLAND:** Are you familiar with
19 this document, Mr. McDonell?

20 **MR. PATRICK McDONELL:** Yes.

21 **MR. FRASER HARLAND:** Okay. And if we could
22 go to paragraph 126, which I think is on page 62 of the PDF?

23 **MR. PATRICK McDONELL:** So in this paragraph,
24 we see that in December 2019, the Clerk of the Privy Council
25 sought the Prime Minister's authorization to implement
26 briefings. The Prime Minister didn't respond. And the same
27 question was sought again in December of 2020, and that
28 package included a draft instruction for letters to the

1 Ministers of Public Safety and Defence to coordinate the
2 briefings.

3 So my question to you, Mr. McDonell is if in
4 December of 2019 Public Safety had come to you, as was
5 instructed here, and sought to carry out those briefings, I
6 take it you would have been happy to assist to ensure that
7 those briefings could be carried out?

8 **MR. PATRICK McDONELL:** Yes.

9 **MR. FRASER HARLAND:** Thank you. I want to
10 turn now to another matter, which is the House of Commons'
11 awareness of the PRC, the People's Republic of China's
12 targeting of my client, who is the Honourable Michael Chong.

13 At paragraphs 80 to 81 of your witness
14 statement, it indicated that you didn't receive any specific
15 intelligence about the targeting of Mr. Chong. Is that
16 right?

17 **MR. PATRICK McDONELL:** That is right.

18 **MR. FRASER HARLAND:** So nothing from CSIS?
19 Nothing from Public Safety?

20 **MR. PATRICK McDONELL:** Not to me.

21 **MR. FRASER HARLAND:** Okay. So forgive me if
22 it's stating the obvious, but you could not possibly have
23 done anything about the targeting of my client without any
24 information having been provided to you? Would you agree
25 with that?

26 **MR. PATRICK McDONELL:** I would.

27 **MR. FRASER HARLAND:** Okay. Those are my
28 questions. Madam Commissioner, thank you very much.

1 **COMMISSIONER HOGUE:** Thank you.

2 Next one is counsel for Erin O'Toole. I
3 think it's on Zoom.

4 **MR. THOMAS JARMYN:** Thank you, Commissioner.

5 **COMMISSIONER HOGUE:** Oh, you're on mute.
6 Okay.

7 **--- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR**

8 **MR. THOMAS JARMYN:**

9 **MR. THOMAS JARMYN:** Thank you, Commissioner.

10 I represent Erin O'Toole and many of my
11 questions actually were addressed by Commission counsel, so I
12 only have a few.

13 HoC01 speaks to the residential and
14 constituency office security program. And as I understand
15 it, that is a program whereby there's risk assessments
16 carried out and then security measures are developed for MPs
17 based upon your understanding of the nature and severity of
18 the threat. Is that correct?

19 **MR. PATRICK McDONELL:** It's not a risk
20 assessment per say. That would be something different. We
21 do a security evaluation of the sites, whether it's a
22 constituency site or a residential site. And based on that
23 evaluation, a decision is made on what security measures,
24 camera, video, contacts, alarms, would be in place -- would
25 have to be installed and put in place to provide an
26 appropriate level of security.

27 **MR. THOMAS JARMYN:** Without getting into the
28 particulars of any specific MP's security measures, my

1 understanding is that there's a range of security measures
2 applied to specific -- or given to particular MPs ranging
3 from personal alert devices, home monitoring, all the way up
4 to actual personal security. Who makes those determinations?

5 **MR. PATRICK McDONELL:** The personal security
6 is done on a case-by-case basis. If a site security is
7 required at the constituency office, sometimes post-incident
8 at a residence, where there's been vandalism or an incident
9 at the MP's residence, so that's done on a case-by-case
10 basis. The respective leaders of the political parties do
11 have the right to request personal security escort.

12 **MR. THOMAS JARMYN:** That seems like a
13 distinctly different process for physical security as related
14 to digital security, which seems to be a one-size fits all
15 approach to security devices and the digital presence. Is
16 that fair?

17 **MR. PATRICK McDONELL:** I can't comment on the
18 digital world. That doesn't fall within my area of
19 responsibilities.

20 **MR. THOMAS JARMYN:** Possibly, Mr. Dicaire,
21 you could comment?

22 **MR. BENOÎT DICAIRE:** I think it depends on
23 the context, so I just -- I want clarity a bit more on the
24 question itself, because it's different types of risk that
25 we're trying to manage.

26 **MR. THOMAS JARMYN:** I guess the question is,
27 is the approach to digital security uniform among all MPs or
28 is it tailored based upon the particular threats, for

1 example, that some of the MPs last week testified to?

2 **MR. BENOÎT DICAIRE:** I would say it's a
3 combination of both. There's parameters that are uniform in
4 terms of if you look at it's a layered approach, right, to
5 cyber security. So there's going to be common elements
6 within the parameter. There's maybe common elements within
7 the digital ID, if you want, or the accounts. There's going
8 to be common parameters at the system level or at the
9 infrastructure level. But then depending on the threats,
10 then we would tailor the approach specifically to a
11 particular attack vector, should we require to do it.

12 **MR. THOMAS JARMYN:** But those parameters are
13 only associated with the assessment of risk in relation to
14 parliamentary systems and devices?

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

16 **MR. THOMAS JARMYN:** So in contrast to
17 physical security, where we could be looking at a residence
18 or a constituency office, we don't engage in the same
19 analysis of personal digital presence for protection?

20 **MR. BENOÎT DICAIRE:** That would be a question
21 for Pat more than anything else.

22 **MR. PATRICK McDONELL:** Could you repeat the
23 question?

24 **MR. THOMAS JARMYN:** Well so there's a
25 contrast between physical security, where there, from what
26 you've told me, are processes in place to protect a personal
27 residence, potentially transit between personal residence and
28 office, et cetera, as contrasted with digital security, where

1 it doesn't seem there's any investment of protection related
2 to a personal digital presence, only the parliamentary
3 digital presence.

4 **MR. PATRICK McDONELL:** Yeah, so I would stick
5 with my original answer and what I'm responsible for and let
6 the conclusions be drawn from there.

7 **MR. THOMAS JARMYN:** Okay. And so if the --
8 based upon what you testified to when Commission counsel was
9 examining you and Mr. Dicaire, you're guided by the policies
10 of the Board of Internal Economy in terms of what will and
11 won't be protected. So if an expansion was required, it
12 would have to be the BOIE that would make that choice? Is
13 that correct?

14 **MR. PATRICK McDONELL:** That is correct.

15 **MR. THOMAS JARMYN:** Okay. And does the House
16 carry out a risk assessment when a member of Parliament
17 leaves office?

18 **MR. PATRICK McDONELL:** To the best of my
19 knowledge, no.

20 **MR. THOMAS JARMYN:** Some Members have been
21 very active parliamentary careers, very outspoken on issues
22 that cause them to be targets during their parliamentary
23 career. And so again, if such an assessment in post-
24 parliamentary life protection were to be applied for, that
25 would be a BOIE decision too? Is that correct?

26 **MR. PATRICK McDONELL:** Not necessarily. If
27 there is a threat based on -- well, if the threat assessment
28 reveals that there is a *bonafide* threat out there, I would

1 imagine that the RCMP Protective Operations, Public Safety
2 would be in that discussion.

3 **MR. THOMAS JARMYN:** Okay. Those are my
4 questions, Commissioner. Thank you very much.

5 **COMMISSIONER HOGUE:** Thank you.

6 Counsel for Jenny Kwan.

7 **--- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR**

8 **MR. SUJIT CHOUDHRY:**

9 **MR. SUJI CHOUDHRY:** My name is Sujit
10 Choudhry. I'm counsel for Jenny Kwan.

11 I have some questions about the APT31
12 incident that we've been discussing quite a bit, and I think,
13 Mr. Dicaire, I think those are probably mostly directed to
14 you.

15 And so I was hoping we could get pulled up
16 again WIT129. Thank you. And could we please go down to --
17 the page with paragraphs 13 to 15? Thank you very much.

18 And so I know that you weren't at this
19 meeting, and you weren't involved in these decisions, and so
20 I understand your answer might be you don't know, but we --
21 but this is now before us and so I'd like to ask you some
22 questions about this if I could.

23 **MR. BENOÎT DICAIRE:** Yeah.

24 **MR. SUJIT CHOUDHRY:** Okay. And so it's about
25 the decision that was taken in February -- on -- in the wake
26 of the February 17th, 2021 meeting between Mr. Touati and
27 members of CSIS and the CSE it would seem regarding the
28 attack and the information that was provided. And if I

1 understand it correctly here, after the briefing, the
2 decision was taken that since the attack was not successful,
3 it was therefore not necessary to warn the MPs. Is that
4 fair?

5 **MR. BENOÎT DICAIRE:** That's a fair
6 assessment.

7 **MR. SUJIT CHOUDHRY:** Okay. Could you tell me
8 who -- I know this came up, but I want to get a bit more
9 precision on this. Who made that decision?

10 **MR. BENOÎT DICAIRE:** I think this is the
11 normal protocol, if we were -- again, this morning as part of
12 my testimony, if we were to advise of every attack, we would
13 be -- we're talking about hundreds of millions of attack
14 attempts.

15 **MR. SUJIT CHOUDHRY:** Okay.

16 **MR. BENOÎT DICAIRE:** So I think we would have
17 a problem in being able to scale.

18 **MR. SUJIT CHOUDHRY:** Okay. And so just to
19 pursue this a bit, would -- even if the decision was made by
20 you or a member of your team, which is what I think the
21 answer is, would the -- are there circumstances in which the
22 speaker would ever be advised that you'd decided not to warn
23 a member of parliament?

24 **MR. BENOÎT DICAIRE:** I think if there were a
25 risk, inherent risk to the House of Commons, the continuity
26 of operation, the infrastructure, the information, something
27 of serious nature, it would go to the clerk of the House of
28 Commons and first, and then ---

1 **MR. SUJIT CHOUDHRY:** Okay.

2 **MR. BENOÎT DICAIRE:** --- through that
3 channel, then a determination would be to advise the speaker
4 on it.

5 **MR. SUJIT CHOUDHRY:** So is it fair to say
6 that what would go to the clerk first and then possibly with
7 the speaker would be threats to the operation of the Commons
8 as an institution?

9 **MR. BENOÎT DICAIRE:** As an institution, yes.

10 **MR. SUJIT CHOUDHRY:** Okay. But that's
11 different than, let's say, interference with the performance
12 of duties by a member of parliament?

13 **MR. BENOÎT DICAIRE:** It's different, yeah.

14 **MR. SUJIT CHOUDHRY:** Okay. And then would --
15 and I think I know the answer to this question, are there any
16 circumstances under which the Board of Internal Economy would
17 ever be advised of a cyber security attack, even if it was
18 not successful?

19 **MR. BENOÎT DICAIRE:** In those parameters? I
20 don't think so.

21 **MR. SUJIT CHOUDHRY:** Okay. And so I ---

22 **MR. BENOÎT DICAIRE:** It's not successful.

23 **MR. SUJIT CHOUDHRY:** Okay. And so just to
24 pursue this point a bit, so you -- I think you've been
25 referred to the testimony of MPs Genius and MP MacKay, who
26 were both targeted by this attack, and they have drawn a
27 direct line between being targets and the work they do as
28 parliamentarians, in particular, as part of the IPAC, this

1 interparliamentary group involving China that's a global
2 group. And so they have sort of said they would have liked
3 to have been told. And that they -- had they been told, they
4 could have taken protective measures. So, for example, they
5 might have known about this, let's call it the pixel attack.
6 I'm not a technical person, so forgive me if I'm getting it
7 wrong. And so I'd like maybe to take you to -- to not look
8 at what's happened, but to think about things on a go-forward
9 basis.

10 **MR. BENOÎT DICAIRE:** M'hm.

11 **MR. SUJIT CHOUDHRY:** Okay? So on a go-
12 forward basis, if your team became aware that an attack was
13 state sponsored, even if it was not successful, do you think
14 the member of parliament in question or the members of
15 Parliament in question should be advised?

16 **MR. BENOÎT DICAIRE:** If -- it's a tricky
17 question to answer. Yes, they should be advised, but by who?

18 **MR. SUJIT CHOUDHRY:** Okay.

19 **MR. BENOÎT DICAIRE:** And is it part of my
20 mandate to provide that advice? I'll give you the example
21 specifically for Mr. Genius, there is no possibility I could
22 ever advise because we -- it wasn't a House of Commons device
23 that was targeted, so we didn't have any information about
24 Mr. Genius.

25 **MR. SUJIT CHOUDHRY:** So I see. Whereas, for
26 Mr. MacKay, it was a House of Commons device?

27 **MR. BENOÎT DICAIRE:** Yes, it was.

28 **MR. SUJIT CHOUDHRY:** Okay. And so then let's

1 focus on House of Commons devices then. So for -- so if a
2 member of parliament's House of Commons device was targeted,
3 and if your team -- and it was unsuccessful, but your team
4 came into possession of information that the attack was state
5 sponsored, going forward, should that member of parliament be
6 advised?

7 **MR. BENOÎT DICAIRE:** Would be a collaboration
8 effort between if there's a recommendation from the security
9 intelligence agencies that they would have a particular angle
10 to want to warn -- because, again, this goes beyond my
11 mandate.

12 **MR. SUJIT CHOUDHRY:** Right.

13 **MR. BENOÎT DICAIRE:** So if they would make a
14 recommendation based on their assessment or based on
15 information I might not be privy to, then they would -- then
16 it would be a collaboration between the security agencies and
17 us and then a decision would be made based on risks, or based
18 on impacts, or based on potential other factors.

19 **MR. SUJIT CHOUDHRY:** And would the warning,
20 or the information, or the briefing come from your team, or
21 from the intelligence agencies, or both?

22 **MR. BENOÎT DICAIRE:** Probably in a
23 combination of the both. So if we participate into an
24 investigation or into the forensics tied to a cyber attack,
25 then they potentially wouldn't require us to be at the table,
26 but if it is completely on their privy, they would coordinate
27 with us to just coordinate the briefing and they would lead
28 the briefing.

1 **MR. SUJIT CHOUDHRY:** Okay. You know, one of
2 the things we're trying to grapple with are these silos of
3 different responsibilities and different legal instruments.
4 So you've probably heard the term "threat reduction measure",
5 and I think that was posed to Mr. McDonell as well. And so,
6 you know, from a layperson's perspective, this type of a
7 briefing about a thwarted cyber attack might -- feels like a
8 threat reduction measure of a sort. It might not be the type
9 of threat that CSIS classifies this as, but it feels like
10 that to a member of parliament. Would you agree?

11 **MR. BENOÎT DICAIRE:** You would have to ask a
12 member of parliament.

13 **MR. SUJIT CHOUDHRY:** Okay. Fair enough. So,
14 look, can I take you to CANSUM27, please? And could we go to
15 paragraph 11(i), or 11(i).

16 So, Mr. Dicaire, are you -- you're familiar
17 with this document?

18 **MR. BENOÎT DICAIRE:** Yes, I am.

19 **MR. SUJIT CHOUDHRY:** So I want to ask you a
20 question about 11(i). And what it says there for the record
21 is that,

22 "Immediately following the 17
23 February meeting, with the [House of
24 Commons], CSE officials internally
25 expressed concern that the [House of
26 Commons] had not been given
27 sufficient information to appreciate
28 the significance of the threat."

MR. BENOÎT DICAIRE: Again, I think the parameters that would have been looked at would have been from the angle of threat to the member specifically at that time for that cyber attack specifically, and the level of risk tied to this attack. So in partnership, of course, it is a partnership with the security agencies, we would have had certain, you know, a dialogue around, okay, what do we do here, but in this context, we didn't have a lot of information, so it's hard for me to speculate what we would have done if we had more information. But at the same point in time, recommendations would have been with more information, probably more prescriptive.

1 **MR. SUJIT CHOUDHRY:** Okay. Thank you, sir.
2 Thank you, gentlemen, for your time.

3 **COMMISSIONER HOGUE:** Thank you. Next one is
4 the Concern Group.

5 **MR. GABRIEL POLIQUIN:** I understand Concern
6 Group doesn't have any questions.

7 **COMMISSIONER HOGUE:** No questions? RCDA?

8 **MR. GUILLAUME SIROIS:** No questions either.
9 Merci.

10 **COMMISSIONER HOGUE:** Human Rights Coalition.

11 --- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR

12 **MS. SARAH TEICH:**

13 **MS. SARAH TEICH:** Good afternoon. We heard
14 last week from MPs Genuis and MacKay and they both expressed
15 concerns about the possibility that in relation to the APT31
16 cyber attacks, members of diaspora communities with whom they
17 were in contact may have been inadvertently exposed. Do you
18 share these concerns?

19 **MR. PATRICK McDONELL:** I didn't hear the
20 question. I'm sorry.

21 **MS. SARAH TEICH:** Is this better?

22 **MR. PATRICK McDONELL:** Hopefully.

23 **MS. SARAH TEICH:** Okay. Let's try this
24 again.

25 **MR. PATRICK McDONELL:** Okay.

26 **MS. SARAH TEICH:** We heard from MPs Genuis
27 and MacKay last week and they both expressed concerns about
28 the possibility that in relation to the cyber attacks,

1 members of diaspora communities with whom they were in
2 contact may have been inadvertently exposed. Do you share
3 these concerns?

4 **MR. PATRICK McDONELL:** I have no comment on
5 that.

6 **MR. BENOÎT DICAIRE:** I think that's beyond
7 our mandate. Our mandate is parliamentarians and
8 parliamentary devices.

9 **MS. SARAH TEICH:** Okay. In general -- and
10 now I'll ask generally about your policies. If a
11 parliamentary account is compromised, does the House of
12 Commons administration look at or investigate potential
13 impacts on diaspora community members who are in contact with
14 the compromised account?

15 **MR. BENOÎT DICAIRE:** I think that the
16 analysis that's going to be done is going to be on the impact of
17 the attack or the compromise and then the scale of it. So
18 should it have ripple effects, regardless of which community,
19 it would be looked at from that perspective. It's really a
20 technical evaluation at that point in time and understanding
21 the depth of the attack or the success of that attack will
22 determine the action.

23 **MS. SARAH TEICH:** Okay. And according, again
24 generally, to your policy, if you were to find out that
25 members of diaspora communities were impacted, would you let
26 them know?

27 **MR. BENOÎT DICAIRE:** If they were part of the
28 technical evaluation, if they were in a scope, I would

1 suspect that, you know, we would action -- take the
2 appropriate actions. It's hard to comment on a very broad
3 statement like that one.

4 **MS. SARAH TEICH:** Okay. Would it be helpful
5 if you had a policy that would tell you in such and such a
6 case, we would notify them or we would offer them these
7 supports? Because it sounds like right now it's on a case-
8 by-case basis.

9 **MR. BENOÎT DICAIRE:** I think our focus is on
10 parliamentarians and parliamentary infrastructure. I don't
11 know about you, Pat, but that's the scenario on our side. So
12 our focus is really around the mandate that we are given.

13 **MS. SARAH TEICH:** Okay. Can we please pull
14 up HOC1? And can we scroll to the top at page 12? Thank
15 you.

16 Here it says:

17 "The House administration maintains
18 strong partnerships..."

19 I won't read the whole sentence:

20 "...including with RCMP, CSIS, Public
21 Safety, and CSE..."

22 Have you ever recommended to one or more of
23 these organizations that they should provide support to
24 members of diaspora communities that may have been impacted
25 by a cyber attack on members of Parliament?

26 **MR. BENOÎT DICAIRE:** Not to my knowledge.

27 **MS. SARAH TEICH:** Should the House of Commons
28 administration make such a recommendation in the future?

1 **MR. BENOÎT DICAIRE:** That is up to the
2 Commission to look at some of those findings.

3 **MS. SARAH TEICH:** Okay. No further
4 questions. Thank you.

5 **COMMISSIONER HOGUE:** Thank you.

6 AG.

7 **--- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR**

8 **MR. GREGORY TZEMENAKIS:**

9 **MR. GREGORY TZEMENAKIS:** Good afternoon. My
10 name is Gregory Tzemenakis. I'm Government counsel. I'm
11 just going to ask you some questions of clarifications from
12 your witness statements, and where appropriate, I will call
13 them up.

14 I will also use the term "Member" and "MP"
15 interchangeably to refer to a Member of the House of Commons.

16 So I want to start with some questions on
17 security. Am I correct that security clearances are not
18 mandatory for members of Parliament?

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

20 **MR. GREGORY TZEMENAKIS:** House administration
21 is not responsible for providing security clearances to
22 members of Parliament? That's done through another vehicle;
23 correct?

24 **MR. PATRICK McDONELL:** We don't provide
25 security clearances to members of Parliament.

26 **MR. GREGORY TZEMENAKIS:** And am I also
27 correct that House administration does not offer direct
28 support for IT matters that extend beyond official

1 parliamentary accounts, such as the personal email accounts,
2 unless it's incidental, if I can put it that way, to
3 parliamentary business?

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

5 **MR. GREGORY TZEMENAKIS:** And MPs are not
6 technically entitled to use devices that have not been
7 authorized by your services, sorry, the Division that you
8 lead, to conduct parliamentary business on personal devices?
9 Is that correct?

10 **MR. PATRICK McDONELL:** That's correct.

11 **MR. GREGORY TZEMENAKIS:** But it -- in the --
12 it is -- sorry. From your testimony of earlier today, I also
13 heard you to say that you -- the House administration does
14 not have an independent way to determine whether or not an
15 MP's personal device has been compromised, because it's not
16 within your mandate and it's not within the scope of the what
17 I'll call parliamentary IT network that you manage? Is that
18 correct?

19 **MR. BENOÎT DICAIRE:** Our mandate is
20 parliamentary.

21 **MR. GREGORY TZEMENAKIS:** Right. But an MP
22 can come to you if there is an issue and ask for your
23 assistance; correct?

24 **MR. BENOÎT DICAIRE:** And we'll do it on a
25 best effort basis.

26 **MR. GREGORY TZEMENAKIS:** Best effort basis.
27 And am I also correct -- this is a question for you, sir, am
28 I also correct that Members do not have an express obligation

1 to report attempts either at physical security or other
2 issues of concern to them, including foreign interference, to
3 your office, to the sergeant-at-arms?

4 **MR. PATRICK McDONELL:** That's correct.

5 **MR. GREGORY TZEMENAKIS:** So I want to turn to
6 the topic of partnerships. Am I correct that the House
7 administration collaborates with external cyber security
8 partners such as CSE, CSIS, and others?

9 **MR. PATRICK McDONELL:** Correct. For CSE.
10 For myself.

11 **MR. GREGORY TZEMENAKIS:** And that you also
12 have strong partnerships with the security intelligence,
13 local law enforcement, government agencies, and the
14 government agencies include RCMP, CSIS, Public Safety, and
15 CSE?

16 **MR. PATRICK McDONELL:** Yes.

17 **MR. GREGORY TZEMENAKIS:** Yes. And more
18 formally, the sergeant-at-arms has an MOU with CSIS and the
19 RCMP; correct?

20 **MR. PATRICK McDONELL:** Correct.

21 **MR. GREGORY TZEMENAKIS:** And the CIO has an
22 MOU with CSE?

23 **MR. PATRICK McDONELL:** Correct.

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

25 **MR. GREGORY TZEMENAKIS:** And that MOU was
26 recently amended this week, I believe? Is that correct?

27 **MR. BENOÎT DICAIRE:** I'm not sure. Last
28 week, peut-être.

1 **MR. GREGORY TZEMENAKIS:** Okay. I want, if I
2 can direct your attention to -- and I'm going to ask the
3 Court Reporter to pull up WIT129, English, and go to
4 paragraph 8, please?

5 Yeah, this is an interview that was conducted
6 with Mr. Touati. And I believe, sir, you were present, Mr.
7 Dicaire?

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

9 **MR. GREGORY TZEMENAKIS:** And at paragraph 8,
10 he says, Mr. Touati says:

11 "The information received, mainly of
12 a technical nature, is 'sufficient to
13 enable the House of Commons to
14 determine whether the measures it is
15 putting in place are mitigating the
16 risks.'"

17 Do you have any reason to depart from that
18 statement, sir?

19 **MR. BENOÎT DICAIRE:** No.

20 **MR. GREGORY TZEMENAKIS:** No. Thank you. I
21 want to turn to the next topic, which is briefings. My
22 understanding, Mr. McDonell, is that the House coordinated
23 security intelligence and law -- with security intelligence
24 and law enforcement partners to provide unclassified foreign
25 interference briefings to caucus members of all recognized
26 parties in the house?

27 **MR. PATRICK McDONELL:** Correct.

28 **MR. GREGORY TZEMENAKIS:** And that was in

1 fact done and that included not only the Liberal Party and
2 the Conservative Party, but the other recognized parties in
3 the House?

4 **MR. PATRICK McDONELL:** And independent
5 members.

6 **MR. GREGORY TZEMENAKIS:** And independent
7 members. Thank you. And just generally speaking, do you
8 agree that more training and more education about FI, FI
9 activities, and FI threats would, in addition to any other
10 efforts made by the Government of Canada, as well as the
11 public, be a good thing for members of Parliament to have?

12 **MR. PATRICK McDONELL:** Yes.

13 **MR. GREGORY TZEMENAKIS:** So I want to switch
14 topics a little bit and talk about the ability to contact
15 your office, sir.

16 So last week we heard some suggestions from
17 an MP, including from the former leader of the opposition,
18 the Honourable Mr. O'Toole, that -- and these are my words,
19 I'm paraphrasing his words, not his words, to the effect that
20 he may not have known who to contact if he had concerns about
21 FI, whether it was in relation to a member, a senator, or
22 someone else. Am I right that he could have contacted your
23 office for guidance and support?

24 **MR. PATRICK McDONELL:** Yes.

25 **MR. GREGORY TZEMENAKIS:** And was that the
26 case -- is that a relatively new phenomenon, or is that --
27 has that always been the case since you became sergeant-at-
28 arms in 2019?

1 **MR. PATRICK McDONELL:** It's always been the
2 case, but there's many Members and staff, because of their
3 portfolios, how busy they are, often they don't know where to
4 reach out. So in those briefings that we just talked about a
5 few minutes ago, when we brought in CSC, CSIS, RCMP, Public
6 Safety, we reminded the caucuses and the independents that if
7 you have a question in regards to anything security, you call
8 us and we'll coordinate it with the appropriate authority.

9 **MR. GREGORY TZEMENAKIS:** Thank you. I'm
10 going to ask some questions about APT31 and I'm going to
11 direct them to you, Mr. Dicaire.

12 So in the interview with Mr. Touati, he
13 described the relationship with CSC as a healthy
14 collaboration. Would you agree with that assessment?

15 **MR. BENOÎT DICAIRE:** I would agree.

16 **MR. GREGORY TZEMENAKIS:** You would. And the
17 following questions are to clarify what I understand some of
18 the key facts surrounding APT31. And if you disagree with
19 them, please feel free to do so.

20 Let me start with this. Am I correct that
21 the House of Commons IT group investigated and discovered
22 that the emails in question did not reach their intended
23 recipients and they were quarantined by the systems you have
24 in place?

25 **MR. BENOÎT DICAIRE:** From the first bulletin.
26 So the -- there was multiple bulletins. The first bulletins,
27 the emails were quarantined.

28 **MR. GREGORY TZEMENAKIS:** And that there was

1 no threat to Parliament or its infrastructure; correct?

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

3 **MR. GREGORY TZEMENAKIS:** And am I correct
4 that once you determined that the emails -- once it was
5 determined that the emails did not reach their recipients,
6 there was not a need to do something more? And that comes
7 from your witness statement. I can pull it up. It's at
8 paragraph 69, for the purposes of the record.

9 **MR. BENOÎT DICAIRE:** For the purpose of our
10 mandate, the threat was addressed.

11 **MR. GREGORY TZEMENAKIS:** All right. I'm
12 going to ask the Court Reporter to pull up WIT129, paragraph
13 13, which my friend just took you to. I'm going to take you
14 to a different part of that paragraph.

15 In this summary, Mr. Touati states that he
16 participated in a classified briefing of February 17th, and
17 then he states during this briefing:

18 "...Mr. Touati was informed that
19 government agencies suspected that a
20 malign hacking group with suspected
21 links to the People's Republic of
22 China, known as APT31, was
23 responsible for the activities
24 detected in January 2021 targeting
25 parliamentarians' email accounts."

26 Was that information relayed to you?

27 **MR. BENOÎT DICAIRE:** I was part of the
28 briefing when he said that.

1 **MR. GREGORY TZEMENAKIS:** All right. So at
2 that time in February of 2021, you knew that the event that
3 took place in January was linked to a hacking group suspected
4 -- sorry, was suspect -- was -- I'm not going paraphrase it.
5 Scratch that. Was -- you knew in February of 2021 that the
6 event that took place in January of 2021 was suspected to be
7 linked to the People's Republic of China through APT31?

8 **MR. BENOÎT DICAIRE:** My organization -- I
9 wasn't there at the time. My organization was briefed that
10 they suspected, so the statements on paragraph 13 are
11 correct.

12 **MR. GREGORY TZEMENAKIS:** Okay. And there's
13 also a reference in the other affidavit that all eight of the
14 MPs -- that emails were sent to all eight of the MPs that
15 were concerned, inquiring whether or not they had received an
16 email of -- the email in question; correct?

17 **MR. BENOÎT DICAIRE:** That was part of the
18 first few actions as part of the follow-up to the bulletin.

19 **MR. GREGORY TZEMENAKIS:** Okay. And all
20 eight MPs responded that they either had not or did?

21 **MR. BENOÎT DICAIRE:** Only two responded.

22 **MR. GREGORY TZEMENAKIS:** Only two responded.
23 So, Madam Commissioner, it seems that I have
24 11 seconds left, but I ask for your indulgence for four
25 minutes to just finish one last topic, please?

26 **COMMISSIONER HOGUE:** You're lucky there's
27 many that have no questions. So you can go on for four
28 minutes.

1 **MR. GREGORY TZEMENAKIS:** Thank you.

2 Mr. Dicaire, I just want to revisit your
3 testimony of earlier today when we were talking about the
4 initial bulletin that had been received from CSE in January
5 of 2021. And you'll recall you had a discussion with
6 Commission counsel around whether or not that event -- the
7 words used by CSC or the Cyber Security Centre was that it
8 was likely not malicious. Do you recall that discussion this
9 morning?

10 **MR. BENOÎT DICAIRE:** Yes.

11 **MR. GREGORY TZEMENAKIS:** And have you had an
12 opportunity to review that bulletin before appearing here
13 today?

14 **MR. BENOÎT DICAIRE:** Yes, I have the bulletin
15 right in front of me right now.

16 **MR. GREGORY TZEMENAKIS:** Okay. I'm going to
17 suggest to you, and we have certain rules in process here,
18 I'm going to suggest to you, and I anticipate that we will
19 hear from CSC on Thursday that the bulletin contains slightly
20 different information. So the first thing the bulletin
21 contained was technical information disclosing that the
22 emails contained a tracking link to it. Are you aware of
23 that -- or were you aware of that at the time and are you
24 aware of that now?

25 **MR. BENOÎT DICAIRE:** I'm aware of it now, as
26 I'm reading it right in front of me.

27 **MR. GREGORY TZEMENAKIS:** Okay. And that the
28 bulletin stated that the emails:

1 "...are likely targeting individuals as
2 part of an ongoing collection
3 campaign."? (As read)

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

5 **MR. GREGORY TZEMENAKIS:** And then -- I'm not
6 a technical person, so if there's a distinction, please
7 educate us. I understand that the bulletin also states that
8 the emails likely contained no malicious content, not that it
9 was likely not malicious. It's the content that wasn't
10 malicious. Is that right?

11 **MR. BENOÎT DICAIRE:** You're right.

12 **MR. GREGORY TZEMENAKIS:** And in plain
13 English to somebody like me, does that mean that it didn't
14 contain, for example, malware?

15 **MR. BENOÎT DICAIRE:** Yes, that would be one
16 good way of saying it.

17 **MR. GREGORY TZEMENAKIS:** Good way of saying
18 it. So the bulletin didn't say that the attack was likely
19 not malicious. It was commenting on the substance of what
20 the emails were concerned about?

21 **MR. BENOÎT DICAIRE:** That's it. There was
22 one word omitted this morning, as I recalled from my memory,
23 but now I'm reading it and it says "no malicious content".

24 **MR. GREGORY TZEMENAKIS:** And sir, my job is
25 just to make sure that the facts come out.

26 **MR. BENOÎT DICAIRE:** That's perfect.

27 **MR. GREGORY TZEMENAKIS:** And that's all. So
28 thank you for that clarification.

1 Thank you, Madam Commissioner, for the
2 indulgence of the extra time.

3 **COMMISSIONER HOGUE:** Thank you.

4 So the attorneys for the House. Do you have
5 -- est-ce que vous avez des questions? C'est Maitre Bédard et
6 Gauthier, je pense?

7 **Me MICHEL BÉDARD:** Bonjour, Madame la
8 Commissaire. Non, nous n'avons aucune question.

9 **COMMISSAIRE HOGUE:** Aucune question.
10 Questions en réinterrogatoire, Maitre
11 Poliquin?

12 **Me GABRIEL POLIQUIN:** Pas de
13 réinterrogatoire, merci.

14 **COMMISSAIRE HOGUE:** Alors, merci beaucoup.
15 Thank you very much.

16 **M. BENOIT DICAIRE:** Merci beaucoup.

17 **COMMISSAIRE HOGUE:** Il est trois heures moins
18 vingt. Le prochain témoin, qui est Stéphane Perreault, est
19 prévu pour 15 h 15. Ce que je suggère, c'est que tout le
20 monde revienne à 15 h 05; s'il est déjà arrivé, on pourra
21 débiter, parce qu'on a une longue journée. S'il est pas
22 arrivé, ben, on attendra et on mettra surtout pas de pression
23 pour qu'il se sente mal à l'aise. C'est vraiment prévu à
24 15 h 15. Alors, 15 h 05 pour tout le monde et on verra.
25 Merci.

26 **LE GREFFIER :** Order please. À l'ordre, s'il
27 vous plait.

28 This hearing of the Commission is now in

1 recess until 3:05 p.m. Cette séance de la Commission est
2 maintenant suspendue jusqu'à 15 h 05.

3 --- Upon recessing at 2:42 p.m./

4 --- L'audience est suspendue à 14 h 42

5 --- Upon resuming at 3:05 p.m.

6 --- L'audience est reprise à 15 h 05

7 **LE GREFFIER:** Order please. À l'ordre, s'il
8 vous plait.

9 This sitting of the Foreign Interference
10 Commission is now back in session. Cette séance de la
11 Commission sur l'ingérence étrangère est de retour en
12 session.

13 The time is 3:05 p.m. Il est 15 h 05.

14 **COMMISSAIRE HOGUE:** Alors, Maitre MacKay,
15 c'est vous qui allez interroger monsieur Perrault cet après-
16 midi?

17 **Me JEAN-PHILIPPE MacKAY:** En partie, Madame
18 la Commissaire. Je vais commencer, et à peu près à la moitié
19 du temps, maitre Sheppard va prendre le relais pour compléter
20 l'interrogatoire.

21 **COMMISSAIRE HOGUE:** D'accord.

22 **Me JEAN-PHILIPPE MacKAY:** Donc, Jean-Philippe
23 MacKay pour la Commission. Je comprends qu'on procède par
24 voie d'affirmation solennelle, Monsieur Perrault?

25 **M. STÉPHANE PERRAULT:** Oui, effectivement.

26 **LE GREFFIER:** OK. Merci, Monsieur Perrault.
27 Pourriez-vous s'il vous plait indiquer votre nom complet et
28 épeler votre nom de famille pour la transcription

1 sténographique?

2 **M. STÉPHANE PERRAULT:** Alors, c'est Stéphane
3 Perrault, P-E-R-R-A-U-L-T.

4 **LE GREFFIER:** Merci beaucoup.

5 **--- M. STÉPHANE PERRAULT, Affirmed/Sous affirmation**
6 **solennelle:**

7 **LE GREFFIER:** Merci beaucoup. Maître, vous
8 pouvez procéder.

9 **--- EXAMINATION IN CHIEF BY/INTERROGATOIRE EN-CHEF PAR**
10 **Me JEAN-PHILIPPE MacKAY:**

11 **Me JEAN-PHILIPPE MacKAY:** Merci beaucoup.

12 Monsieur Perrault, on va commencer par le
13 dépôt en preuve de certains documents. On va commencer par
14 le document WIT 74, qui est le résumé de l'entrevue que nous
15 avons réalisé avec vous le 8 août dernier. Vous étiez à ce
16 moment-là accompagné de monsieur Caron, madame Villeneuve et
17 madame Torosian. C'est un document... en fait, vous voyez ici,
18 c'est la version française, la traduction du résumé original.
19 On peut procéder avec la version française, mais la version
20 originale est le WIT 74.EN.

21 **--- EXHIBIT No. /PIÈCE No. WIT0000074.EN:**

22 Interview Summary - Elections Canada
23 (Stage 2)

24 **--- EXHIBIT No. /PIÈCE No. WIT0000074.FR:**

25 Résumé d'entrevue: Élections Canada
26 (Stéphane Perrault, Serge Caron,
27 Josée Villeneuve et Susan Torosian)

28 **Me JEAN-PHILIPPE MacKAY:** Donc, vous avez eu

1 l'occasion de réviser ce document-là, Monsieur Perrault,
2 avant votre témoignage aujourd'hui?

3 **M. STÉPHANE PERRAULT:** Oui, absolument.

4 **Me JEAN-PHILIPPE MacKAY:** Et vous acceptez
5 que ce document fasse partie de votre preuve?

6 **M. STÉPHANE PERRAULT:** Absolument.

7 **Me JEAN-PHILIPPE MacKAY:** Devant la
8 Commission.

9 **M. STÉPHANE PERRAULT:** Absolument.

10 **Me JEAN-PHILIPPE MacKAY:** Je vais également,
11 Madame la Commissaire, produire, outre la version française,
12 la version anglaise du résumé d'entrevue... trois affidavits
13 qui accompagnent le résumé d'entrevue. Et donc, c'est WIT
14 74.1, .2 et .3 qui sont les affidavits des trois
15 fonctionnaires d'Élections Canada qui accompagnaient monsieur
16 Perrault lors de l'entrevue. Il n'est pas nécessaire de
17 présenter les affidavits.

18 **--- EXHIBIT No./PIÈCE No. WIT0000074.1:**

19 Affidavit of Jose Villeneuve

20 **--- EXHIBIT No./PIÈCE No. WIT0000074.2:**

21 Affidavit of Serge Caron

22 **--- EXHIBIT No./PIÈCE No. WIT0000074.3:**

23 Affidavit of Susan Torosian

24 **Me JEAN-PHILIPPE MacKAY:** Et le deuxième
25 document que je veux produire, Monsieur Perrault, est le
26 rapport institutionnel complémentaire, donc ELC.IR.2. On l'a
27 dans les deux langues officielles. Si c'est possible de
28 présenter le document, ELC.IR.2. Donc document, Monsieur

1 Perrault, qui fait 27 pages. Vous reconnaissez le document
2 qu'on voit à l'écran en ce moment?

3 **M. STÉPHANE PERRAULT:** J'en reconnais ce que
4 j'en vois, mais oui, je suis...

5 **Me JEAN-PHILIPPE MacKAY:** Oui, en fait, on
6 voit une partie de la première page, mais c'est un document
7 qui a été partagé avec la Commission. On l'a dans les deux
8 langues. Et vous reconnaissez que ce document a été préparé
9 par Élections Canada et au nom de l'organisation? Vous en
10 reconnaissez le contenu comme étant... comme faisant partie de
11 votre preuve devant la Commission?

12 **M. STÉPHANE PERRAULT:** Oui. C'est un
13 document qu'on a préparé à la demande de la Commission et
14 qu'on a produit.

15 **Me JEAN-PHILIPPE MacKAY:** Donc, dans les deux
16 langues officielles, Madame la Commissaire, donc, par le
17 suffixe EN et FR, les deux documents sont produits devant
18 vous.

19 **--- EXHIBIT No. /PIÈCE No. ELC.IR.0000002.FR:**

20 Elections Canada's Supplementary
21 Institutional Report August 2024

22 **--- EXHIBIT No. /PIÈCE No. ELC.IR.0000002.EN:**

23 Rapport institutionnel supplémentaire
24 d'élections Canada

25 **Me JEAN-PHILIPPE MacKAY:** Donc, Monsieur
26 Perrault, je vais commencer. Vous avez témoigné devant la
27 Commission au mois de mars dernier, et vous avez expliqué à
28 cette occasion le mandat d'Élections Canada et le rôle du

1 directeur général des élections, mais je vais vous demander
2 de revenir et de nous expliquer quel est le mandat
3 d'Élections Canada, de manière générale, et quel est votre
4 rôle à titre de directeur général des élections?

5 **M. STÉPHANE PERRAULT:** Alors, à titre de
6 directeur général des élections, je suis le dirigeant
7 principal de l'organisme Élections Canada. Je suis, en fait,
8 techniquement le dirigeant principal du bureau du directeur
9 général des élections, qui inclut aussi le bureau de la
10 commissaire, mais qui œuvre de manière indépendante
11 d'Élections Canada.

12 Et Élections Canada a pour mandat
13 l'administration - le mandat principal - l'administration des
14 élections fédérales, que ce soit des élections partielles ou
15 des élections générales. Ça inclut la nomination des
16 quelques, maintenant, 343 directeurs et directrices du
17 scrutin, qui, eux, embauchent évidemment le personnel lors
18 d'une élection. Ça inclut la tenue de campagnes
19 d'information aux électeurs, notamment, et tous les
20 préparatifs liés à l'élection. Et ça inclut, entre autres
21 choses, l'administration des règles de financement politique.
22 Donc, les audits qui ont cours après une élection pour
23 vérifier la conformité des rapports des différents
24 participants au processus électoral.

25 **Me JEAN-PHILIPPE MacKAY:** Et j'ai oublié de
26 le mentionner, Monsieur Perrault, mais puisqu'il y a de
27 l'interprétation simultanée dans les langues officielles,
28 également en langage des signes, je vais vous demander, s'il

1 vous plait, de ne pas trop parler rapidement. Si tant est
2 que la chose soit possible. Mais je vais vous le rappeler si
3 je vois que le rythme est un peu trop rapide, donc je vous le
4 signale.

5 **Me STÉPHANE PERRAULT:** Merci. N'hésitez pas.

6 **Me JEAN-PHILIPPE MacKAY:** Et je vous le
7 signalerai à nouveau au besoin.

8 Et rapidement, quel est le rapport entre
9 votre organisation et le Bureau de la commissaire aux
10 élections fédérales?

11 **Me STÉPHANE PERRAULT:** Alors, à titre de
12 directeur général des élections, je suis appelé à nommer le
13 ou la commissaire aux élections fédérales. Je le fais en
14 consultation avec la directrice des poursuites pénales, comme
15 le prévoit la loi.

16 Mon organisme assure aussi certains aspects
17 administratifs, par exemple au niveau des TI, de
18 l'utilisation des locaux pour le Bureau de la commissaire.
19 Mais la commissaire opère de façon entièrement indépendante
20 dans les décisions qu'elle prend de mener des enquêtes et des
21 choix qu'elle prend pour l'exécution de la loi.

22 **Me JEAN-PHILIPPE MacKAY:** Et très rapidement,
23 est-ce que c'est dans ce contexte que les... on en a discuté
24 lors de l'entrevue, lorsque le Bureau de la commissaire aux
25 élections fédérales souhaite obtenir des infrastructures, par
26 exemple, traitées durant le renseignement classifié, on
27 comprend que vous avez un rôle à jouer avec..

28 **Me STÉPHANE PERRAULT:** On a un rôle, comme je

1 disais, de soutien administratif, alors, oui, on est en ce
2 moment en train de mettre sur pied des installations pour lui
3 permettre de conserver des documents de niveau très secret.

4 **Me JEAN-PHILIPPE MacKAY:** Et on va en discuter
5 un peu plus tard de la question de l'obtention du
6 renseignement, mais maintenant qu'on parle de ce dossier,
7 pouvez-vous nous expliquer rapidement, vous en faites état
8 lors de l'entre... vous en avez fait état lors de l'entrevue,
9 mais est-ce qu'Élections Canada ressent le besoin d'avoir
10 accès à de tels locaux sur place dans les bureaux d'Élections
11 Canada ou c'est pas quelque chose qui est nécessaire?

12 **Me STÉPHANE PERRAULT:** Donc, pour nous, on est
13 des consommateurs de renseignement, mais pas au même niveau
14 que la commissaire l'est. Pour nous, ce n'est pas nécessaire
15 d'avoir... de pouvoir conserver sur place des niveaux... des
16 documents de niveau très secret. On peut nous le présenter,
17 au besoin. Ça arrive rarement. Et on a, plus régulièrement,
18 là, on est exposés à de la documentation de niveau secret, si
19 on est outillés pour conserver ces documents-là.

20 **Me JEAN-PHILIPPE MacKAY:** Excellent. Sur la
21 question de l'ingérence étrangère, est-ce que vous pouvez
22 nous expliquer de manière générale – et on va entrer dans des
23 sujets un peu plus spécifiques par la suite –, de manière
24 générale, la manière dont le thème ou le sujet de l'ingérence
25 étrangère interagit avec le mandat d'Élections Canada.

26 **Me STÉPHANE PERRAULT:** Alors, Élections Canada
27 est responsable d'une certaine façon de la sécurité du
28 processus électoral, et quand je parle de sécurité, je parle

1 de sécurité de ses infrastructures physiques, sécurité aussi
2 de ses systèmes informatiques et de ses données. Alors, on
3 travaille pour ça en étroite collaboration avec le Centre
4 canadien de cybersécurité qui ont une expertise là-dedans,
5 mais on a un rôle, nous, à jouer pour cette sécurité-là.

6 Alors, on assure aussi la sécurité de
7 l'information dont disposent les électeurs pour pouvoir
8 voter, donc pour s'assurer que les électeurs ne soient pas
9 l'objet de mésinformation ou de désinformation sur le
10 processus électoral. On informe les électeurs, mais aussi on
11 fait une veille de l'environnement, tant des médias sociaux
12 que des médias, pour s'assurer que s'il y a de l'information
13 qui est inexacte sur le processus électoral, et surtout qui
14 pourrait induire les électeurs en erreur sur la manière ou le
15 moment de voter, qu'on puisse s'assurer de fournir
16 l'information exacte.

17 Alors, évidemment, ces enjeux-là de sécurité
18 peuvent chevaucher avec des situations d'interférence
19 étrangère. De la même façon, Élections Canada – je
20 l'indiquais il y a quelques instants – administre les règles
21 de financement politique, donc pour s'assurer que l'argent
22 qui circule dans le processus politique est fait de façon
23 conforme à la *Loi électorale du Canada*, et encore là, ça peut
24 avoir... il y a des éléments d'ingérence étrangère qui peuvent
25 intéresser mon bureau sous cet aspect-là.

26 Et donc, de façon générale, nous ne sommes
27 pas des experts en sécurité nationale, nous ne sommes donc,
28 un rôle de premier plan sur l'ingérence étrangère, mais nous

1 devons assurer la sécurité du processus électoral, et il y a
2 des aspects là-dedans certainement d'ingérence étrangère qui
3 nous intéressent.

4 **COMMISSAIRE HOGUE:** Monsieur Perrault, quand
5 vous dites que vous faites ou votre organisation fait une
6 veille de l'information qui circule...

7 **Me STÉPHANE PERRAULT:** Oui.

8 **COMMISSAIRE HOGUE:** ...est-ce que c'est
9 l'information qui est en lien avec le processus électoral,
10 par exemple quand voter, comment voter, qu'est-ce qu'il faut
11 présenter, ou est-ce que c'est plus large que ça et vous
12 regardez également le contenu, par exemple, des informations
13 qui peuvent justement circuler?

14 **Me STÉPHANE PERRAULT:** Alors, notre veille
15 vise essentiellement le processus électoral. Ça inclut...

16 J'entends un écho dans la voix là.

17 ...ça inclut des... des inf... du rensei... de
18 l'information sur quand, comment voter, ça peut inclure aussi
19 des choses comme lors du jour du scrutin s'il y a des routes
20 qui sont bloquées ou des choses qui peuvent interférer avec
21 le vote, ou la perception qu'ont les Canadiens du processus
22 électoral et d'Élections Canada.

23 Mais c'est important de souligner qu'on ne
24 s'intéresse pas au discours partisan pour ou contre des
25 partis ou des candidats, alors c'est évident que quand on
26 fait des recherches avec des mots-clés comme « vote
27 élections », on prend dans nos filets, si je peux dire,
28 toutes sortes de conversations qui sont publiques, on ne

1 rentre pas dans les bulles privées, mais qui peuvent avoir un
2 caractère partisan, mais notre lentille est vraiment sur le
3 processus de vote et s'assurer que les Canadiens et
4 Canadiennes puissent voter. Donc, c'est une lentille qui est
5 différente.

6 On n'a pas d'expertise particulière qui nous
7 permettrait de détecter ce qui est étranger, ce qui est
8 domestique. On fait de la veille dans une quinzaine de
9 langues, mais de là à savoir si ce sont des gens qui
10 s'expriment au Canada ou ailleurs ou s'ils sont influencés
11 par des gens qui viennent d'ailleurs, ça, on n'a pas cette
12 expertise-là.

13 **COMMISSAIRE HOGUE:** Merci.

14 **Me JEAN-PHILIPPE MacKAY:** Monsieur Perrault,
15 je vais... on va aborder immédiatement la question de la
16 désinformation, on va vider cette question et on reviendra
17 par la suite à la question de la sécurité des élections et
18 des interactions que vous avez avec d'autres agences
19 gouvernementales.

20 Pour ce qui est de la désinformation, vous
21 avez abordé ce sujet lors de votre témoignage antérieur
22 devant la Commission, mais est-ce que vous pouvez nous
23 expliquer brièvement l'infrastructure qui est présente au
24 sein d'Élections Canada pour faire le travail que vous venez
25 de décrire à Madame la Commissaire, donc le travail de
26 surveillance ou de vigie des médias sociaux, et de quelle
27 manière, en fait, vous générez... est-ce qu'il y a des produits
28 qui sont générés, par exemple est-ce que c'est échangé avec

1 d'autres partenaires gouvernementaux ou autres. Donc,
2 j'aimerais que vous nous présentiez le portrait de
3 l'organisation interne d'Élections Canada sur cette question.

4 **Me STÉPHANE PERRAULT:** Alors, on a une équipe
5 qui est dédiée à la veille des médias sociaux qui, lors de la
6 dernière élection, faisait la veille dans 15 langues de 67
7 plateformes – les plateformes évoluent avec le temps, y'en a
8 des nouvelles et certainement que le nombre sera appelé peut-
9 être à augmenter lors de la prochaine élection générale –,
10 fait une veille en continu, donc, pas uniquement pendant les
11 élections, mais aussi entre les élections pour comprendre
12 les... – je vais prendre une expression qui est peut-être un
13 anglicisme – les narratifs, les trames narratives qu'on
14 entend au sujet du processus électoral. Donc, on s'intéresse
15 à ce qui se passe dans les élections provinciales, dans ce
16 qui se passe dans les élections américaines, pour comprendre
17 les types de sujet qui sont susceptibles de donner lieu à de
18 la mésinformation au sujet du processus électoral.

19 On constate que les thèmes sont souvent
20 communs entre les juridictions, les préoccupations des
21 électeurs où la mauvaise information est souvent commune.

22 Donc, on fait cette veille-là en continu et
23 on produit des rapports hebdomadaires sur les tendances et
24 les grands thèmes qu'on recèle dans les médias sociaux. En
25 matière... en période électorale, on fait des rapports qui sont
26 quotidiens, donc on augmente la fréquence de ces rapports-là.
27 Et ces rapports-là sont partagés avec nos partenaires en
28 matière de sécurité, évidemment avec la Commissaire aux

1 élections fédérales, avec nos partenaires de sécurité qui
2 sont membres du groupe SITE – vous excuserez l’acronyme
3 anglais, mais il est mieux connu sous ce nom-là –, et avec le
4 Groupe de réponse rapide aux Affaires mondiales. Donc, ces
5 gens-là ont accès à ce qu’on recèle dans cette veille des
6 médias sociaux là, mais ce sont des... enfin, c’est de
7 l’information qu’on collecte pour nos fins à nous et qu’on
8 partage.

9 **Me JEAN-PHILIPPE MacKAY:** Est-ce que vous..
10 lorsqu’on regarde votre rapport institutionnel, vous parlez
11 de l’intention qui est derrière la désinformation ou encore
12 des questions d’attribution, ce ne sont pas des choses qui
13 sont... qui font l’objet de recherches ou d’un travail précis
14 au sein d’Élections Canada. Donc, pouvez-vous nous expliquer
15 brièvement la raison pour laquelle c’est de déterminer
16 l’intention qui peut sous-tendre la désinformation ou encore
17 la source de la désinformation, pourquoi ces choses-là ne
18 sont pas nécessairement examinées.

19 **Me STÉPHANE PERRAULT:** Alors, effectivement,
20 pour nous, ce qui est important, c’est que l’information
21 disponible aux Canadiens et aux Canadiennes soit de
22 l’information qui soit juste, qu’ils ne soient pas
23 mésinformés sur le processus. Donc, de comprendre les
24 intentions derrière le contenu qu’on retrouve n’est pas
25 particulièrement utile pour ça. Ça peut être utile pour
26 certains de nos partenaires en matière de sécurité, ça peut
27 être utile pour la Commissaire dans certains cas
28 d’infractions où il y a un élément intentionnel qui est

1 important, mais pour ce qui est d'informer les Canadiens,
2 c'est pas un exercice auquel on se livre.

3 On a souvent du contenu dans les médias
4 sociaux qui circule beaucoup; le même contenu peut, selon la
5 personne qui le partage, être animé d'une intention mauvaise
6 ou pas. On peut parler de mésinformation ou de désinformation
7 parce qu'il y a plusieurs personnes qui partagent le même
8 contenu. Alors, dans notre cas, c'est pas utile de savoir ça.

9 Ce n'est pas non plus utile et on n'a pas
10 l'expertise pour déterminer la source de l'information.
11 Alors, on fait la veille dans une quinzaine de langues, comme
12 je l'indiquais; le fait que ça soit de l'information en
13 langues étrangères, c'est-à-dire et en français et en
14 anglais, ne signifie pas pour autant que c'est de l'ingérence
15 étrangère, évidemment. Et donc, pour nous, la source, c'est
16 pas quelque chose qu'on est capable ni c'est pas quelque
17 chose qui est utile pour s'assurer que le contenu soit juste.

18 **Me JEAN-PHILIPPE MacKAY:** Et maintenant, quand
19 vous... lorsqu'il y a des éléments, par exemple, qui sont
20 détectés qui peuvent induire les électeurs en erreur, quelle
21 est la réponse, de quelle manière Élections Canada réagit
22 face à ce type d'informations là?

23 **Me STÉPHANE PERRAULT:** Le principal mécanisme
24 – hein? – c'est de s'assurer que notre contenu est ajusté
25 pour amplifier certains messages clés qui poussent
26 l'information juste auprès des électeurs. Alors, oui, on peut
27 aussi intervenir auprès des plateformes numériques, on peut
28 indiquer qu'il y a un message qui est inexact, et les

1 plateformes numériques ont chacune leurs politiques pour
2 traiter de ça, mais typiquement, on ne demande pas le retrait
3 de l'information. À date, on a trouvé que c'était efficace de
4 signaler des erreurs sur l'information et, de notre côté, de
5 pousser de l'information, de rendre disponible de
6 l'information qui est exacte.

7 Et une des motivations derrière la veille
8 qu'on fait en dehors des élections, c'est pour constamment
9 ajuster nos messages pour s'assurer qu'on est au diapason
10 avec les conversations qui ont cours sur le processus
11 électoral.

12 **Me JEAN-PHILIPPE MacKAY:** Et de quelle manière
13 Élections Canada diffuse ses messages de manière générale?
14 Pas nécessairement en réponse à un incident de mésinformation
15 ou de désinformation, mais de manière générale, comment
16 Élections Canada s'y prend pour...

17 **Me STÉPHANE PERRAULT:** Diffuser de
18 l'information? Alors, il y a plusieurs mécanismes, je vais
19 devoir élaborer un peu. Alors, on a... j'ai dans mon mandat un
20 mandat d'informer les Canadiens sur le processus électoral.
21 Il y a quatre grands axes dans ce mandat-là. Le premier,
22 qu'on appelle la campagne d'information des électeurs, qui
23 est le plus général, c'est un mandat d'informer l'ensemble de
24 la population sur le processus électoral, soit par notre site
25 web où on a beaucoup de contenu relatif au processus
26 électoral, soit en période électorale par des campagnes
27 publicitaires, ou la carte d'information d'électeur, ou le
28 guide aux électeurs.

1 Tout ça, ce sont des produits qui visent la
2 population générale et qui typiquement dirigent les Canadiens
3 vers notre site web où là il y a de l'information plus
4 détaillée. Donc, cet axe-là est l'axe, si on veut, le plus
5 général de notre mandat d'information.

6 On a aussi des agents de relations
7 communautaires qui sont engagés pendant la période électorale
8 par les directeurs et les directrices de scrutin. À la
9 dernière élection, il y en avait quelque 1 500
10 approximativement. Et ce sont de gens qui sont embauchés pour
11 travailler auprès de groupes au sein des communautés qui
12 peuvent vivre certaines barrières à la participation
13 électorale. Donc, on parle des sans-abris, on parle
14 d'Autochtones, on parle de groupes ethnoculturels, on parle
15 de jeunes, de personnes âgées surtout en centres de soins.

16 Donc, les directeurs et directrices de
17 scrutin, en fonction de la composition de leurs communautés,
18 embauchent ces personnes-là qui œuvrent auprès de ces
19 communautés-là pour les informer, mieux les informer sur le
20 processus électoral.

21 Au niveau ethnoculturel, pour donner un ordre
22 de grandeur, il y en avait environ 200 à la dernière élection
23 générale. Donc, ça, c'est les agents de relations
24 communautaires.

25 **Me JEAN-PHILIPPE MacKAY:** Si vous me
26 permettez, Monsieur Perrault, sur ce point-là...

27 **Me STÉPHANE PERRAULT:** Oui.

28 **Me JEAN-PHILIPPE MacKAY:** ...dans le cadre de la

1 première entrevue qui a été menée avec vous, il a été
2 mentionné que dans le contexte de discussions entourant
3 l'ingérence étrangère, la question du secret du scrutin avait
4 été soulevée comme étant une préoccupation qui pouvait
5 exister au sein de certaines communautés. Est-ce que c'est
6 par l'entremise de ces agents de relations communautaires ou
7 encore les campagnes d'information que ce type de... je
8 l'utilise comme exemple, ce type de préoccupation là liée au
9 secret du scrutin, est-ce que c'est de cette manière-là
10 qu'Élections Canada répond pour s'assurer que les voteurs de
11 toutes catégories puissent bien connaître les mécanismes de
12 protection de...

13 **Me STÉPHANE PERRAULT:** Alors, on a augmenté
14 dans les derniers mois le contenu en termes de mécanismes de
15 protection dans l'ensemble de nos mécanismes de
16 communications. Alors, oui, c'est vrai, il y a des agents de
17 relations communautaires qui sont outillés d'informations qui
18 « est » plus explicites sur la question, entre autres, du
19 secret du vote, qui est un aspect, je pense, qui est très
20 important de comprendre pour les personnes qui pourraient
21 autrement se sentir intimidées ou avoir des préoccupations
22 quant à leur participation électorale, donc on a augmenté ça.

23 Mais c'est pas le seul mécanisme. On a – et
24 là, j'en arrive au troisième volet de notre mandat
25 d'information –, on a un programme qui s'appelle « Inspirer
26 la démocratie », c'est un programme qui fait appel à un
27 réseau de groupes communautaires qui ont des relations
28 privilégiées avec certaines communautés au sein de la

1 population. C'est un réseau de quelque 800 intervenants qui
2 utilisent du matériel qu'on prépare pour eux pour que les
3 gens comprennent mieux comment se fait la participation
4 électorale, que ça soit comme électeur, comme candidat, ou
5 même comme travailleur électoral.

6 Et donc, parmi les 800, il y en a, je crois,
7 une centaine qui sont des groupes pour lesquels on émet un
8 contrat, on leur soumet des tâches particulières, mais le
9 reste le font de façon volontaire, et il y en a une
10 quarantaine qui sont vraiment des groupes qui œuvrent auprès
11 des communautés ethnoculturelles. Alors, là aussi, le contenu
12 sur les mesures de protection a été rehaussé et inclut le
13 secret du vote.

14 Et on a finalement l'éducation citoyenne qui
15 vise principalement les jeunes, les non-électeurs, où on a
16 des programmes pour utilisation dans les écoles qui, là
17 aussi, il y a du contenu qui a été rehaussé en termes de
18 protection du processus électoral.

19 Donc, ça, c'est les grands mécanismes, en
20 gros, qu'on utilise pour informer les Canadiens.

21 **Me JEAN-PHILIPPE MacKAY:** Et sur...

22 J'aimerais qu'on mette WIT74 à l'écran.

23 Et je vais attirer votre attention sur le
24 paragraphe 28, Monsieur Perrault, et j'aimerais vous entendre
25 sur le sujet qu'on a abordé pendant l'entrevue sur certaines
26 informations qui donnent à penser que des États étrangers
27 peuvent instrumentaliser certains groupes ou organismes
28 communautaires au Canada comme étant des intermédiaires dans

1 un contexte d'ingérence étrangère, et j'aimerais que vous
2 élaboriez un peu sur ce sujet.

3 Puisqu'Élections Canada fait affaire avec des
4 groupes communautaires, est-ce qu'il y a une... est-ce que
5 c'est une préoccupation ou, en fait, un élément qui est
6 présent à votre esprit lorsque vous engagez ou vous
7 interagissez ou travaillez avec des... certains groupes?

8 **Me STÉPHANE PERRAULT:** Alors, comme je
9 l'indiquais lors de mon entrevue, parce que c'était en
10 réaction à une question qu'on m'avait posée, on n'a pas de
11 mécanisme dans lequel on vérifie auprès des services de
12 renseignement ces groupes-là. Mais c'est important de garder
13 à l'esprit que ce sont des groupes qu'on outille avec de
14 l'information que nous avons préparée, de l'information qui
15 est exacte sur le processus électoral. Donc, ils partent
16 outillés avec des produits d'Élections Canada.

17 Alors, dans ce sens-là, je ne suis pas
18 préoccupé que ces outils-là servent à faciliter de
19 l'interférence étrangère. Non.

20 **Me JEAN-PHILIPPE MacKAY:** Et quand vous
21 mentionnez que la seule... en fait, une surveillance qui est
22 cependant importante, c'est au niveau... vous ne voulez pas que
23 les groupes utilisent ces occasions-là pour faire des
24 activités partisans ou encore tenter d'influencer le vote
25 là.

26 **Me STÉPHANE PERRAULT:** Alors, ils peuvent
27 avoir des activités partisans. On a... les gens qui ne sont
28 pas en relation contractuelle avec nous n'ont pas

1 l'obligation de neutralité. On donne ces produits-là
2 notamment aux partis politiques pour qu'ils s'en servent
3 lorsqu'ils recrutent des candidats. Donc, parmi les 800, il y
4 a des groupes qui peuvent avoir des orientations partisans.

5 Les groupes qui travaillent en relation
6 contractuelle avec Élections Canada ont une obligation de
7 neutralité, et ça, on veille à ça. Donc, il y a un mélange,
8 si on veut, de groupes, mais tous ces groupes-là utilisent
9 des produits qui ont été... qui leur ont été fournis par
10 Élections Canada et qui reflètent véritablement des éléments
11 du processus électoral canadien.

12 **Me JEAN-PHILIPPE MacKAY:** Et, en fait, vous
13 avez les quatre... les quatre programmes que vous venez
14 d'énumérer s'inscrivent un peu dans la manière dont on a
15 abordé le sujet lors de l'entrevue, c'était certains groupes
16 de Néo-Canadiens qui peuvent subir des formes de répression
17 transnationale, et de quelle manière Élections Canada répond
18 à certaines préoccupations ou à certains... certaines
19 conséquences de certaines formes d'intimidation qui peuvent
20 tenter d'influencer les Canadiens à ne pas aller voter, par
21 exemple, ou à voter dans un certain sens en fonction des
22 pressions qu'ils puissent subir?

23 **Me STÉPHANE PERRAULT:** Alors, vraiment, c'est
24 un sujet de préoccupations et c'est un sujet qui intéresse
25 d'autres organismes qu'Élections Canada, mais de notre point
26 de vue, je dirais qu'il y a deux éléments qui sont à mettre
27 en lumière.

28 D'abord, une des choses qu'on doit bien

1 expliquer aux électeurs, aux électrices, c'est le fait qu'il
2 existe une multitude de façons de voter. Que ça soit au
3 bureau de scrutin le jour du vote, que ça soit au vote par
4 anticipation, ça peut être par la poste, ça peut être au
5 bureau du directeur de scrutin, ça peut même être au bureau
6 d'un autre directeur de scrutin en contexte urbain où il y a
7 plusieurs circonscriptions. Un électeur peut se présenter à
8 n'importe quel bureau de directeur de scrutin pour qu'il ou
9 elle se sente à l'aise de voter. Donc, ça, c'est un élément.

10 L'autre élément, on l'a mentionné, c'est le
11 caractère secret du vote. Alors, il y a des processus en
12 place pour s'assurer que le vote demeure secret et les
13 Canadiens doivent être rassurés quant au fait que personne ne
14 peut connaître la manière dont ils ont voté.

15 **Me JEAN-PHILIPPE MacKAY:** Une dernière
16 question sur ce thème. Au niveau de l'accessibilité de
17 l'information, quelles sont les mesures mises en place par
18 Élections Canada pour s'assurer que l'information puisse être
19 communiquée dans un... selon un moyen qui est compris par les
20 Canadiens qui parlent pas nécessairement le français ou
21 l'anglais?

22 **M. STÉPHANE PERRAULT:** Oui. Alors, on a une
23 gamme de produits qui sont principalement le guide de
24 l'électeur, qui est disponible en 51 langues, c'est-à-dire 49
25 langues plus l'anglais et le français. Ça inclue 16 langues
26 autochtones et 33 autres langues qui sont parlées à travers
27 le pays.

28 On a aussi produit un - pour la prochaine

1 élection - un guide pour les médias culturels ou aux langues
2 autres que l'anglais et le français, en particulier pour
3 mandarin et cantonais et punjabi. Donc, pour expliquer le
4 processus, mais expliquer aussi les mécanismes de protection
5 du vote dans le processus électoral.

6 Donc, on a quand même une gamme
7 d'information. Les électeurs aussi peuvent communiquer
8 auprès d'Élections Canada et on a un service d'interprétation
9 qui permet là dans une très large... très large nombre de
10 langues. Je crois que c'est pas loin de 200 qui peuvent... 200
11 langues qui peuvent être utilisées en l'interprétation auprès
12 des Canadiens.

13 **M. JEAN-PHILIPPE MacKAY:** On va revenir sur
14 la question de la désinformation, mésinformation. Dans le
15 résumé d'entrevue - et on l'a à l'écran - on peut aller au
16 paragraphe 54. C'est au niveau de la relation avec le
17 mécanisme de réponse rapide d'Affaires mondiales Canada. Et
18 il a été mentionné, c'est madame Torosian, je crois, qui nous
19 a mentionné que Élections Canada tente de conclure... ou tente
20 encore de conclure un accord sur le partage d'information
21 avec Affaires mondiales afin de formaliser la relation. Et
22 on nous expliquait que l'objectif est que cet accord serait
23 en vigueur d'ici à la 45^e élection générale. On comprend que
24 vous avez une relation avec le mécanisme de réponse rapide,
25 mais quel est l'objectif de cet accord? Quel serait
26 l'objectif pour formaliser? Quand on lit ça, qu'est-ce que
27 ça veut dire exactement?

28 **M. STÉPHANE PERRAULT:** Ben, c'est pour donner

1 une certaine clarté qu'en aux circonstances... qu'est-ce qui
2 est partagé à quel moment et à qui. Donc, essentiellement
3 encadrer les attentes de part et d'autre des deux organismes.
4 Donc, ça se fait de manière informelle en ce moment, mais on
5 pense que c'est souhaitable d'avoir un cadre plus précis sur
6 le partage de l'information.

7 **M. JEAN-PHILIPPE MacKAY:** Et est-ce que
8 Élections Canada a des rapports sur le thème de la
9 désinformation, de la mésinformation en lien avec le
10 processus électoral? Est-ce qu'Élections Canada a des
11 rapports avec d'autres agences ou d'autres ministères au sein
12 du gouvernement canadien?

13 **M. STÉPHANE PERRAULT:** Donc, on partage nos
14 rapports avec différents partenaires à travers le groupe...
15 vous avez employé l'acronyme SITE tout à l'heure, qui est un
16 groupe qui regroupe les Affaires mondiales, le SCRS, la GRC
17 et le Centre canadien de sécurité des communications. C'est
18 un groupe qui est actif en période électorale, y inclus
19 depuis le printemps 2023. On va peut-être y venir en période
20 d'élection partielle, mais il y a aussi le groupe de
21 coordination en matière de sécurité électorale qui existe au
22 niveau DG, sous-ministre adjoint et sous-ministre, qui est un
23 groupe qui permet de regrouper un nombre plus large de
24 partenaires en matière de sécurité. Et c'est vraiment à
25 travers... par le truchement, si on veut, de ce groupe de
26 travail-là que l'information circule.

27 **M. JEAN-PHILIPPE MacKAY:** Donc, on va venir à
28 ces structures dans quelques instants. Mais avant, vous avez

1 mentionné lors de notre entrevue avec vous cet été que
2 l'intelligence artificielle était une préoccupation pour vous
3 et c'était quelque chose qui devait être surveillé. En fait,
4 on devait répondre à la menace grandissante de l'intelligence
5 artificielle dans le domaine de l'influence de l'information
6 dans l'écosystème de l'information. Et j'aimerais vous
7 entendre sur cette préoccupation-là que vous avez partagée
8 avec nous.

9 **M. STÉPHANE PERRAULT:** Alors, c'est un
10 phénomène qui est évidemment émergent et qui évolue très
11 rapidement. Le Centre canadien pour la cybersécurité en
12 parle dans ses rapports réguliers. Il y a le phénomène
13 évidemment de l'hyper-trucage, qu'on appelle en anglais les
14 « *deepfakes* », qui est une préoccupation. On va observer
15 évidemment ce qui se passe sous les élections américaines là-
16 dessus.

17 J'aurai l'occasion, possiblement, dans le
18 contexte du projet de loi C-65, de comparaître en comité. Je
19 crois qu'il y a des mesures qu'on peut prendre pour à tout le
20 moins interdire certaines formes d'hyper-trucage. Alors ça,
21 c'est un aspect. On n'a pas vu ça de façon importante à date
22 au Canada, mais on sait que ça existe dans d'autres pays; au
23 Royaume-Uni, en Angleterre, c'est un phénomène qui est réel.

24 Il y a aussi toute la question de
25 l'intelligence artificielle pour les moteurs de recherche et
26 générer de l'information qui pourrait s'avérer inexacte sur
27 le processus électoral. Donc, on a l'intention de discuter
28 avec les plateformes, les producteurs de moteurs de recherche

1 qui utilisent l'intelligence artificielle pour s'assurer que
2 l'information qui est produite grâce à l'intelligence
3 artificielle ne soit pas de l'information trompeuse, que ce
4 soit amplifier des faux renseignements sur le processus
5 électoral.

6 **M. JEAN-PHILIPPE MacKAY:** Donc, maintenant,
7 je vais vous montrer un document, Monsieur Perrault, qui va
8 servir de point de départ pour la suite de mes questions. On
9 peut mettre à l'écran CAN 4599, CAN 4599.

10 **--- EXHIBIT No./PIÈCE No. CAN004599:**

11 Site Status Update and Summary of
12 Foreign Interference Threats to
13 Canadian Democratic Institutions-2023

14 **M. JEAN-PHILIPPE MacKAY:** Donc, c'est un
15 document, Monsieur Perrault, simplement pour vous situer,
16 c'est une mise à jour du Groupe de travail SITE, MSRE,
17 l'acronyme est MSRE en français, mais on peut continuer à
18 parler de SITE, puisque c'est probablement plus simple pour
19 se faire comprendre si on utilise l'acronyme consacré en
20 anglais. Et donc, c'est une mise à jour au comité de sous-
21 ministres, auquel vous avez fait allusion un peu plus tôt,
22 sur la coordination sur la sécurité électorale.

23 Et en fait, ma question, lorsqu'on regarde le
24 premier paragraphe, on décrit les élections comme étant une
25 fenêtre d'opportunité. Donc, le texte est en anglais, *window*
26 *of opportunity*, mais une fenêtre d'opportunité sur le plan de
27 l'ingérence ou de la menace d'ingérence étrangère. Donc,
28 lorsqu'on regarde en fait la question de la sécurité

1 électorale, est-ce que vous... cette manière de décrire les
2 élections, est-ce que vous partagez cette vision des choses
3 lorsque on parle d'élections, d'ingérence étrangère en lien
4 avec les élections? Est-ce que vous voyez les élections
5 comme étant un point qu'on pourrait qualifier de plus
6 critique sur le plan de la sécurité et des menaces
7 d'ingérence étrangère?

8 **M. STÉPHANE PERRAULT:** Écoutez, vous m'amenez
9 au-delà de mon expertise. C'est quelque chose qui m'apparaît
10 tout à fait crédible et plausible, mais je pense que c'est
11 pas à moi à me prononcer sur ça. C'est quelque chose à
12 laquelle je suis extrêmement sensible, évidemment, en
13 particulier de par les interactions qu'on a avec nos
14 partenaires en matière de sécurité, mais c'est leur parole
15 qu'il faut prendre là-dessus.

16 **M. JEAN-PHILIPPE MacKAY:** En fait, c'est
17 plutôt en ce qui a trait à votre compétence ou à votre
18 mandat.

19 **M. STÉPHANE PERRAULT:** Oui.

20 **M. JEAN-PHILIPPE MacKAY:** Et on comprend que
21 votre mandat, puisque les élections sont probablement le
22 processus démocratique par excellence, est-ce que ce risque
23 ou cette menace qui pèse sur les élections influence la
24 posture qu'Élections Canada peut prendre au niveau de la
25 protection de sa propre sécurité et de la sécurité des
26 élections?

27 **M. STÉPHANE PERRAULT:** C'est-à-dire que ça a
28 influencé certainement l'ampleur des mécanismes qu'on a mis

1 en place. Alors, comme je disais tout à l'heure, on n'est
2 pas à même de faire une distinction, par exemple, en matière
3 de cyberattaques, s'il y a des cyberattaques étrangères, en
4 matière de mésinformation ou de désinformation, si ça vient
5 de sources étrangères.

6 On est cependant conscient qu'il y a cette
7 fenêtre d'opportunité, qu'il y a cet intérêt de certains
8 états pour influencer le processus. Et donc, ça, ça augmente
9 le niveau de risque. Donc, tout ce qu'on fait pour sécuriser
10 le processus électoral, bien que ça ne vise pas
11 spécifiquement l'ingérence étrangère, certainement que ça a
12 été motivé en grande partie par l'augmentation de la menace
13 qu'on a vue, surtout, je dirais, à partir là des années 2016-
14 2017.

15 Évidemment, ça remonte à avant ça, mais il y
16 a eu une accélération à partir de ce moment-là de nos efforts
17 en cette matière-là, qui était motivée par... qui a été générée
18 par la suite de constats et d'informations qu'on a reçues sur
19 les risques que présente l'ingérence étrangère.

20 **M. JEAN-PHILIPPE MacKAY:** Et sur ce point-là,
21 quand vous parlez du... de l'appareil de comités concernant la
22 coordination de la sécurité des élections, j'aimerais vous
23 entendre - vous en avez discuté lors de votre premier
24 témoignage - mais j'aimerais que vous reveniez sur les
25 origines de cet appareil de coordination de sécurité des
26 élections et de quelle manière ces comités opèrent, en fait,
27 en ce qui concerne votre rapport à ces comités-là et votre
28 participation.

1 **M. STÉPHANE PERRAULT:** Alors, il faut
2 remonter à l'élection présidentielle de 2016. Il y avait
3 aussi le référendum au Royaume-Uni sur le Brexit. On a vu
4 dans les deux cas des situations de préoccupation d'ingérence
5 étrangère dans les deux événements. Je pense que c'était en
6 janvier ou février 2017. Suite à ça, j'ai rencontré des
7 responsables au Conseil privé et au Centre canadien de
8 sécurité et des communications pour augmenter la
9 collaboration avec les agences de sécurité.

10 Il faut savoir qu'auparavant, il y avait
11 toujours des exercices de sécurité avant une élection. On
12 faisait spécifiquement une rencontre avec des partenaires en
13 matière de sécurité. On discutait de scénarios. Typiquement
14 des situations soit possiblement de terrorisme qui pourraient
15 survenir dans le contexte d'une élection ou de désastre
16 naturel ou d'incident sécuritaire de quelque nature que ce
17 soit. Mais beaucoup plus physique que cybernétique. Et
18 beaucoup moins axé sur la désinformation ou la
19 mésinformation. C'était beaucoup la sécurité physique qui
20 était discutée.

21 Et donc, suite surtout à la présidentielle
22 américaine, où on a vu de l'ingérence par le biais des médias
23 sociaux, on a vu aussi des attaques, des cyberattaques contre
24 les infrastructures, entre autres là, du Parti démocrate
25 américain. J'ai constaté, et j'étais pas le seul,
26 évidemment, qu'il y avait un changement de... assez important
27 dans l'environnement qui justifiait une relation plus
28 étroite, plus continue avec les partenaires en matière de

1 sécurité et qui englobaient d'autres considérations là que
2 celles qui étaient discutées auparavant.

3 Alors ça, ça été mes rencontres. Évidemment,
4 le gouvernement, de son côté, a sans doute fait des
5 réflexions similaires. Quoi qu'il en soit, dans les mois qui
6 ont suivi, il y a eu la mise sur pied de groupe de
7 coordination en matière de sécurité électorale qu'Élections
8 Canada coprécide avec le bureau du Conseil privé. Donc, au
9 niveau DG, au niveau sous-ministre adjoint et au niveau sous-
10 ministre.

11 Et ces rencontres-là qui sont périodiques
12 visent d'abord et avant tout à s'assurer qu'on a une bonne
13 compréhension des mandats respectifs des différents
14 partenaires. Il y a des exercices de mise en situation qui
15 visent à peaufiner, si on veut, les interactions qui
16 pourraient être requises dans des situations particulières.
17 Et il y a aussi dans ce contexte-là typiquement des breffages
18 là au niveau de la situation sécuritaire, l'évolution de la
19 menace. Donc, ça sert à ces différents objectifs-là.

20 Et c'est quelque chose qui a continué
21 d'exister à des fréquences qui ont varié dans le temps, il
22 faut le dire, mais qui a continué d'exister depuis ce moment-
23 là. Donc, avant l'élection de 2019 et qui est bien en place
24 maintenant.

25 **M. JEAN-PHILIPPE MacKAY:** Et maintenant, on
26 est sept ans plus tard, est-ce que vous estimez que cet
27 appareil ou ces comités ont rempli leur mission et
28 remplissent toujours leur mission?

1 **M. STÉPHANE PERRAULT:** Je pense qu'ils sont
2 toujours absolument nécessaires. Il faut comprendre aussi
3 qu'au gouvernement, il y a un roulement continu du personnel.
4 Il y a des gens qui arrivent dans ces organismes-là qui ne
5 connaissent pas spécifiquement le contexte électoral ou les
6 mandats respectifs et qui ne se connaissent pas non plus.

7 Et donc, c'est important parce qu'en
8 situation d'élection, il peut survenir des situations où on
9 doit intervenir rapidement, que les gens se connaissent,
10 qu'ils comprennent leurs mandats, qu'ils ont eu des pratiques
11 valider les interactions et les mandats respectifs de chacun.
12 Donc, je pense que ça continue d'être absolument essentiel.

13 **M. JEAN-PHILIPPE MacKAY:** Et brièvement, quel
14 est le rapport entre les comités de coordination de la
15 sécurité des élections et le Groupe de travail SITE? De
16 quelle manière les deux entités interagissent ensemble?

17 **M. STÉPHANE PERRAULT:** Alors, il y a un
18 certain chevauchement dans les participants. Donc, les
19 partenaires du groupe SITE sont aussi membres du comité de
20 coordination et il y a lors des rencontres un partage de
21 l'information qui vient du groupe SITE.

22 **M. JEAN-PHILIPPE MacKAY:** Et depuis... lors de
23 votre témoignage antérieur devant la Commission, il était
24 question évidemment des 43^e et 44^e élections. Depuis 2021,
25 est-ce qu'il y a eu des nouveautés ou des changements au
26 niveau de la coordination de la sécurité électorale?

27 **M. STÉPHANE PERRAULT:** Alors, la coordination
28 a continué entre les élections. Ce qui est nouveau depuis le

1 printemps 2023, c'est que le gouvernement a décidé de rendre
2 actif le groupe SITE en période d'élection partielle. Donc,
3 auparavant, ce groupe-là n'était actif que pendant les
4 élections générales. Le groupe de coordination continuait,
5 comme je disais tout à l'heure, à des fréquences qui
6 pouvaient être variables. Mais là, on a mis en place et on a
7 rendu actif, si je peux dire, le groupe SITE pendant les
8 périodes d'élections partielles avec des rapports qui
9 suivent. Et pendant ces élections-là, il y a des rencontres
10 régulières avec le groupe de coordination au niveau DG et
11 sous-ministres adjoints pour s'assurer qu'il y a des
12 opportunités de partager l'information, au besoin.

13 **M. JEAN-PHILIPPE MacKAY:** Donc, on aura des
14 témoins du Groupe de travail SITE qui témoigneront devant la
15 Commission. Mais simplement, en ce qui vous concerne, on
16 comprend que pendant les élections générales, vous n'êtes pas
17 membre du Panel des cinq institué par le protocole en cas
18 d'incident... Protocole public en cas d'incident électoral
19 majeur, mais le Protocole prévoit un mécanisme de
20 communication entre le Panel et vous-même, puisque certaines
21 annonces, s'il y a un incident qui touche l'administration
22 des élections, on comprend que ce sera pas le Panel qui va
23 être responsable de faire une annonce publique, mais ce sera
24 vous. C'est exact? C'est une façon...

25 **M. STÉPHANE PERRAULT:** Exact. Donc, on a
26 séparé... évidemment, ça reflète l'indépendance dont jouit
27 Élections Canada par rapport au gouvernement, nos partenaires
28 en matière de sécurité. Donc, on collabore - on collabore

1 assez étroitement - mais on a chacun nos imputabilités
2 propres. Et donc, le Panel de cinq, comme on l'appelle
3 parfois, n'inclut pas le directeur général des élections. Je
4 ne fais pas partie de ce Panel-là.

5 Mais il y a une compréhension que s'il devait
6 y avoir une annonce de part et d'autre qui concerne la
7 sécurité des élections, les partis seraient informés. Il y a
8 une compréhension que si c'est un enjeu qui touche
9 strictement l'administration électorale et qui relève de mon
10 mandat, et que je sentais le besoin de faire une annonce
11 publique pour rassurer les Canadiens ou informer les
12 Canadiens, ce serait moi qui ferais cette annonce-là. Ça
13 pourrait être en compagnie ou accompagné d'un partenaire en
14 matière de, par exemple, cybersécurité. Il y a rien qui
15 empêche ça, mais ce ne serait pas le Panel.

16 De la même façon, si le Panel devait se
17 prononcer de façon publique pendant une élection, il est
18 entendu que ce serait pas une surprise pour moi. Et il
19 pourrait y avoir des situations de chevauchement où il y
20 aurait des annonces parallèles. Donc, tout ça est dans
21 l'ordre du possible. C'est pas quelque chose qui a été
22 testé.

23 En matière d'élection partielle, parce qu'on
24 n'est pas en convention de transition, le groupe SITE, on... le
25 groupe, pardon, le Panel des cinq n'est pas actif. C'est un
26 groupe de sous-ministres dont je ne fais pas partie qui, à ce
27 moment-là, pourrait servir un peu le même rôle, mais si je
28 comprends bien, communiquerait à travers les ministres. Ce

1 serait probablement des ministres qui feraient l'annonce.

2 Encore là, ce n'est pas à moi à donner des
3 détails de ça, mais je suis conscient de cette dynamique-là.
4 Et j'ai les mêmes attentes que s'il devait y avoir une
5 annonce pendant une période d'élection partielle, que je
6 serais informé essentiellement de la même manière. Ou
7 encore, si c'est moi qui devais faire une annonce, que
8 j'informerais... à travers le comité de coordination, que
9 j'informerais les partenaires en matière de sécurité. Il y a
10 personne qui cherche à se surprendre.

11 **M. JEAN-PHILIPPE MacKAY:** Donc, simplement
12 pour votre bénéfice de Madame la Commissaire, le comité de
13 sous-ministres dont Monsieur Perrault vient de parler, en
14 français, c'est le Comité de sous-ministres chargé des
15 interventions en matière de renseignement, mieux connu sous
16 l'acronyme anglais DMCIR, D-M-C-I-R. Et vous allez avoir des
17 témoins qui vont vous expliquer le fonctionnement et la
18 composition de ce comité.

19 Dernier sujet que je veux aborder avec vous,
20 Monsieur Perrault, avant de céder la parole à mon collègue,
21 si c'est possible, on va parler de cybersécurité. C'est
22 possible d'afficher à l'écran le document COM 601, la version
23 française, s'il vous plait. Donc, COM 601.

24 Monsieur Perrault, pour vous situer, c'est
25 une mise à jour de 2023 du Centre canadien... Centre de
26 sécurité des télécommunications, CST.

27 **LE GREFFIER:** Pouvez-vous répéter le doc ID,
28 s'il vous plait?

1 **M. JEAN-PHILIPPE MacKAY:** Oui. COM 601, 6-0-
2 1.

3 **LE GREFFIER:** Ce document n'est pas dans la
4 base de données de l'audience.

5 **M. JEAN-PHILIPPE MacKAY:** Parfait. Ben,
6 écoutez, je veux pas prendre trop de temps, mais Monsieur
7 Perrault, c'est un document dans lequel... et je vais le...
8 simplement, c'est... on mentionne dans ce document qu'il y a
9 une hausse à l'échelle mondiale des cybermenaces qui pèsent
10 contre les institutions démocratiques et les processus
11 électoraux.

12 Et dans ce contexte, vous avez mentionné en
13 entrevue, lors des deux entrevues, différentes mesures
14 qu'Élections Canada a... des mesures qui ont été prises au
15 cours des dernières années pour renforcer l'environnement...
16 en fait, la cybersécurité au sein d'Élections Canada. Et
17 j'aimerais simplement vous entendre brièvement sur la réponse
18 qui est donnée par Élections Canada sur le plan de
19 l'augmentation des cybermenaces et la manière dont vous vous
20 y prenez pour protéger vos infrastructures.

21 **M. STÉPHANE PERRAULT:** Alors, comme je
22 l'indiquais plus tôt, on a une relation qui s'est renforcée
23 avec le Centre canadien... ce qui est devenu le Centre canadien
24 de cybersécurité, mais qui est un sous-élément du Centre
25 canadien de sécurité des télécommunications, à compter de
26 2017. Évidemment, on est au courant de l'augmentation de la
27 menace à travers cette relation-là et à travers ces rapports-
28 là. On accueille favorablement tout le soutien que le Centre

1 canadien nous donne, entre autres en termes de surveillance
2 de nos infrastructures, chacun des appareils à Élections
3 Canada, que ce soit un téléphone cellulaire, une tablette, un
4 ordinateur, fait l'objet d'une surveillance continue du
5 Centre canadien de cybersécurité.

6 Alors, évidemment, personne est à l'abri des
7 cyberattaques. C'est quelque chose qui n'existe pas, mais on
8 est à l'affut de ça. C'est quelque chose dont on tient
9 compte dans l'ensemble de nos activités qui impliquent des
10 infrastructures technologiques. Pratiquement toutes nos
11 activités, il y a une centaine de systèmes qui sont impliqués
12 dans une élection fédérale. Donc, on est très sensible à ça.

13 On fait aussi des campagnes de
14 sensibilisation auprès de nos employés, notamment à travers
15 des campagnes d'hameçonnage, pour assurer que les employés
16 soient alertes à des possibilités d'hameçonnage. Et on donne
17 de la formation à nos employés et, évidemment, aux directeurs
18 et directrices de scrutin pour qu'aussi il y ait cette
19 sensibilité-là dans les bureaux des directeurs de scrutin
20 pendant une élection.

21 Donc, on a augmenté la sensibilisation et on
22 a aussi augmenté la surveillance de notre infrastructure en
23 collaboration avec le Centre canadien de cybersécurité.

24 **Me JEAN-PHILIPPE MacKAY:** Je vais m'arrêter
25 ici, Madame la Commissaire. Je vais céder la parole à mon
26 collègue pour la suite de l'interrogatoire de monsieur
27 Perrault.

28 **COMMISSAIRE HOGUE:** Merci. Maître Sheppard?

1 --- EXAMINATION IN-CHIEF BY/CONTRE-INTERROGATOIRE PAR

2 MR. DANIEL SHEPPARD:

3 MR. DANIEL SHEPPARD: For the record, it's
4 Daniel Sheppard, Commission counsel.

5 Mr. Perrault, I'd like to move to a new area,
6 and that's the regulation of political finance.

7 So when you testified before the Commission
8 back in March, you noted the fact that the *Canada Elections*
9 *Act* contains rules about how different entities collect,
10 expend, and report expenditures related to the electoral
11 process, and that conversation took place kind of in the
12 specific context of nomination contests.

13 Today I'm going to talk to you a little more
14 generally about those rules, but before I kind of get into
15 the substance of it, maybe I can just invite you to explain
16 why it is that we have political finance rules within our
17 electoral system.

18 MR. STÉPHANE PERRAULT: So generally
19 speaking, the *Elections Act* seeks to establish a level
20 playing field among -- or rather level the playing field
21 amongst electoral competitors and seeks to prevent the undue
22 influence of money. And it does that through a number of
23 mechanisms including transparency rules; contribution limits,
24 which have evolved over the years; spending limits for
25 entities that participate in the electoral process, meaning
26 candidates, parties, and third parties; and in recent years
27 has expanded third-party rules to include pre-writ
28 expenditures.

1 **MR. DANIEL SHEPPARD:** Okay. And I think
2 you've quite helpfully set out some of the details of the
3 system in your supplementary institutional report, and so I'm
4 not going to pull that up, people can make reference to that.

5 Today I'm going to focus more specifically on
6 contributions so the question of who is allowed to give money
7 and who's allowed to kind of accept that money and then kind
8 of expend it on certain regulated activities.

9 Before I get into those rules, I think it's
10 going to be helpful for us to understand who it is we're
11 talking about when it comes to regulated entities. So who
12 are the subjects of these rules in the first place. So can
13 you just indicate who it is that we're regulating with these
14 rules?

15 **MR. STÉPHANE PERRAULT:** Sure, and there's an
16 important distinction. There are, on the one hand, third
17 parties, which are subject to slightly different rules, and
18 then there's the rest of the entities, namely nomination
19 contestants, candidates, leadership contestants, parties, and
20 electoral district associations. And they are subject to a
21 more, I would say, consistent or coherent set of rules
22 regarding contributions.

23 **MR. DANIEL SHEPPARD:** Okay. So let's start
24 with the easy stuff. Let's put third parties aside for a
25 moment, although I'll be bringing us back to that topic and
26 we'll talk about the "Everyone else" that has kind of these
27 more consistent rules.

28 When it comes to all of those other groups,

1 who's allowed to make a contribution to those entities?

2 **MR. STÉPHANE PERRAULT:** So only individuals
3 who are either Canadian citizens or permanent residents can
4 make a contribution to any of those entities.

5 **MR. DANIEL SHEPPARD:** Could the Court
6 Operator pull up CAN4599?

7 And this was a document that Mr. MacKay had
8 taken to you a few minutes ago, the SITE briefing to the
9 Deputy Minister ESCC.

10 And if we could scroll down to page 3,
11 please? Under the heading, "Money, and the first word there
12 is "HASA," which I believe stands for hostile activities by
13 state actors, and what this says is:

14 "HASA also channeled monetary
15 donations and other assistance to
16 preferred candidates in elections
17 with the intent of fostering a bond
18 of obligation to the foreign state
19 and/or its proxies. This is usually
20 done via trusted interlocutors such
21 as proxy agents or coöpted community
22 organizations." (As read)

23 I'm not going to talk to you about this
24 briefing in particular, but I take it this sort of
25 information has been conveyed to you in the past via the
26 security and the intelligence community as a foreign
27 interference activity that may take place in Canada.

28 **MR. STÉPHANE PERRAULT:** I am aware of that

1 risk, certainly.

2 MR. DANIEL SHEPPARD: Is what is described in
3 this document permitted under the political finance rules?

4 MR. STÉPHANE PERRAULT: It is not.

5 MR. DANIEL SHEPPARD: Okay. What makes it
6 not permitted?

7 MR. STÉPHANE PERRAULT: Well, there's a
8 number of things, but contributions must be made out of a
9 person's own funds. So one person cannot accept money to
10 pass it on to a regulated political entities. In French we
11 call that (inaudible) but that is unlawful under the Act. So
12 that's certainly -- and, of course, foreign states and
13 foreigners cannot make contributions, directly or indirectly,
14 to political entities.

15 MR. DANIEL SHEPPARD: And am I right that
16 there's also kind of a general anticircumvention rule that
17 says you're not allowed to structure transactions in a way
18 that seeks to evade the basic rules of the regime?

19 MR. STÉPHANE PERRAULT: Correct. So no
20 system can be perfectly airtight, and I can expand on that.
21 But this is the regime, these are the rules that govern it.

22 MR. DANIEL SHEPPARD: Okay. And we may get
23 to some of the issues that may exist in the regime.

24 So while this type of activity is not
25 permitted, there is at least some reporting, at least by the
26 SITE Task Force, that this is a strategy that foreign actors
27 may engage in. Which I think takes us away from the rules
28 and to the question of, kind of in practice how are those

1 rules implemented?

2 And I think we can take this document down.

3 So can you explain what are some of the
4 things that players within the political finance realm are
5 expected to do in order to ensure compliance with a rule that
6 says only a citizen, or a permanent residence may make a
7 contribution?

8 **MR. STÉPHANE PERRAULT:** So maybe I should
9 start by dividing the ways in which money can flow and the
10 scenarios that are alluded to in this document.

11 In any system money can flow out, what we
12 call outside the regime. It is not lawful to make
13 contributions in cash in excess of \$20. It doesn't mean it
14 doesn't happen. The fact that we have low spending limits,
15 however, makes it difficult to spend large amounts of money
16 in electoral competitions without being noticed by
17 competitors. So it's not saying it's not possible, it
18 certainly is, but there is a limitation that comes with the
19 existence of a spending limit.

20 If someone were to want to funnel that money
21 through the regime so that it finds its way into the campaign
22 account, it would have to go to use proxies; essentially, use
23 persons to bring that money, who have the ability to make
24 contributions.

25 We have low contribution limits. In Canada
26 they are, right now, set at \$1,725 annually. And that is a
27 total sum of the contributions can be made to the candidates
28 and the local district associations within a political party

1 or within a family. There's a small amount of contribution,
2 and in fact, on average contributions tend to be around \$200.
3 So if one were to try to fragment contributions and find
4 people to funnel that money, they would have to find a very
5 large number of willing partners to do that. So just kind of
6 put that in context, so I'm not saying it's impossible, but
7 it is difficult, and it's difficult not to be seen doing that
8 in any large kind of way.

9 The Political Financing Unit receives returns
10 and audits them on their face. It doesn't do an
11 investigation, but it does what we call horizontal audits.

12 So it looks at contributions across a
13 political family to make sure that people who do bring money
14 have not over contributed, in excess of the annual limits.
15 We also publish the names of every person who contributes
16 more than \$200 in a given year. So that is visible to the
17 general public. People who contribute can be seen. We do
18 not have information that would allow us to vet whether all
19 of these contributors are either Canadian citizens or
20 permanent residents. That's not information that we possess.
21 But by publishing the information, the logic of the system is
22 to make it available to the -- in full daylight, so that if
23 there are situations of unlawful contribution, they can be
24 possibly identified by other ---

25 **MR. DANIEL SHEPPARD:** And that's some of the
26 things that Elections Canada is able to do to kind of
27 implement that rule. Moving to the regulated entities
28 themselves, are they under an obligation to inform a

1 potential donor that they have to be a citizen or a permanent
2 resident?

3 **MR. STÉPHANE PERRAULT:** We encourage them to
4 do so, and I'm aware that they do so as a matter of good
5 practice. They have only a legal obligation to return
6 contributions once they are made aware that it is unlawful,
7 either because it exceeds the limit or it comes from an
8 unallowed source, but they have no legal obligation to
9 ascertain the source of the contribution as being a valid
10 source.

11 **MR. DANIEL SHEPPARD:** And so I take it then
12 that if they don't have a duty to ascertain that it's from a
13 lawful source they would not, for example, be under an
14 obligation to require a donor to provide proof of citizenship
15 or permanent residency?

16 **MR. STÉPHANE PERRAULT:** Correct. I'm aware
17 that many have a checkbox when they make their contributions
18 and go through that step. I think that's valuable, but there
19 is no documentary evidence that's required.

20 **MR. DANIEL SHEPPARD:** Right. And I think you
21 referred a -- to essentially a trust-based system whereby you
22 ask the question, but you trust that the answer that you're
23 receiving from the donor is truthful and accurate?

24 **MR. STÉPHANE PERRAULT:** Correct.

25 **MR. DANIEL SHEPPARD:** Okay. Let's move on
26 and talk about third parties, the one that you've said have
27 different rules. Before we talk about those rules, can you
28 give a basic definition of what is a third party?

1 **MR. STÉPHANE PERRAULT:** So there are
2 technical differences between the pre-writ and the writ
3 period, but, generally speaking, a third party is any entity
4 other than a registered party, or a candidate, or a district
5 association. That's generally speaking the scope of what
6 we're covering there. So it's anybody, foreign or domestic,
7 individual or group, corporation or otherwise, not being one
8 of those three.

9 **MR. DANIEL SHEPPARD:** Okay. And as I
10 understand it, there's limits on expenditures for regulated
11 activities during pre-election period when there's a ---

12 **MR. STÉPHANE PERRAULT:** Correct.

13 **MR. DANIEL SHEPPARD:** --- fixed date election
14 and then during the election period itself, from the writ to
15 the election for certain types of activities like certain
16 forms of advertising or partisan activities. Is that a
17 general description of ---

18 **MR. STÉPHANE PERRAULT:** That is kind of ---

19 **MR. DANIEL SHEPPARD:** --- some of the rules?

20 **MR. STÉPHANE PERRAULT:** Yes, we can get into
21 the nitty-gritty of the details, but, yes, and those
22 categories of expenses have been expanded in Bill C-76. They
23 used to include only election advertising during the election
24 period. Now they include partisan activities and surveys and
25 partisan advertising in the pre-writ period.

26 **MR. DANIEL SHEPPARD:** Okay. And so if we're
27 talking about contributions that are being made to fund these
28 types of regulated activities and the scope of those

1 activities have changed over time, are third parties limited
2 to using funds from citizens or permanent residents in order
3 to engage in those activities?

4 **MR. STÉPHANE PERRAULT:** So they cannot use
5 funds from foreign sources. They can use contributions from
6 individuals, or groups, or entities that are not foreign
7 entities, so it's not limited to Canadian citizens and
8 permanent residents in the sense that you could have
9 corporate money, or unions, or association's money, and they
10 can also use their own funds for that purpose.

11 **MR. DANIEL SHEPPARD:** Okay. And it's
12 probably obvious, but just to make the point explicit, when
13 you're talking about foreign sources, that will include
14 entities like foreign governments or foreign political
15 parties?

16 **MR. STÉPHANE PERRAULT:** Right. Or entities
17 that have no activities in Canada.

18 **MR. DANIEL SHEPPARD:** And then we've also
19 kind of briefly touched on the fact that there is certain
20 reporting requirements and that third parties are required to
21 disclose to Elections Canada information about contributions
22 they receive and expenditures they make, and that information
23 is made public by Elections Canada once certain thresholds
24 are passed; is that right?

25 **MR. STÉPHANE PERRAULT:** Correct. That is
26 correct.

27 **MR. DANIEL SHEPPARD:** In the course of your
28 discussions with the Commission, you identified a number of

1 issues that exist in terms of transparency when it comes to
2 contributions and expenditures from third parties, and I'd
3 like to talk to you about some of them. I think they're
4 closely related, but I'm going to try to break them up into
5 three kind of categories. The first is one that you've
6 already mentioned, and that's a third party relying on their
7 own funds when it comes to reporting their expenditures.

8 **MR. STÉPHANE PERRAULT:** Right.

9 **MR. DANIEL SHEPPARD:** Can you just explain
10 what that is and what sort of transparency issues you view
11 that to give rise to?

12 **MR. STÉPHANE PERRAULT:** Sure. I mean, that
13 is an area of concern. We've seen over the last few
14 electoral cycles the percentage of third-party expenditures
15 that are funded, or their contributions that are of their own
16 funds go from 8 per cent I think it's close to 40 per cent
17 now. So increasingly, we see third parties relying on their
18 own funds. And that may include money they've amassed over
19 the years from different sources. It should not be money
20 received for the specific purpose of regulated activities
21 under the Act, but it can be money received from General
22 purposes. It can include commercial revenue or donations and
23 can include in the mix donations from foreign sources. At
24 some point in time, this is all fungible money and it's their
25 own assets, it's their own funds. And so when they use that
26 money, they are using their own funds, and in this way, a
27 certain amount of illegal funding could find its way in third
28 party's expenditures during an election or a pre-writ

1 campaign.

2 **MR. DANIEL SHEPPARD:** And so when they report
3 the use of their own funds, the reporting doesn't kind of go
4 beyond that and provide any indication of the ultimate source
5 of that money?

6 **MR. STÉPHANE PERRAULT:** Correct, and that's
7 why -- and probably get into that, made recommendations to
8 that effect.

9 **MR. DANIEL SHEPPARD:** We -- you've predicted
10 kind of my next area of questioning, but let's talk about
11 some of the other related transparency issues. And the next
12 one is kind of an extension of the own funds issue you've
13 identified, and it's when entities do receive funds from a
14 variety of sources. And I'd like you to imagine an entity
15 that is receiving funds from sources, some domestic, but
16 also, some international, and we can imagine potentially from
17 a foreign government or political party.

18 **MR. STÉPHANE PERRAULT:** Right.

19 **MR. DANIEL SHEPPARD:** And they receive these
20 funds from various sources outside of the election period,
21 they amass it, an election is called, and they now begin to
22 make expenditures on regulated activities and report it as
23 the use of their own funds. Is the political finance regime
24 kind of equipped to trace out and identify a foreign source
25 of funds in that type of scenario?

26 **MR. STÉPHANE PERRAULT:** So there are two
27 scenarios. One is -- which is this one, and the answer, of
28 course, is no, unless they are essentially funded from

1 foreign sources, as long as they have some domestic sources
2 as well. It cannot assign dollar figures to particular
3 categories of expenditures, one for their rent or hydro bill
4 and one for their election campaign activity. So it's all
5 fungible. It is possible that, indirectly, groups may be
6 using foreign funds to support their activities, including
7 campaigning. So that's one area.

8 Another area is third party A receives money
9 from a range of groups, including group B, and reports as
10 money from group B. Group B is a Canadian group, but we
11 don't know where group B gets its funding. So there's a
12 limited degree of transparency. It does not reach all the
13 way down to individual contributors as citizens or permanent
14 residents. So there is a limited amount of transparency in
15 the regime as it exists today.

16 **MR. DANIEL SHEPPARD:** And so the hypothetical
17 I gave was kind of an intermixing of funds from different
18 sources. And it sounds like what you're describing in
19 addition to that is a chain of contributions ---

20 **MR. STÉPHANE PERRAULT:** Correct.

21 **MR. DANIEL SHEPPARD:** --- whereby
22 contributions flow from one entity to another entity to
23 another entity, and you can only trace back the source of
24 those funds really one step to who gave it to the ultimate
25 expender; is that fair?

26 **MR. STÉPHANE PERRAULT:** That's correct. And
27 so both scenarios are, in my view, problematic.

28 **MR. DANIEL SHEPPARD:** And going back, then,

1 to the scenario that was described in that SITE briefing --
2 and we can pull it up if you'd like, but just kind of
3 thinking about this foreign interference threat that's been
4 identified by the security and intelligence community, do you
5 view these types of transparency issues we've just been
6 talking about as raising kind of problems or concerns with
7 respect to foreign interference of a financial nature in the
8 Canadian electoral process?

9 **MR. STÉPHANE PERRAULT:** Certainly. But I
10 would say there's a greater degree of concern for third
11 parties because of the different rules that are at play.

12 **MR. DANIEL SHEPPARD:** So you've made
13 reference to the fact that you've made some recommendations
14 in this area.

15 If the Court Operator could please pull up
16 ELC54.

17 **--- EXHIBIT No./PIÈCE No. ELC0000054:**

18 Meeting New Challenges -
19 Recommendations from the Chief
20 Electoral Officer of Canada following
21 the 43rd and 44th General Elections

22 **MR. DANIEL SHEPPARD:** And while that's coming
23 up, Mr. Perrault, I take it that it's actually part of your
24 formal mandate as Chief Electoral Officer to make
25 recommendations to Parliament about reforms to our electoral
26 laws. Is that ---

27 **MR. STÉPHANE PERRAULT:** It is. It's provided
28 for in the Act and this report that you see is a report that

1 I made after the last two General Elections.

2 Normally we tend to see one after each GE.
3 The time span between the last two was very short and it was
4 the pandemic, so there was none between the two.

5 **MR. DANIEL SHEPPARD:** Okay. And if we could
6 scroll to page 20. And kind of starting in this area, you're
7 discussing some of the issues with respect to third parties.
8 Right here there's a registration threshold, but if we go
9 further down, I think you discuss in your report some of the
10 concerns about transparency.

11 And so if we can kind of scroll down and
12 there, third party contributions, I think, is where the
13 discussion begins.

14 And if we continue to go down to page 22, we
15 see there Recommendation 2.3.1. You've provided a
16 recommendation in terms of some potential reforms to how the
17 contribution rules for third parties ought to operate.

18 Can you just explain to the Commissioner what
19 your recommendation has been in this area?

20 **MR. STÉPHANE PERRAULT:** So in a nutshell,
21 that the ability to use one's own funds would be limited to
22 those entities that are either individuals, Canadian citizen
23 or permanent resident, or groups that are not what I call
24 fundraising entities, that is, groups that we see no more
25 than 10 percent. And the threshold is somewhat arbitrary,
26 but groups that do not significantly rely on contributions as
27 part of their revenues on an annual basis.

28 So only those entities would be allowed to

1 use their own funds. Other entities would have to
2 exclusively rely on contributions received by individuals
3 that are Canadian citizens or permanent residents that are
4 placed in a bank account, as is the case now, and used for
5 their regulated expenditures.

6 **MR. DANIEL SHEPPARD:** So the recommendation
7 is that for many third parties, essentially make the rules
8 similar to or the same as the earlier rules we discussed for
9 all of the other regulated entities.

10 **MR. STÉPHANE PERRAULT:** Correct. Correct.

11 **MR. DANIEL SHEPPARD:** And maybe just for a
12 point of clarity, are you able to give an example of a type
13 of third party that would exist in that exception for the
14 non-fundraising type of entities?

15 **MR. STÉPHANE PERRAULT:** A commercial entity
16 that has, you know, commercial revenue -- a union would
17 receive union dues -- but do not rely on donations.

18 **MR. DANIEL SHEPPARD:** In response to a
19 question that Mr. MacKay asked you, you made reference to
20 Bill C-65. I take it that's a statute you're -- or rather, a
21 Bill that you're familiar with?

22 **MR. STÉPHANE PERRAULT:** Somewhat, yes.

23 **MR. DANIEL SHEPPARD:** Yes.

24 This is a statute that implements at least
25 some of the recommendations that have been made in this
26 report.

27 **MR. STÉPHANE PERRAULT:** That is correct.

28 **MR. DANIEL SHEPPARD:** And in particular, does

1 Bill C-65 reflect this recommendation that you've made?

2 **MR. STÉPHANE PERRAULT:** It does.

3 **MR. DANIEL SHEPPARD:** So once again thinking
4 about this in terms of foreign interference threats in
5 particular, do you think that these proposed changes would go
6 some distance to addressing some of the issues that have been
7 identified in terms of the use of contributions within the
8 electoral system as a form of foreign interference?

9 **MR. STÉPHANE PERRAULT:** I believe that they
10 would. I believe they serve a broader purpose in terms of
11 transparency, but certainly they include protection against
12 the introduction of foreign funds in the regulated activities
13 of third parties.

14 **MR. DANIEL SHEPPARD:** But as well, a point
15 you've also made earlier in your testimony is that, of
16 course, there are the rules but there are people who seek to
17 avoid the application of the rules.

18 I take it you'd agree that this
19 recommendation or Bill-65 would not be a perfect solution,
20 that one could still evade the rules by using proxies or
21 other means to obscure financial transactions.

22 **MR. STÉPHANE PERRAULT:** It is always
23 possible. As I said earlier, though, the Canadian system
24 has, relatively speaking, when you compare around the world,
25 very little money involved in our political system. I think
26 that's a virtue, not a fault. And it does reduce the ability
27 of that free-flowing of illicit funding. It does not
28 eliminate it.

1 **MR. DANIEL SHEPPARD:** So those are all of the
2 questions I'd like to ask specifically about political
3 finance, but I am going to stick with the topic of some of
4 the recommendations that you've made in this document and
5 Bill C-65.

6 And I'd like to focus on two recommendations
7 that you've made. I think you've discussed a number of them
8 in your interview summary, and if participants would like to
9 ask you questions about that, I'm sure they will.

10 The first area of recommendations that I'd
11 like to talk to you about has to do with platform
12 transparency, so a fairly different topic.

13 Could we go to page 29 of this document?

14 And this is a section of your report in which
15 you're discussing the role of online platforms and what they
16 do and the influence they have in the information environment
17 surrounding elections.

18 And if we scroll down to page 30, you make
19 two particular recommendations with respect to transparency.

20 Could you just describe what those
21 recommendations are and what your thinking was behind making
22 them?

23 **MR. STÉPHANE PERRAULT:** So essentially, it's
24 to increase the accountability of platforms regarding how
25 they deal with information, including in the first case how
26 they deal with paid electoral communications, but also how
27 they deal with misinformation specifically around ways to
28 vote early, the electoral process.

1 So right now, there is no transparency. Some
2 platforms may disclose their policies. They can change their
3 policies. In many cases, we don't know exactly what those
4 policies are, so it's very difficult for Canadians to
5 understand or hold the platforms at least morally accountable
6 for how they deal with disinformation and campaign activities
7 during the writ period.

8 **MR. DANIEL SHEPPARD:** And so I take it just
9 in terms of how this would operate -- and I'll use Facebook
10 as just one example, but it could be any number of entities.

11 Under this recommendation, they would be
12 required to publish and make available to the general public
13 whatever their policy happens to be in dealing with these two
14 areas you've identified.

15 **MR. STÉPHANE PERRAULT:** Correct. So it is,
16 in that regard, a modest proposal. It calls for more
17 transparency. It does not set specific standards in that
18 respect.

19 **MR. DANIEL SHEPPARD:** And that's my next
20 question because certainly there have been calls in some
21 quarters for kind of baseline legislated standards, not just
22 saying "Tell us what you're going to do", but a requirement
23 to adhere to certain basic threshold rules.

24 I wonder why you chose to make this more
25 modest proposal and not to propose any type of kind of
26 substantive regulation in this area.

27 **MR. STÉPHANE PERRAULT:** This is, first of
28 all, a beginning. I think it's important to start with

1 transparency. I'm not necessarily opposed to minimal
2 standards. However, I think we have to be careful when we
3 get into prescribing content rules and asking for takedowns.

4 I think there's a risk of backlash. I think
5 there is a universe out there of people who are very
6 sensitive to the issue of state censorship, and that feeds
7 narratives that are -- tend to be hostile to the whole
8 electoral process.

9 So in our case, we've not asked platforms to
10 take down information. We respond with correct information.
11 And in this case, I've not -- I've chosen not to impose or
12 recommend imposing content requirements, but rather, start
13 with the transparency.

14 **MR. DANIEL SHEPPARD:** And then moving from
15 your recommendations to Bill C-65, are these recommendations
16 reflected in that Bill?

17 **MR. STÉPHANE PERRAULT:** They are not.

18 **MR. DANIEL SHEPPARD:** They are not. The
19 other recommendation that I wanted to discuss with you has to
20 do with false statements respecting the electoral process.
21 And so if the Court Operator could please scroll up to page
22 25? And in this section of your report, you note that
23 there's no specific prohibition in the *Canada Elections Act*
24 against making false statements about the electoral process
25 itself. Why is that a concern for you?

26 **MR. STÉPHANE PERRAULT:** So there are specific
27 -- there are provisions, for example, on obstructing the vote
28 and preventing from voting. And we've relied on that in the

1 past. We -- the Commissioner has relied on that in the past
2 for certain prosecutions. But there is no general
3 prohibition that would catch a broader range of scenarios
4 that do not necessarily prevent people from voting or are not
5 necessarily aimed at preventing people from voting, but
6 rather, aimed at undermining the voting process, and in
7 particular, in undermining trust in the process and trust in
8 the results. That is in no way captured by the current
9 rules. And that is something that could be leveraged by
10 nefarious actors, including foreign state actors.

11 **MR. DANIEL SHEPPARD:** And so could you then
12 describe kind of the structure of the provision that you've
13 recommended should be enacted to kind of address that gap?

14 **MR. STÉPHANE PERRAULT:** So my recommendation
15 is for a fairly high standard or strict requirement, which
16 calls for a dual *mens rea* element, if I can use the legal
17 aspect, dual mental element. One is the fact that the person
18 would have to know that the information that they are
19 publishing or disseminating is false. Certainly, there is no
20 intent to capture people who share information that they
21 believe to be true, and, in fact, we should be open to those
22 conversations. But if the person knows the person -- that
23 the information to be false, and that's a second requirement,
24 publishes the information in order to undermine trust in the
25 electoral process, or undermine trust in the results, then I
26 believe that there is a very strong case for the prohibition
27 of this kind of content.

28 **MR. DANIEL SHEPPARD:** So let's talk about

1 that mental element a little bit more. The Commission has
2 certainly heard quite a lot of evidence about the challenge
3 of misinformation and disinformation, and tomorrow we'll be
4 hearing a fair bit more about that topic. Why not simply
5 prohibit knowingly false statements about the electoral
6 process itself? Why add an additional mental element?

7 **MR. STÉPHANE PERRAULT:** Well, I think there
8 are a number of circumstances where a person -- expanding
9 here, outside of the electoral process, but there are
10 different reasons why people may lie or exaggerate, and the
11 line between lying and exaggerating may be a blurry one. And
12 so I think it has to be clear that the person knows beyond a
13 reasonable doubt that this information is false.

14 **MR. DANIEL SHEPPARD:** Okay. And in addition,
15 your proposal requires them to have kind of one of two
16 purposes.

17 **MR. STÉPHANE PERRAULT:** Correct.

18 **MR. DANIEL SHEPPARD:** One purpose is to
19 disrupt the conduct of the election, and the other purpose is
20 to undermine the legitimacy of the election or its results.
21 And if you go and you spend some time reading the *Canada*
22 *Elections Act*, as I know we all have, you'll see this
23 reference to disrupting the conduct of the election appear in
24 provisions that already exist, but the notion of undermining
25 the legitimacy of the election or of its results seems to be
26 a new type of concept that you're recommending be introduced.
27 And I wonder if you could just speak to why is it that you
28 felt it was important to cover not just disrupting the

1 election, but undermining confidence as well?

2 **MR. STÉPHANE PERRAULT:** I think it's an
3 essential element. There's already a number of, as you've
4 noted, offences regarding disrupting the conduct. And I
5 think the main area where we're lagging -- lacking is on that
6 second component of undermining trust in the process or the
7 results. We do see narratives of this nature and we see them
8 internationally in different jurisdictions. And I think
9 there are a concern to the health of our democracy and even
10 the stability of government. So the extent that various
11 actors including foreign state actors could leverage
12 misinformation tools to push our narratives that undermine
13 trust in the outcome of the election, trust in the legitimacy
14 of the election or its results, that would be a significant
15 threat to our democracy, and I think it's important to
16 address that.

17 **MR. DANIEL SHEPPARD:** And in terms of Bill C-
18 65, does that Bill incorporate your recommendations in this
19 portion of your report?

20 **MR. STÉPHANE PERRAULT:** In part, but not to
21 the element that we've just discussed regarding undermining
22 trust in the electoral process or the results. That is not
23 included in Bill C-65.

24 **MR. DANIEL SHEPPARD:** So what is included is
25 a provision relating to knowingly false statements made about
26 the electoral process with the intent to disrupt the conduct
27 of the election, but it does not include those same knowingly
28 false statements made in order to undermine the legitimacy of

1 the election or its results?

2 **MR. STÉPHANE PERRAULT:** Not at this time, no.

3 **MR. DANIEL SHEPPARD:** Okay. Thank you. We
4 can take that document down.

5 So we've talked a little bit about
6 recommendations that you've made previously. I'd like to
7 move now to be a little bit more forward looking at
8 recommendations that may be to come. In your interview, you
9 made note of the fact that Elections Canada is in the process
10 of considering new or additional recommendations, which could
11 include changes to the rules relating to nomination contests
12 and leadership contests, as well as some other topics.
13 First, are those recommendations ready to be made public to
14 the Commission?

15 **MR. STÉPHANE PERRAULT:** They are not. We're
16 still working on that, and we're hearing from the
17 participants in the Commission and taking good note of what's
18 being discussed.

19 **MR. DANIEL SHEPPARD:** So this is an ongoing
20 process ---

21 **MR. STÉPHANE PERRAULT:** It is.

22 **MR. DANIEL SHEPPARD:** --- within Elections
23 Canada?

24 **MR. STÉPHANE PERRAULT:** Yes.

25 **MR. DANIEL SHEPPARD:** Am I right in hoping or
26 assuming that at some point those recommendations will be
27 made available to the Commission for the Commissioner's
28 consideration?

1 **MR. STÉPHANE PERRAULT:** It is certainly my
2 intention to make them available in time for the policy
3 discussions stage of the Commission's mandate and, of course,
4 I'll make them to Parliament as well, as per my mandate.

5 **MR. DANIEL SHEPPARD:** If we're not able to
6 get into very much of the substance of your deliberations in
7 this respect, could you talk about why it is that you've
8 engaged in this process? And in particular, what is it that
9 has caused you to start reflecting on the existing rules that
10 apply to nomination and leadership contests?

11 **MR. STÉPHANE PERRAULT:** I think the testimony
12 we've heard in this Commission and the work of the -- what's
13 referred to as the NSICOP Committee both have highlighted the
14 vulnerability of nomination contests in particular, but also,
15 leadership contest potential to cases of foreign
16 interference. I think the trust of Canadians has been shaken
17 in that regard. So both for the reason of better protecting
18 the processes, but also, reinforcing trust of Canadians, I
19 think it's important to consider what can be done.

20 **MR. DANIEL SHEPPARD:** And in thinking about
21 what can be done, one of the values you identified during
22 your interview as being important was party autonomy, and I
23 think you described it as an important value in our
24 democratic system. Can you expand on that and explain, first
25 of all, what you mean by party autonomy, and then why you
26 view it as an important value in our system.

27 **MR. STÉPHANE PERRAULT:** Certainly. I think
28 that's something you've heard from other witnesses and,

1 certainly, I've heard from parties in my discussions with
2 them, and I share, to a certain degree, their perspective in
3 the sense that the freedom of parties to determine how they
4 will determine, how they will decide who runs under their
5 banner, when those decisions take place, including the right
6 to decide not to accept as one of their candidates someone
7 who's been selected at the local level because that person
8 may have in the past done things or said things that do not
9 reflect the values of the party. This is really at the core
10 of political party's freedom, in my view, just as much as
11 deciding what their party platform is. So parties in Canada
12 have enjoyed and should continue to enjoy a certain degree of
13 latitude in deciding not only who runs for them, but what are
14 the circumstances that surround that decision, including to
15 disallow a person to be a candidate for their party.

16 **MR. DANIEL SHEPPARD:** I take it then this is
17 one of the values, though perhaps not the only one, that
18 you're taking into account as you consider possible reforms
19 to the system for nomination and leadership contests?

20 **MR. STÉPHANE PERRAULT:** That is correct. I
21 do believe that there are ways to look at reinforcing the
22 nomination and leadership contest rules without necessarily
23 taking away from parties the freedom that they enjoy and the
24 selection processes that they put in place.

25 **MR. DANIEL SHEPPARD:** One particular reform
26 proposal that has been discussed in public is to assign the
27 duty to kind of run nomination contests and leadership
28 contests to Elections Canada. That is a topic that you were

1 able to discuss in your interview with Commission counsel.
2 And I wonder if you'd just like to take this opportunity to
3 kind of express your views about whether that is an
4 appropriate role for Elections Canada to undertake?

5 **MR. STÉPHANE PERRAULT:** It's certainly not
6 one that is possible in the system that we have, and that's
7 the main point. Even accepting the freedom of parties inside
8 their rules, one could theoretically conceive a situation
9 where Elections Canada is called upon to administer whatever
10 rules the parties put in place.

11 We do not have fixed date elections in
12 Canada. We have byelections that come at any time in the
13 electoral cycle. We have general elections that, as we know,
14 can happen at any time in the electoral cycle.

15 There are nomination processes -- nomination
16 contests that take place across the country and the lead up
17 to the 43rd GE, we had, I believe, somewhere around 850 that
18 are known to us, they may not all be known to us, around 700
19 for the last general election.

20 The timing of these are unknown. The
21 duration of these are unknown to us. They may be a few hours
22 and a few weeks long, but that varies from party to party.

23 Elections Canada does not have a permanent
24 decentralized infrastructure to deal with that kind of
25 administration. In fact, even with a permanent
26 infrastructure, like Australia has, it would be extremely
27 difficult to conduct or oversee the nominations in the same
28 way that we oversee the elections themselves.

1 So I think in terms of administrating the
2 nomination contests, I do not see that as something that we
3 could do.

4 Again, it doesn't mean that the rules or the
5 safeguards around nomination and leadership contests cannot
6 be improved.

7 **MR. DANIEL SHEPPARD:** Well, Mr. Perrault, I
8 will await your eventual recommendations with interest, but
9 at this time, Madam Commissioner, those are all my questions.

10 **COMMISSIONER HOGUE:** Thank you, Me Sheppard.

11 We'll take a 10-minute break before beginning
12 the cross-examination. So that means 4:45.

13 **THE REGISTRAR:** Order, please. À l'ordre,
14 s'il vous plait.

15 This hearing of the Commission is now in
16 recess until 4:45 p.m. Cette séance de la Commission est
17 maintenant suspendue jusqu'à 16 h 45.

18 --- Upon recessing at 4:34 p.m./

19 --- La séance est suspendue à 16 h 34

20 --- Upon resuming at 4:51 p.m.

21 --- La séance est reprise à 16 h 51

22 **THE REGISTRAR:** Order, please. À l'ordre,
23 s'il vous plait.

24 This sitting of the Foreign Interference
25 Commission is now back in session. Cette séance de la
26 Commission sur l'ingérence étrangère est de retour en
27 session.

28 The time is 4:51 p.m. Il est 16 h 51.

1 **MR. DANIEL SHEPPARD:** Madam Commissioner,
2 it's Dan Sheppard for the Commission.

3 I know I said those were all of my questions.
4 During the break I realized I actually had forgotten to ask
5 one, and with your permission, if I could take another minute
6 of our time.

7 **COMMISSIONER HOGUE:** Go ahead.

8 **--- MR. STÉPHANE PERRAULT, Resumed/Sous la même affirmation:**

9 **--- EXAMINATION IN-CHIEF BY/INTERROGATOIRE EN-CHEF PAR**

10 **MR. DANIEL SHEPPARD (cont'd/suite):**

11 **MR. DANIEL SHEPPARD:** If the Court Operator
12 could bring up WIT74.

13 And Mr. Perrault, this is just another one of
14 the Bill C-65 amendments that I just wanted to ask you a
15 question about.

16 If we can go to page 20 and look at -- down
17 under 8.4 "Undue Foreign Interference".

18 The undue foreign interference provision, as
19 I understand it, prohibits a number of foreign actors,
20 including political Parties, governments and entities like
21 that, from unduly influencing an electoral to vote or refrain
22 from voting or casting their ballot in certain ways. And
23 just so that we're all clear, there's a particular definition
24 of what constitutes "undue foreign influence".

25 Can you just explain what is "undue foreign
26 influence"?

27 **MR. STÉPHANE PERRAULT:** So "undue influence"
28 is -- make sure I'm not going to mess it up, but it's either

1 -- it's influencing electors to vote for a particular Party
2 or candidate or vote against through either spending money or
3 contravening any law of Canada. And that clause allows the
4 Commissioner of Canada Elections to gain access to -- creates
5 an extra-territorial dimension to the provision as well and
6 gives her a mandate to investigate that.

7 It does exclude a number of activities, and
8 perhaps this is what you're wanting me to get to. It does
9 exclude things that are merely the expression of like opinion
10 or media articles that are supportive or critical of a Party
11 or candidate.

12 **MR. DANIEL SHEPPARD:** Right. So I guess kind
13 of inherent in the notion of prohibiting undue foreign
14 influence is that there are forms of foreign influence that
15 are not prohibited ---

16 **MR. STÉPHANE PERRAULT:** Correct.

17 **MR. DANIEL SHEPPARD:** --- by the legislation,
18 and so you've kind of touched on those.

19 Could you give an example of kind of the sort
20 of thing that a foreign government or state might do to kind
21 of potentially induce an elector to vote in a particular way
22 that would not violate the undue influence provision?

23 **MR. STÉPHANE PERRAULT:** So again, if a state
24 actor merely expresses his or her personal opinion, then that
25 would not constitute undue influence. If media articles are
26 published and are connections to a state actor -- the BBC
27 comes to mind, but there are other examples -- this would not
28 constitute undue influence.

1 **MR. DANIEL SHEPPARD:** And then bringing you
2 forward to recommended changes, as this provision is
3 currently drafted, I understand it only applies during the
4 election period itself.

5 **MR. STÉPHANE PERRAULT:** That is correct.

6 **MR. DANIEL SHEPPARD:** And you've made a
7 recommendation to change that. Is that right?

8 **MR. STÉPHANE PERRAULT:** I have recommended
9 that it be expanded to the previous period, but, in fact, as
10 I sit here today, I think Bill C-65 is correct in expanding
11 it at all times. There's no reason to put a time limitation
12 on that.

13 **MR. DANIEL SHEPPARD:** So if Bill C-65 were
14 enacted as it's currently drafted, the undue foreign
15 influence -- the undue influence provision would prohibit the
16 conduct that we described earlier regardless of when it
17 occurs in respect of our elections.

18 **MR. STÉPHANE PERRAULT:** That is correct. But
19 it would not cover nomination or leadership contests. That's
20 a separate conversation.

21 **MR. DANIEL SHEPPARD:** I think I may have
22 taxed the indulgence I've been granted, so I won't go down
23 that path.

24 Madam Commissioner, I appreciate that
25 opportunity.

26 **COMMISSIONER HOGUE:** Thank you.

27 So the first one is the Concern Group.

28 **--- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR**

1 **MR. NEIL CHANTLER:**

2 **MR. NEIL CHANTLER:** Good afternoon.

3 **MR. STÉPHANE PERRAULT:** Good afternoon.

4 **MR. NEIL CHANTLER:** I'm Neil Chantler,
5 counsel for the Chinese Canadian Concern Group.

6 Mr. Perrault, I'm going to start with a
7 question arising from your testimony earlier this afternoon.
8 And it's simply the rules are clear surrounding third-party
9 financing and the prohibition against receiving funds
10 contributed by a foreign entity; correct?

11 **MR. STÉPHANE PERRAULT:** Correct.

12 **MR. NEIL CHANTLER:** The problem seems to be
13 enforcement of those rules.

14 I'm just trying to get a sense of the scale
15 of this problem. Can you tell me whether such cases are ever
16 identified and investigated by Elections Canada?

17 **MR. STÉPHANE PERRAULT:** So if they were to be
18 -- just for clarity, if they were to be investigated, it
19 would be by the Commissioner of Canada Elections.

20 I do not recall a case we would have made a
21 referral for that specific prohibition, but I may be
22 incorrect in that regard.

23 **MR. NEIL CHANTLER:** And sorry, you do not
24 recall such case.

25 **MR. STÉPHANE PERRAULT:** I do not recall.

26 **MR. NEIL CHANTLER:** Thank you.

27 **MR. STÉPHANE PERRAULT:** It's important just
28 to keep in mind that the problem that I'm laying out here or

1 that I was trying to explain is that, as third parties use
2 their own funds, it's very difficult to parse out within
3 these funds what is foreign funding and what is domestic
4 funding.

5 **MR. NEIL CHANTLER:** My next questions are
6 about the data collection conducted by Elections Canada on
7 voter participation rates, particularly among diaspora
8 communities.

9 Elections Canada conducts surveys and
10 collects data on a population it calls "new Canadians";
11 correct?

12 **MR. STÉPHANE PERRAULT:** Correct.

13 **MR. NEIL CHANTLER:** And this category is
14 defined as people who have attained citizenship since the
15 last federal election, so they haven't voted in a federal
16 election before.

17 **MR. STÉPHANE PERRAULT:** Correct.

18 **MR. NEIL CHANTLER:** This category is not
19 limited to new Canadians who might identify with one of our
20 many diaspora communities. The category is much broader than
21 that.

22 **MR. STÉPHANE PERRAULT:** It is. There's
23 overlap, but it's much broader, yes.

24 **MR. NEIL CHANTLER:** And it does not capture
25 members of our diaspora communities that have been in Canada
26 for a long time.

27 **MR. STÉPHANE PERRAULT:** It does not.

28 **MR. NEIL CHANTLER:** Now, the Terms of

1 Reference of this Inquiry recognize that Canada's diaspora
2 groups are among the most vulnerable to foreign interference.
3 You're familiar with that.

4 **MR. STÉPHANE PERRAULT:** I am.

5 **MR. NEIL CHANTLER:** And it's clear from your
6 testimony today that Elections Canada sees education and
7 outreach to Canada's diaspora communities as an important
8 part of its mandate.

9 **MR. STÉPHANE PERRAULT:** Yes.

10 **MR. NEIL CHANTLER:** This includes educating
11 diaspora members on the voting process, the secret vote,
12 methods of voting and so on; correct?

13 **MR. STÉPHANE PERRAULT:** Yes.

14 **MR. NEIL CHANTLER:** And obviously, that has
15 value in its own right, but it's also your response, I
16 believe, in your evidence to foreign interference itself.
17 People need to know where to vote in any event, but it's
18 especially important in the context of foreign interference
19 to assure people the system is sound; correct?

20 **MR. STÉPHANE PERRAULT:** Absolutely.

21 **MR. NEIL CHANTLER:** And this is to combat the
22 harmful effects of mis and disinformation that are sometimes
23 spread about the voting system; correct?

24 **MR. STÉPHANE PERRAULT:** I agree.

25 **MR. NEIL CHANTLER:** And it's also a way to
26 respond to intimidation of voters who may not vote because
27 they fear they may be -- it may be discovered by their home
28 country who they voted for.

1 **MR. STÉPHANE PERRAULT:** They may not
2 understand or appreciate the secrecy of the vote in Canada.

3 **MR. NEIL CHANTLER:** And this is why education
4 and outreach is so important.

5 **MR. STÉPHANE PERRAULT:** Agreed.

6 **MR. NEIL CHANTLER:** And at this point in
7 time, Elections Canada does not know the democratic
8 participation rates of members of different diaspora groups,
9 for example, such as Chinese Canadians, because it's not
10 measured. Is that right?

11 **MR. STÉPHANE PERRAULT:** Not at this point in
12 time, no.

13 **MR. NEIL CHANTLER:** And so you'd agree that
14 Elections Canada does not know if its education and outreach
15 efforts are having the desired effect of increasing
16 participation?

17 **MR. STÉPHANE PERRAULT:** I'd want to be very
18 careful here when we talk about participation rates. There
19 are so many factors that come into play when we talk about
20 participation. There's motivation, there are barriers, there
21 may be intimidation. It's very, very difficult. In fact, we
22 believe it's not possible to identify and isolate factors.
23 It doesn't mean that we should not evaluate the quality of
24 our products and find ways to evaluate whether they are
25 useful to the communities, but participation may not be the
26 right measure for that.

27 **MR. NEIL CHANTLER:** We do know, based on
28 Elections Canada's own surveys, that new Canadians have a

1 lower turn out at elections compared to other Canadian
2 voters; correct?

3 **MR. STÉPHANE PERRAULT:** I believe that's the
4 case, yes.

5 **MR. NEIL CHANTLER:** And of course, perhaps
6 stating the obvious, but the outcome of low participation
7 among a particular group of Canadians is that group of
8 Canadians' interests are underrepresented in our House of
9 Commons?

10 **MR. STÉPHANE PERRAULT:** That is the case.

11 **MR. NEIL CHANTLER:** And this is a problem
12 that we should certainly be striving to fix?

13 **MR. STÉPHANE PERRAULT:** Just to be clear,
14 Elections Canada's concern is with addressing barriers. It
15 is not about stimulating participation. It's a sensitive
16 area because there are political dynamics involved in
17 stimulating or encouraging participation. We want to make
18 sure that Canadians who want to participate have the
19 information and do not face undue barriers. And that
20 includes understanding the protections that they have or the
21 options that they have for voting in a federal election. So
22 that's why we're focusing our efforts there.

23 **MR. NEIL CHANTLER:** Many of the types of
24 hostile actions by foreign states that we've identified
25 discussed in this Inquiry that you've spoken to earlier today
26 would amount to those kinds of barriers; correct?

27 **MR. STÉPHANE PERRAULT:** Some do.

28 **MR. NEIL CHANTLER:** And so Elections Canada

1 has, within its mandate, the removal of those barriers?

2 **MR. STÉPHANE PERRAULT:** Correct.

3 **MR. NEIL CHANTLER:** Could the Court Operator
4 please call up ELC54? This is a document, Mr. Perrault,
5 called *Meeting New Challenges: Recommendations from the Chief*
6 *Electoral Officer of Canada Following the 43rd and 44th*
7 *General Elections*. I presume you're familiar with it?

8 **MR. STÉPHANE PERRAULT:** I am.

9 **MR. NEIL CHANTLER:** If we could please scroll
10 to page 61? The paragraph starting with, "Elections Canada
11 does not have..."

12 **MR. STÉPHANE PERRAULT:** Correct.

13 **MR. NEIL CHANTLER:** There it is. I'll read
14 it aloud.

15 "Elections Canada does not have a
16 clear legislative mandate to collect
17 demographic information about
18 electoral participants."

19 It goes on to explain why, or the consequence
20 of that, and then it says:

21 "Crucially, the lack of legislative
22 mandate also means that demographic
23 data about electoral participants is
24 not fully available to Parliament or
25 researchers."

26 Now, if we can scroll further down the page
27 to the recommendation that arises from this discussion,
28 9.4.1? And it says:

1 "To further progress toward a more
2 inclusive and representative
3 electoral system, a new legislative
4 mandate should be included in the Act
5 to allow Elections Canada to collect,
6 on a voluntary basis, and make
7 publicly available anonymized
8 demographic data about electoral
9 participants, including gender,
10 ethnic origin, age, Indigenous status
11 and disability."

12 I'm sure you'll agree with me that this type
13 of granular demographic data on electoral participants would
14 greatly assist Elections Canada in combating the harmful
15 effects of foreign interference on voter participation rates?

16 **MR. STÉPHANE PERRAULT:** It would certainly
17 help us get a better picture of those who participate,
18 including as candidates in the electoral process. It would
19 be on a voluntary basis though. We do not want to compel
20 people to disclose any information that they do not wish to
21 disclose.

22 **MR. NEIL CHANTLER:** No, but it would allow
23 you to not only tailor your responses and your education and
24 your outreach better, but it would allow you to see whether
25 those efforts were having any results?

26 **MR. STÉPHANE PERRAULT:** I would hope so, yes.

27 **MR. NEIL CHANTLER:** Thank you. Those are my
28 questions.

1 **MR. STÉPHANE PERRAULT:** Thank you.

2 **COMMISSIONER HOGUE:** Thank you.

3 So next one is RCDA.

4 **--- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR**

5 **Me GUILLAUME SIROIS:**

6 **Me GUILLAUME SIROIS:** Bonjour.

7 **M. STÉPHANE PERRAULT:** Bonjour.

8 **Me GUILLAUME SIROIS:** J'aimerais vous
9 entendre brièvement sur l'indépendance financière d'Élections
10 Canada. Est-ce qu'un gouvernement qui n'est pas satisfait,
11 par exemple, avec votre travail pourrait facilement retirer
12 le financement d'Élections Canada pour... ou décider de pas
13 renouveler votre financement, par exemple?

14 **M. STÉPHANE PERRAULT:** Alors, en partie, oui.
15 Évidemment, ce gouvernement-là devrait avoir l'assentiment de
16 la Chambre des communes. C'est la Chambre des communes qui
17 vote les budgets.

18 Mais pour répondre à votre question,
19 Élections Canada a deux sources de financement. Une
20 appropriation annuelle, donc, qui doit être votée à chaque
21 année et qui pourrait être variée selon la volonté des
22 partenaires qui porte sur le salaire des personnes qui
23 occupent un poste de durée indéterminée à Élections Canada.
24 Donc, on parle d'environ 550 postes à durée... pardon...
25 indéterminée, dont le salaire doit être voté annuellement.
26 Donc, sur cet aspect-là, il y a une dépendance au budget
27 annuel.

28 Il y a dans la Loi un mécanisme qu'on

1 retrouve pratiquement dans toutes les juridictions
2 canadiennes au niveau provincial sous une forme qui varie un
3 peu, mais qu'on appelle... je suis pas sûr que c'est du bon
4 français... l'autorité statutaire, mais qui est une
5 autorisation législative permanente d'engager des dépenses
6 que je juge nécessaires à la préparation et la conduite d'une
7 élection.

8 Alors, sur ce point-là, j'ai une
9 indépendance. Évidemment, j'ai une reddition de comptes.
10 J'ai comparu la semaine dernière devant le Sénat pour
11 expliquer mes dépenses. J'ai une reddition de compte, mais
12 c'est moi qui décide de l'ampleur et, évidemment, du moment
13 de l'engagement des dépenses compte tenu du fait qu'on ne
14 sait pas quand une élection aura lieu.

15 **Me GUILLAUME SIROIS:** Ce deuxième volet-là
16 des dépenses est spécifique aux élections? Comme, par
17 exemple, l'aspect surveiller les médias sociaux?

18 **M. STÉPHANE PERRAULT:** Alors, la surveillance
19 des médias sociaux fait partie de notre préparation
20 électorale. Et on a effectivement, j'ai utilisé
21 l'autorisation statutaire pour bâtir cette équipe-là en 2019.
22 Je l'ai maintenu jusqu'à date sur l'autorisation statutaire.
23 Je pense que ce serait souhaitable éventuellement d'en faire
24 un programme permanent et voté annuellement.

25 Donc ça, c'est les choses qui surviennent.
26 J'ai la capacité donc de réagir et de mettre sur pied
27 l'équipe, mais je pourrais lui souhaiter, lui donner une
28 pérennité au moins pour une partie de l'équipe suite à la

1 prochaine élection.

2 **Me GUILLAUME SIROIS:** OK. Merci. Et
3 pourquoi c'est important d'avoir cette sorte d'indépendance
4 financière là pour Élections Canada?

5 **M. STÉPHANE PERRAULT:** Alors, d'abord, en
6 raison de notre système parlementaire, dont on ne connaît pas
7 la date des élections, donc ça peut survenir à tout moment.
8 Mais aussi pour assurer une certaine indépendance. Donc, les
9 choix que je fais, dont je rends compte auprès des
10 parlementaires, mais je les fais sans demander la permission.
11 Donc, les investissements que je fais pour les campagnes
12 d'information aux électeurs, par exemple, sont des dépenses
13 qui sont sur l'autorisation statutaire. Donc, je rencontre,
14 mais je ne demande pas une autorisation préalable aux
15 parlementaires.

16 C'est la même chose, je dois dire, pour la
17 Commissaire aux élections fédérales. Donc, dans ses
18 enquêtes, elle a accès à une autorisation statutaire qui lui
19 évite d'avoir à demander des autorisations spéciales pour
20 engager ces dépenses-là.

21 **Me GUILLAUME SIROIS:** Merci. J'aimerais
22 changer un peu sur les contributions indirectes en service.
23 Particulièrement, un phénomène un peu plus récent, les
24 influenceurs en ligne. Disons qu'on a un influenceur ou une
25 influenceuse qui est payé par un état étranger qui fait la
26 promotion d'un parti politique ou d'un candidat politique.
27 Est-ce que ça pourrait être considéré comme une contribution
28 au parti politique ou au candidat lui-même?

1 **M. STÉPHANE PERRAULT:** Alors, pour qu'il y
2 ait une contribution, il faut que l'entité l'accepte. Il
3 faut qu'il y ait une forme de connivence. On peut pas avoir...
4 on peut pas se faire imposer... si quelqu'un plante une
5 pancarte sur votre propriété, sur votre terrain, vous avez
6 pas reçu une contribution. Si vous la laissez là pendant
7 quelques semaines, je pense qu'on pourrait dire que vous
8 l'avez reçue.

9 Donc, par analogie, c'est pas tant sous
10 l'angle de la contribution. Ça pourrait être certainement
11 sous l'angle de l'influence induite des dispositions, dont on
12 discutait. Ça pourrait être aussi sous la forme d'activités
13 partielles réglementées. Donc, il y a différents chapeaux
14 sur lesquels la Loi pourrait s'accrocher pour regarder cette
15 situation-là.

16 **Me GUILLAUME SIROIS:** Et je me demande si
17 vous êtes au courant que certains autres groupes du
18 gouvernement, d'autres branches du gouvernement, surveillent
19 quant à elles le discours politique en ligne. Est-ce que
20 c'est quelque chose que vous êtes au courant? Vous avez des
21 discussions avec le gouvernement sur ces questions-là?

22 **M. STÉPHANE PERRAULT:** C'est-à-dire, je sais
23 que nos partenaires en matière de sécurité ont un intérêt
24 pour le discours étranger, entre autres, en ligne ou
25 ailleurs, mais je peux pas... vous aurez l'occasion de les
26 interroger sur l'étendue de leur écoute ou de leur veille des
27 médias.

28 Il y a le groupe, évidemment, des affaires

1 mondiales, qu'on appelle le groupe de réponse rapide.
2 J'essaie de trouver l'acronyme français, mais qui travaille
3 avec les partenaires internationaux pour comprendre ce qui se
4 dit dans l'environnement. Toujours sous l'angle de sécurité
5 et pas sous un angle de partisanerie, si on veut.

6 **Me GUILLAUME SIROIS:** Oui, oui, évidemment.
7 Je me demande s'il y avait... il y a eu une considération de la
8 part d'Élections Canada d'avoir ce pouvoir-là de surveillance
9 ou d'avoir ce mandat-là de surveillance plus d'un point de
10 vue politique considérant qu'Élections Canada a un aspect...
11 ben, une certaine indépendance que les fonctionnaires peuvent
12 ne pas avoir. Mais une plus grande indépendance, justement.
13 Est-ce que c'est quelque chose qui a été considéré par
14 Élections Canada?

15 **M. STÉPHANE PERRAULT:** C'est une bonne
16 question. C'est une question qui est importante et je pense
17 que je dois être très clair, Élections Canada... et c'est peut-
18 être pas la réponse que vous souhaitez entendre, mais
19 Élections Canada ne doit pas avoir pour mandat de surveiller
20 le discours partisan. Je pense que c'est essentiel à son
21 indépendance qu'il ne soit pas l'arbitre des discours
22 partisans, que ce soit des discours authentiques, faux,
23 mensongers, des exagérations. Ce n'est pas le rôle d'un
24 administrateur électoral de se mêler là-dedans. Alors, c'est
25 pour ça que notre veille vraiment cible le discours qui porte
26 sur le processus pour informer les Canadiens comme il faut,
27 de la façon dont ils peuvent participer au processus
28 électoral.

1 Je suis conscient, évidemment, que ça ouvre
2 la porte à des campagnes d'influence. C'est un des grands
3 défis qu'on a de vivre dans une société ouverte.

4 **Me GUILLAUME SIROIS:** Dans le contexte de
5 cette surveillance-là, et menée quand même par d'autres
6 acteurs gouvernementaux, et même par des acteurs privés comme
7 des compagnies privées qui sont sous contrat avec le
8 gouvernement ou des organismes sans but lucratif, considérant
9 que ce travail-là est fait quand même... je suis d'accord qu'il
10 y a des risques avec la surveillance partisane, politique des
11 réseaux sociaux, mais ce serait pas mieux de rendre ça dans
12 les mains d'un organisme qui est complètement indépendant et
13 qui peut avoir certaines garanties à ce niveau-là?

14 **M. STÉPHANE PERRAULT:** Je pense qu'il y a des
15 groupes, il y a des universitaires qui s'intéressent à la
16 désinformation. Je pense qu'il y a différentes lentilles qui
17 peuvent être portées par différents groupes sur la
18 désinformation. Je pense que c'est très sain. Je ne pense
19 pas qu'il y a une seule lentille qui doit être portée là-
20 dessus, mais je reviens à mon point. Je pense qu'un
21 administrateur d'élection doit se tenir loin de l'arbitrage
22 des discours partisans.

23 **Me GUILLAUME SIROIS:** Et pourquoi, selon
24 vous, que...

25 **M. STÉPHANE PERRAULT:** Parce que dans le
26 discours... ce faisant, un administrateur électoral serait vu
27 comme prenant parti pour un côté ou un autre dans le débat
28 partisan. Donc, je pense que l'indépendance et

1 l'impartialité d'Élections Canada en souffrirait
2 nécessairement.

3 **Me GUILLAUME SIROIS:** Dans un contexte où
4 l'information est clairement fausse, ça peut être catégorisé
5 comme de l'information qui ne s'intéresse pas au processus
6 électoral lui-même, mais de l'information clairement fausse.
7 Est-ce que c'est pas quelque chose qui pourrait tomber... qui
8 pourrait éventuellement tomber sur le champ de compétences
9 d'Élections Canada?

10 **M. STÉPHANE PERRAULT:** Je ne crois pas, à
11 moins que... il y a des cas spécifiques, il y a des
12 dispositions de la Loi. Je pense à l'article 91, par
13 exemple, des mensonges sur le dossier criminel d'un candidat
14 ou des mensonges... il y a des catégories qui sont très
15 spécifiques et, dans ce cas-là, ces infractions-là tombent
16 sur le mandat de la Commissaire. C'est pas quelque chose que
17 j'ai à administrer. Il y a des infractions qui doivent être
18 très, très, très précises quand on ne parle pas du processus
19 électoral.

20 **Me GUILLAUME SIROIS:** OK. Ça conclut mes
21 questions, Madame la Commissaire.

22 **COMMISSAIRE HOGUE:** Merci.

23 Human Rights Coalition?

24 **(SHORT PAUSE/COURTE PAUSE)**

25 **MS. SARAH TEICH:** Good afternoon.

26 Can we please pull up WIT74? And scroll down
27 to paragraph 28. Thank you.

28 **--- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR**

1 **MS. SARAH TEICH:**

2 **MS. SARAH TEICH:** Here you note that
3 Elections Canada does not ask CSIS to validate the community
4 organizations that EC works with. What work does Elections
5 Canada do with community organizations, and why?

6 **MR. STÉPHANE PERRAULT:** So we provide, to
7 anybody, in fact, but some organizations are part of a
8 network, and being part of the network they receive periodic
9 information bulletins and information about our activities.
10 But they are equipped with tools about -- that serve to
11 inform Canadians on how to participate, whether as an
12 elector, as a worker, or as a candidate.

13 So as I indicated earlier, we welcome anybody
14 to use those tools because they are vetted, proper
15 information that come from Elections Canada, and that's why
16 we are not concerned with the identity of -- the availability
17 of that tool is, in fact, not limited to that network.
18 Anybody can have access to them; they're on our website.

19 **MS. SARAH TEICH:** I see, okay.

20 Actually, that answers all of the questions I
21 was going to ask, so that will be the end of my questions.

22 **COMMISSIONER HOGUE:** Thank you.

23 Counsel for Erin O'Toole?

24 **MR. THOMAS JARMYN:** Thank you, Commissioner.

25 **--- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR**

26 **MR. THOMAS JARMYN:**

27 **MR. THOMAS JARMYN:** Mr. Perrault, my name is
28 Tom Jarmyn, and I represent Erin O'Toole.

1 COMMISSIONER HOGUE: You're muted.

2 MR. THOMAS JARMYN: Oh.

3 COMMISSIONER HOGUE: Ah, okay.

4 MR. THOMAS JARMYN: Okay.

5 Mr. Perrault, my name is Tom Jarmyn, and I
6 represent ---

7 MR. STÉPHANE PERRAULT: Good afternoon.

8 MR. THOMAS JARMYN: --- I represent Erin
9 O'Toole.

10 If I could ask the reporter to bring up
11 WIT15?

12 --- EXHIBIT No./PIÈCE No. WIT0000015.EN:

13 Interview Summary: Leona Alleslev

14 MR. THOMAS JARMYN: And scroll down to the
15 bottom of page 1 and the top of page 3 [sic] where we're
16 looking at paragraph 3. So just a little bit further,
17 please. That's good, thank you.

18 This is the interview summary of a Leona
19 Alleslev, who was a member of Parliament and a candidate in
20 the Aurora riding. And she discusses some of the reports
21 that she'd heard about citizens who are -- were afraid to
22 vote.

23 Have you heard any reports similar to this
24 with respect to either the 2019 or 2021 elections?

25 MR. STÉPHANE PERRAULT: I have not, not
26 outside the work of this Commission. So this is something
27 that, of course, I'm aware of from herself, but I have not
28 received, for example, any intelligence to corroborate that

1 kind of information.

2 MR. THOMAS JARMYN: Okay. And Mr. Chiu
3 testified that he heard similar reports as well. Do you
4 recall that?

5 MR. STÉPHANE PERRAULT: I do. Again, these
6 are things that I've heard in the course of the work of the
7 Commission, and in part these are the piece of evidence that
8 have motivated my desire to increase awareness on protections
9 around the secrecy of the vote to reassure participants.

10 MR. THOMAS JARMYN: Mr. Chiu testified that,
11 in fact, what had been passed on to him was that voters were
12 afraid to even been seen as voting. So it's not -- it wasn't
13 secrecy of the ballot, it was the fact that they were even
14 showing up.

15 MR. STÉPHANE PERRAULT: Correct. There are
16 several ways to vote, and again, I alluded to that earlier.
17 Voters can vote in person at the polling stations where they
18 can be seen. They can vote by mail; they can vote at the RO
19 office. They can vote at another RO office. So in an urban
20 setting, they have the choice of neighbouring returning
21 offices across the city where they could go. So there are
22 different avenues for voters to participate, and I think it's
23 our role to make sure they understand these avenues, they
24 understand the secrecy of the vote, and then decide whether
25 or not to participate.

26 MR. THOMAS JARMYN: The specific allegation
27 of Ms. Alleslev is that agents of the Chinese Communist Party
28 were working in the local election office and in the polling

1 stations. And we don't know whether or not that's as an
2 employee of Elections Canada, or as a scrutineer from a
3 political party. What steps does Elections Canada take to
4 vet either its employees or to encourage parties from
5 inadvertently hiring agents of a foreign country?

6 **MR. STÉPHANE PERRAULT:** So we do conduct
7 security clearances for headquarters' employees, as well as
8 those who work in the offices of Returning Officers who deal
9 with Protected B information, so personal information, or who
10 have access to our IT systems.

11 It's important for everyone who is listening
12 or hearing the work of the Commission to understand that at
13 any given moment an election can be called, and within days
14 we must recruit and train roughly 230,000, 250,000 people.
15 So this system is not one in which we could conduct or even
16 ask security partners to conduct security clearances for
17 250,000 people within a matter of days.

18 So the protections around the voting process
19 lie elsewhere; they lie, as I said, in the various
20 opportunities to vote and the fact that the vote takes place
21 in public, in front of observers, and in the secrecy of the
22 ballot.

23 But the notion that we could screen 250,000
24 people in a number of days when we recruit all the way to the
25 weekend prior to polling day on Monday, is simply not an
26 option for us.

27 **MR. THOMAS JARMYN:** And so it's fair to say
28 that this risk is a structural necessity, not that has to be

1 managed?

2 MR. STÉPHANE PERRAULT: Correct. It's
3 inherent to our system.

4 MR. THOMAS JARMYN: Okay, thank you.

5 Mr. Sheppard asked a great deal of questions
6 about the third-party financing.

7 So if I could ask the Court Reporter to bring
8 up CAN11293?

9 --- EXHIBIT No./PIÈCE No. CAN011293:

10 China: Domination of Chinese-Language
11 Media in Canada Poses National
12 Security Threats - IM 30/2023

13 MR. THOMAS JARMYN: And this is a memorandum
14 from the Intelligence Assessment Secretariat, and I believe
15 the author, Mr. Green, will be testifying in about two weeks
16 from now. So I'd just like to scroll up a little bit so we
17 can see the entirety of the box entitled, "Key Judgment."
18 And if you look at the third bullet it says, "The CPC" --
19 that being the Communist Party of China:

20 "...controls narratives by limiting
21 opportunities for dissenting voices,
22 [redacted] by providing economic
23 incentives, [redacted] and fostering
24 censorship." (As read)

25 And then later on relates these efforts to
26 the ability to attempt to influence electoral outcomes.

27 Is it fair to say, first of all, that if
28 these activities occurred during the course of an election

1 period, they would offend the undue foreign influence
2 provisions of the Act?

3 **MR. STÉPHANE PERRAULT:** Not necessarily. So
4 as we discussed earlier, there are exceptions to the undue
5 influence clause in the *Canada Elections Act* that pertain to
6 media content; right? And that is one ---

7 **MR. THOMAS JARMYN:** Yes, but if they were --
8 if they were providing economic incentives, ---

9 **MR. STÉPHANE PERRAULT:** But that -- so
10 there's a range of conduct that you -- that this box refers
11 to. Yes. Yes, if they were providing economic incentives,
12 yes.

13 **MR. THOMAS JARMYN:** Yeah. And possibly also
14 the foreign contribution rules or the third-party
15 contribution rules as well?

16 **MR. STÉPHANE PERRAULT:** Possibly, yes.

17 **MR. THOMAS JARMYN:** Okay. And I'd like to go
18 down to paragraph 12 of this memo. Exactly. There.

19 And it says:

20 "The widespread use of WeChat
21 presents two enduring challenges."

22 (As read)

23 And then it talks about:

24 "More recently, opensource reporting
25 notes a coordinated disinformation
26 campaign aimed at WeChat dissuading
27 voters from supporting parliamentary
28 candidates with anti-China views in

1 2021.” (As read)

2 It seems that the Communist Party of China is
3 employing -- using its own employees to attempt to do - -
4 carry out this behaviour on WeChat. This too would seem to
5 offend the undue foreign interference -- or foreign influence
6 provisions. Is that ---

7 **MR. STÉPHANE PERRAULT:** So I don't have the
8 facts behind this. As I noted earlier, there is an exception
9 for the media content. Whether this falls within that
10 exception is something that would be -- would have to be
11 determined.

12 **MR. THOMAS JARMYN:** Okay. Thank you. Mr.
13 Sheppard asked you about your recommendations regarding
14 transparency of online platforms. Is it correct that these
15 legal obligations would only apply to those platforms that
16 have a legal presence in Canada?

17 **MR. STÉPHANE PERRAULT:** It would apply to
18 those platforms that provide content in Canada.

19 **MR. THOMAS JARMYN:** So TikTok ostensibly has
20 a legal presence in Canada, so I would see how that would
21 fall in. Would -- how would WeChat, which is -- its platform
22 is entirely located in China, fall within the application of
23 those policies? Or do you understand that it wouldn't?

24 **MR. STÉPHANE PERRAULT:** So it depends how the
25 legislation is drafted. It's possible to draft legislation
26 to carry out -- to have extraterritorial aspects, I think
27 there has to be a significant nexus with Canada. So it would
28 depend on the drafting of the provision. My recommendation

1 does not go into those details in any way.

2 It does touch upon -- the point that you
3 raised touched upon the challenge of enforcing,
4 extraterritorially, some rules that may be devised to secure
5 the election.

6 **MR. THOMAS JARMYN:** Particularly with a
7 country where we do not have a mutual legal assistance
8 treaty? Is that correct?

9 **MR. STÉPHANE PERRAULT:** Correct. Again, this
10 is a matter for the Commissioner to speak to, but that is my
11 understanding.

12 **MR. THOMAS JARMYN:** Yeah. And if you saw
13 violations of any of these provisions, you would be referring
14 that to the Commissioner of Elections for investigation or
15 review and potential prosecution?

16 **MR. STÉPHANE PERRAULT:** That is correct.

17 **MR. THOMAS JARMYN:** In discussing the -- I'll
18 just conclude with this question. In discussing the
19 governance of political parties in leadership races and
20 nomination races, would you be in favour of a type of model
21 similar to the B.C. *Professional Governance Act*, which
22 essentially delegates to professions the authority to
23 regulate their profession as long as they meet the standards
24 of accountability and transparency set out in the Act? In
25 other words, Election Canada sets standards and relies upon
26 the political parties to apply those standards.

27 **MR. STÉPHANE PERRAULT:** So again, this is
28 something we need to consider at a later stage. I would say

1 two things.

2 First of all, I do believe there's room for
3 some standards, but there's also a need for flexibility, and
4 different parties will have different rules. So the level of
5 uniformity should not be necessarily very high. That's one
6 area.

7 My other comment is that we have roughly, at
8 election time, over 20 parties right now, or just below that.
9 Some parties are extremely small and hardly conduct any
10 nominations that are contested. And I think we'd have to
11 think about having standards that are tailored to the
12 realities of the different parties.

13 **MR. THOMAS JARMYN:** Okay. Those are all my
14 questions. Thank you very much, sir.

15 **COMMISSIONER HOGUE:** Thank you.

16 Counsel for Jenny Kwan?

17 **--- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR**

18 **MS. MANI KAKKAR:**

19 **MS. MANI KAKKAR:** Good afternoon, Mr.
20 Perrault and Commissioner. My name is Mani Kakkar and I'm
21 counsel for Jenny Kwan.

22 This afternoon, Mr. Perrault, I just had a
23 few questions for you. One, a small housekeeping matter that
24 I was curious about.

25 You had mentioned that third parties that
26 donate individuals are asked if they are allowed to make
27 those donations on an honour system by checking a box. Are
28 you aware if Elections Canada knows or has identified cases

1 of foreigners donating money?

2 **MR. STÉPHANE PERRAULT:** So we have made
3 referrals or we've asked questions about, for example, if we
4 see a cheque that's from a foreign bank, we will raise that
5 question with the relevant entity. So this is something we
6 do look into, and there have been referrals for foreign
7 contributions.

8 **MS. MANI KAKKAR:** Okay. I appreciate your
9 answer on that point. I want to turn for a moment to the
10 regulation of nomination and leadership contests. Mr.
11 Sheppard had brought you to this and had indicated the
12 importance of regulating nominations, as you agreed, that
13 this process and Commission has showed that there are
14 loopholes being taken advantage of. Did I understand your
15 testimony?

16 **MR. STÉPHANE PERRAULT:** I think there's been
17 a recognition that it is largely unregulated and therefore an
18 area of vulnerability.

19 **MS. MANI KAKKAR:** Thank you. And I
20 appreciate that you can't speak to the specific
21 recommendations that you may make later this month or prior
22 to the policy phase of this Commission, but I wanted to
23 understand a little bit about what any regulations in this
24 area might mean for Elections Canada's budget and capacity?

25 **MR. STÉPHANE PERRAULT:** It would be more for
26 the capacity of the Commissioner of Canada Elections, and
27 depending on the rules that are imposed, whether there are
28 enforceability challenges that she would face.

1 So for example, if there are rules regarding
2 the nomination process, regarding the participation, but
3 there is no paper trail that is kept by the parties or the
4 district associations, then that presents challenges for her.
5 But the concerns are not so much financial, as they are about
6 enforceability.

7 **MS. MANI KAKKAR:** I appreciate that. And
8 maybe I'll take a step back so we can understand what this
9 means not just at the broader level of regulations, as you
10 mentioned, it will affect the OCCE, but more specifically,
11 with some of the recommendations that you've specified.

12 First, I'd like to take you to your summary,
13 WIT74. Paragraph 110 in particular.

14 In this paragraph, you describe the challenge
15 that you would have as Elections Canada, an organization that
16 springs into life in electoral districts across the country
17 when an election is called, if you were in fact administering
18 nomination and leadership contests. You talk about the
19 operational difficulty that you would have. And that's part
20 of the reason why it's clear from your interview summary that
21 that's not the path that Elections Canada is likely to
22 recommend?

23 **MR. STÉPHANE PERRAULT:** Correct.

24 **MS. MANI KAKKAR:** However, if -- you do
25 provide some baseline regulations, like those, if we scroll
26 up to paragraph 108. Will that mean that Elections Canada
27 now has to act for a longer period of time or an extended
28 period of time, given that there will be some of these

1 measures in place for nomination contests -- nomination and
2 leadership contests?

3 **MR. STÉPHANE PERRAULT:** No, not necessarily.

4 **MS. MANI KAKKAR:** Okay. Are you able to
5 elaborate a little bit on that point? And I appreciate ---

6 **MR. STÉPHANE PERRAULT:** Well, for example, if
7 there's a mandatory -- a legislative requirement to vote,
8 this is something that would be administered by the parties
9 and their district associations. Should there be a complaint
10 regarding someone voting that is not entitled to vote, then
11 that complaint would be handled by the Commissioner. And so
12 she has a permanent capacity. That would impact her, of
13 course her workload, and it raises questions, as I mentioned,
14 about, you know, paper trails that she could rely on. But it
15 does not require us to have a permanent presence in the
16 regions, for example, to administer that.

17 **MS. MANI KAKKAR:** I appreciate your answer
18 and testimony on that point. And just to go through these
19 measures in particular, would you say that about all four,
20 including whether existing prohibitions under the *Canada*
21 *Elections Act*, such as undue influence for conduct that is
22 inherently criminal should apply to nomination and leadership
23 contests? Would your office have any role?

24 **MR. STÉPHANE PERRAULT:** It would mainly be
25 for the Commissioner to enforce these rules. So it would not
26 impact my office as much as it would impact her office.

27 **MS. MANI KAKKAR:** I appreciate your
28 testimony. Thank you. Moving to a different point, I wanted

1 to take you to Section 282.4, which Mr. Sheppard addressed
2 with you, as well as my friend, Mr. Jarmyn. I appreciate you
3 have this, it seems, down to memory, but if you'd like, I can
4 put the section up for you.

5 **MR. STÉPHANE PERRAULT:** I would, please.

6 **MS. MANI KAKKAR:** Okay. Not a problem. Can
7 I ask for CEF 302_R to be pulled up?

8 **--- EXHIBIT No./PIÈCE No. CEF0000302 R:**

9 Memo for CCE_Summary 2022-0925

10 **MS. MANI KAKKAR:** And, Commissioner, I seek
11 your leave before doing so. This was a document not on my
12 list, but I'm only doing so for the purposes of having the
13 excerpt of this section.

14 **MS. ERIN DANN:** Sorry, Mr. Court Operator, I
15 believe that permission was granted. You can pull up the
16 document.

17 **MS. MANI KAKKAR:** Thank you, Ms. Dann. And
18 it's just page 4. There's a small footnote there. If you
19 want to expand or zoom in, Mr. Perrault, you'll be able to
20 see it excerpts ---

21 **MR. STÉPHANE PERRAULT:** Yeah.

22 **MS. MANI KAKKAR:** --- part of, at least, the
23 provision on undue influence.

24 **MR. STÉPHANE PERRAULT:** Correct.

25 **MS. MANI KAKKAR:** And there seem to be three
26 key components, which you summarized quite well. One, that
27 you influence an elector or unduly influence an elector to
28 vote or refrain from voting, whether it's for a particular

1 candidate, or registered party, or at all; that you knowingly
2 incur an expense to directly promote or oppose a candidate,
3 registered party, or leader of a registered party; and that
4 you -- that the conduct may be an offence under a law or
5 regulation, whether federally or provincially.

6 **MR. STÉPHANE PERRAULT:** So A and B are
7 alternatives; right? It's not ---

8 **MS. MANI KAKKAR:** That's correct. It's not
9 an A and a B situation. Either you incur the expense, and
10 you could be unduly influencing, or, B, you could violate a
11 law or a regulation. Can I get your thoughts on why you
12 think these parameters are in place to limit what would
13 otherwise be undue influence?

14 **MR. STÉPHANE PERRAULT:** This came out of Bill
15 C-76, so this was not one of my recommendations, so I cannot
16 speak to the policy analysis that went beyond that.
17 Certainly, it must be read in conjunction with another
18 provision that's in the vicinity, which provides
19 extraterritorial jurisdiction to the Commissioner, and so if,
20 in the case of clause B, it would allow her, if there are
21 violations of other Acts, to also include that in her
22 investigation. But, obviously, what I can tell you, I can
23 tell you simply from reading the provision itself, so I'm not
24 sure I can add much value there.

25 **MS. MANI KAKKAR:** Would you mind if I took
26 you through just a hypothetical? And just to get your
27 thoughts, not to necessarily get a legal opinion of any kind,
28 but we've seen in this Commission ways in which foreign

1 actors engage in interference. For example, they may be
2 influential community organisations or an FI actor that enter
3 into a free campaign, whether it's through WeChat, in person,
4 in small events, whatever it may be, let's assume for the
5 purposes of this hypothetical that it has no cost. That a
6 particular candidate, if elected, is going to -- is anti-
7 Chinese or going to cause the retaliation of the Chinese
8 government and cause them to perhaps take retributive
9 measures. And let's say, again, that there's no cost to
10 that, and that doesn't presumptively violate any law or
11 regulation. It's my understanding that this provision would
12 not apply to that.

13 **MR. STÉPHANE PERRAULT:** It would not. Now
14 I'll put two caveats. One is, I mean, the kind of conduct
15 you're describing is, to a certain degree, an inherent
16 challenge in living in an open society, that electors will be
17 subject to all kinds of influences, and it's very hard to
18 differentiate between those that may originate from state
19 actors and those that are not. So that is a challenge, and
20 foreign states can and do take advantage of the open nature
21 of our society, and that's what we have to deal with. I
22 would point to Bill C-70, which is now law, and Section 20.4,
23 which expands the scope of illegal conduct and would be
24 triggered, or would connect, if I can use that term, with
25 paragraph 2B here. So that's a new provision that talks
26 about influencing the political process at federal and
27 provincial levels. It's not before us, so apologies for
28 that. But by deceptive -- I believe language is deceptive

1 and/or surreptitious means, or something of that nature. So
2 there is an element here that could be captured, depending on
3 the fact scenario, by that provision, and through that by
4 paragraph 2B here.

5 **MS. MANI KAKKAR:** I appreciate that, and I do
6 appreciate you bringing it up. Do you think, though, outside
7 of making individual changes to legislation that may make
8 certain Acts -- that may prohibit certain Acts, and,
9 therefore, allow you to act under 282.4, do you think 282.4
10 itself needs any amendment to better capture FI activity?

11 **MR. STÉPHANE PERRAULT:** So I'm presuming here
12 you're referring to, because I don't have it in front of me
13 to -- paragraph 4, are you talking -- sorry, 282.4 as a whole
14 or any particular provision?

15 **MS. MANI KAKKAR:** Let's say that, to be fair,
16 I stick to subsection (2), which is up above.

17 **MR. STÉPHANE PERRAULT:** Yeah, so in my view,
18 this should be expanded in time and to include at all times,
19 and this is what's in Bill C-65. And it should be expanded
20 to cover nomination in the leadership contests.

21 **MS. MANI KAKKAR:** Okay. And no other
22 expansions you feel would be necessary to capture FI
23 activity?

24 **MR. STÉPHANE PERRAULT:** I'm open to
25 suggestions, but not that I can think of.

26 **MS. MANI KAKKAR:** I appreciate that. Thank
27 you very much.

28 **COMMISSIONER HOGUE:** Thank you.

1 Counsel for Michael Chong?

2 **--- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR**

3 **MR. FRASER HARLAND:**

4 **MR. FRASER HARLAND:** Good afternoon, Mr.
5 Perrault. I'm Fraser Harland, counsel for Michael Chong. I
6 just wanted to ask you a few questions about the social media
7 monitoring that Elections Canada undertakes. So I understand
8 that Elections Canada has a limited role in social media
9 monitoring, focused only on the electoral process, if I can
10 put it that way; is that right?

11 **MR. STÉPHANE PERRAULT:** It is. So it
12 includes information about where and when to vote, and how to
13 vote, but it also may include information that's of interest
14 to Canada -- to Elections Canada, including how people feel
15 about the process, whether they're frustrated, or satisfied,
16 or happy, or whether there are incidents like roadblocks that
17 may affect, you know, the opening of a polling place,
18 whatnot. But the focus is really about participation in the
19 voting process. It is not about partisan opinion.

20 **MR. FRASER HARLAND:** Right. And so I
21 appreciate that distinction, and I wanted to just ask a
22 couple questions about the resourcing that's dedicated to
23 social media monitoring. So are you able to tell me how many
24 people Elections Canada employs to conduct this monitoring
25 during an election?

26 **MR. STÉPHANE PERRAULT:** So the size of the
27 team at the last election, and I'm including here -- I don't
28 have the breakdown between monitoring and doing the daily

1 reports, for example, but the team it was 27 resources. I've
2 approved 41 for the next election. I -- this is a reflection
3 of the fact that our electoral process is increasingly
4 impacted by online conversations, and social media will play
5 in the future an even greater role than it has in the past.

6 **MR. FRASER HARLAND:** And does that team have
7 people who are proficient in foreign languages, or is it only
8 English and French?

9 **MR. STÉPHANE PERRAULT:** No, no, we have
10 people who are proficient. At the last election, it was 15
11 languages. We are -- again, it depends on the recruitment,
12 but we're aiming to have the similar languages, but
13 certainly, it would include, again, Mandarin, Cantonese, and
14 Punjabi, and Russian, and a range of languages.

15 **MR. FRASER HARLAND:** And do you know how many
16 employees for Mandarin and Chinese specifically you would be
17 targeting for the next election?

18 **MR. STÉPHANE PERRAULT:** I'd be -- I would
19 have to come back to the Commission. I don't have that ---

20 **MR. FRASER HARLAND:** Okay. That's fine. And
21 do you know if that person would be monitoring the WeChat
22 platform, or that would be part of ---

23 **MR. STÉPHANE PERRAULT:** Yes, we have been
24 monitoring WeChat since 2019.

25 **MR. FRASER HARLAND:** Okay. Those are all my
26 questions. Thank you very much.

27 **COMMISSIONER HOGUE:** Thank you.

28 Attorney General?

1 --- CROSS-EXAMINATION BY/CONTRE-INTERROGATOIRE PAR

2 MR. BARNEY BRUCKER:

3 MR. BARNEY BRUCKER: Good afternoon, Mr.
4 Perrault. Barney Brucker for the AG. I took from reviewing
5 your materials and your evidence a number of impressions, and
6 I just wanted to go through a few of them and see if you
7 agree. It seemed to me that Elections Canada has made
8 considerable effort to promote education and understanding of
9 the electoral process, particularly with respect to diaspora,
10 Indigenous and vulnerable communities. Would you agree with
11 that?

12 MR. STÉPHANE PERRAULT: That is correct. In
13 the case of diaspora communities, we are increasing our
14 efforts.

15 MR. BARNEY BRUCKER: And insofar as political
16 finance rules are concerned, it is my impression that ours,
17 or Canada's, are among the most comprehensive and strict of
18 any democratic nation, in terms of ability to limit undue
19 influence of money, transparency, and level the playing field
20 for actors in the electoral space. Would you agree with
21 that?

22 MR. STÉPHANE PERRAULT: That is my view. You
23 can see aspects of our regime reflected in other
24 jurisdictions, but rarely do you see the combination of roles
25 that we have. As I said, no system is watertight, but I
26 believe we have the -- if not the most robust, one of the
27 most robust in the world.

28 MR. BARNEY BRUCKER: And I also got the sense

1 that upgrades are being made or are planned to security
2 measures around Election Canada's IT systems, including its
3 capacity to detect misinformation and disinformation. Is
4 that fair?

5 **MR. STÉPHANE PERRAULT:** So in terms of IT
6 infrastructure, we continually engage with security experts
7 and upgrade our systems and enhance our posture. There is no
8 complete safety in that area.

9 In the case of misinformation or
10 disinformation, we are also -- and that's a different aspect,
11 but we are also enhancing our efforts in that area.

12 **MR. BARNEY BRUCKER:** I think you said the
13 SITE Task Force was stood up for the byelections, the recent
14 byelections in 2023/'24, and that the electoral coordination
15 security system, I've probably got that moniker wrong, but
16 they met regularly -- Elections Security Coordination
17 Committee. How's that?

18 **MR. STÉPHANE PERRAULT:** That's correct.

19 **MR. BARNEY BRUCKER:** Okay. We had a 10-page
20 handout yesterday of acronyms. Well, our friends at the
21 Commission. And I'm still on page one.

22 But my understanding is that Elections Canada
23 is the co-chair of that ECSS? Is that fair?

24 **MR. STÉPHANE PERRAULT:** That's correct.

25 **MR. BARNEY BRUCKER:** Along with PCO?

26 **MR. STÉPHANE PERRAULT:** Correct. So it
27 exists at different levels at the DG, ADM, and DM levels.
28 I'll be quite frank, the DM level meets more rarely. But

1 certainly during byelections, the ADM and DG levels meet
2 regularly.

3 **MR. BARNEY BRUCKER:** And the SITE Task Force
4 or its representatives regularly brief the committee?

5 **MR. STÉPHANE PERRAULT:** That is correct.

6 **MR. BARNEY BRUCKER:** And so you would, as
7 being on the committee, get access to any information they
8 might have that may impact the election integrity?

9 **MR. STÉPHANE PERRAULT:** That is my
10 expectation.

11 **MR. BARNEY BRUCKER:** And you could make
12 whatever use you would be able to do with that?

13 **MR. STÉPHANE PERRAULT:** Absolutely.

14 **MR. BARNEY BRUCKER:** Okay.

15 **MR. STÉPHANE PERRAULT:** Subject to the
16 protection of the classified documents, of course.

17 **MR. BARNEY BRUCKER:** And -- of course. And
18 you know, recent legislation, Bill C-70 and the legislative
19 initiatives that are planned, I understand, in Bill C-65, so
20 that -- these are some that's already passed and some that
21 are planned are -- also enhance the electoral process or the
22 security of electoral process? Is that fair?

23 **MR. STÉPHANE PERRAULT:** They do to a certain
24 degree, and I look forward to appearing before committee. I
25 think Bill C-65 makes a number of improvements. I think it's
26 something that can be built on, and I'm hopeful that it will.

27 **MR. BARNEY BRUCKER:** And as Canada's Chief
28 Electoral Officer, you have overall responsibility for

1 Elections Canada and the administration of federal elections;
2 right?

3 **MR. STÉPHANE PERRAULT:** That's correct.

4 **MR. BARNEY BRUCKER:** All right. Now no
5 system is perfect, and everything can improve with change,
6 but would you agree with me, are you confident that the
7 integrity of our federal electoral processes is being
8 maintained through the efforts of Elections Canada and its
9 partners?

10 **MR. STÉPHANE PERRAULT:** I have a high degree
11 of confidence in the overall integrity of our electoral
12 process in Canada. One of the reasons for that is that it's
13 always open for improvements, and after each election, it's
14 examined and looked at ways to improve the process, and this
15 is partly what's happening here.

16 **MR. BARNEY BRUCKER:** Last week we had a
17 witness who described Canada as a foreign interference
18 playground. From where you sit as Chief Electoral Officer,
19 and in your perspective, confined to elections, do you agree
20 with that statement?

21 **MR. STÉPHANE PERRAULT:** I can't comment on
22 that statement. I believe that the scope of that statement
23 must -- probably expands well beyond my mandate in the
24 administration of the election.

25 **MR. BARNEY BRUCKER:** Yes. And I'm only
26 asking in respect of your mandate. Do you have any comment
27 on that, whether ---

28 **MR. STÉPHANE PERRAULT:** So with respect to my

mandate, I do not believe that it is a playground for foreign interference.

MR. BARNEY BRUCKER: Thank you, sir.

COMMISSIONER HOGUE: Thank you.

Counsel for Elections Canada, do you have any questions?

UNIDENTIFIED SPEAKER: No questions. Thank you.

COMMISSIONER HOGUE: No questions.

Mr. MacKay or Mr. Sheppard?

MR. DANIEL SHEPPARD: Thank you, Commissioner. No questions.

COMMISSIONER HOGUE: No re-examination.

So it's over for you.

MR. STÉPHANE PERRAULT: Merci.

COMMISSAIRE HOGUE: Merci beaucoup. Bonne soirée. Bonne soirée à tous. Demain matin à 9 h 30.

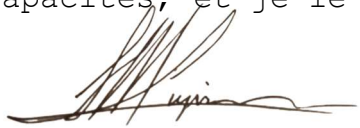
THE REGISTRAR: Order, please. À l'ordre, s'il vous plait.

This sitting of the Foreign Interference Commission is adjourned until tomorrow, Wednesday, the 24th - the 25th of September, 2024, at 9:30 a.m. Cette séance de la Commission sur l'ingérence étrangère est suspendue jusqu'à demain, mercredi le 25 septembre 2024, à 9 heures et demie.
--- Upon adjourning at 5:44 p.m.
--- L'audience est suspendue à 17 h 44

C E R T I F I C A T I O N

I, Sandrine Marineau-Lupien, a certified court reporter,
hereby certify the foregoing pages to be an accurate
transcription of my notes/records to the best of my skill and
ability, and I so swear.

Je, Sandrine Marineau-Lupien, une sténographe officielle,
certifie que les pages ci-hautes sont une transcription
conforme de mes notes/enregistrements au meilleur de mes
capacités, et je le jure.



Sandrine Marineau-Lupien