



CHAMBRE DES COMMUNES  
HOUSE OF COMMONS  
CANADA

44<sup>e</sup> LÉGISLATURE, 1<sup>re</sup> SESSION

---

# Comité permanent de la procédure et des affaires de la Chambre

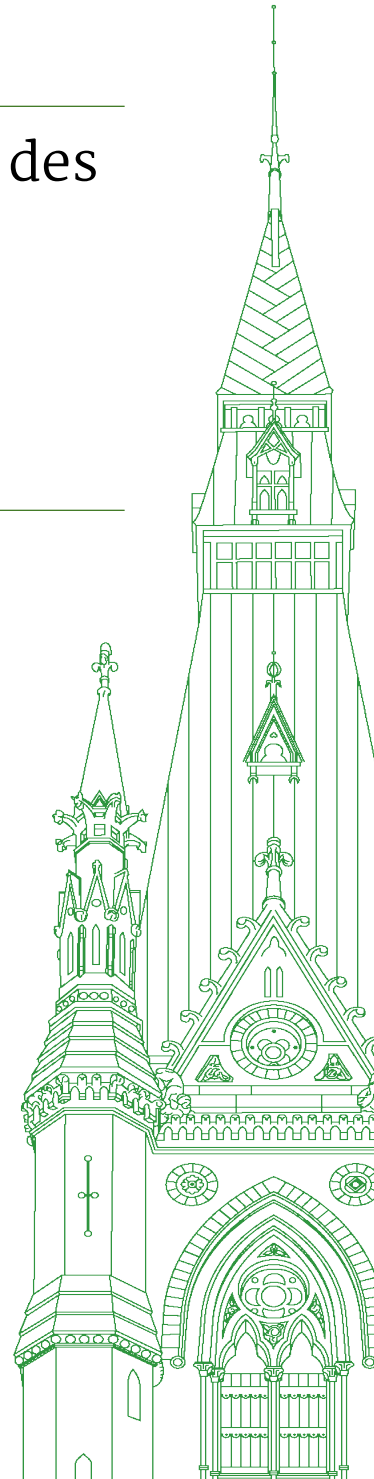
TÉMOIGNAGES

NUMÉRO 120

**PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY**

Le mardi 11 juin 2024

---



Président : M. Ben Carr



## Comité permanent de la procédure et des affaires de la Chambre

Le mardi 11 juin 2024

• (1105)

[Traduction]

**Le président (M. Ben Carr (Winnipeg-Centre-Sud, Lib.)):** Bonjour, chers collègues. C'est bon de vous voir tous ici.

[Français]

J'espère que vous avez passé un bon lundi.

[Traduction]

Nous sommes réunis pour la 120<sup>e</sup> réunion du Comité permanent de la procédure et des affaires de la Chambre.

Chers collègues, comme vous le savez, nous poursuivons notre étude de la question de privilège concernant des cyberattaques menées contre des députés.

La réunion d'aujourd'hui prendra la même forme que celle de la semaine dernière, à savoir que sa première heure se déroulera en public, alors que sa deuxième heure se déroulera à huis clos. Nous devons prendre quelques minutes pour passer à huis clos à la fin de la première heure.

Les témoins du Service canadien du renseignement de sécurité qui se joignent à nous aujourd'hui sont David Vigneault, directeur, Peter Madou, directeur adjoint, Exigences, et Bo Basler, directeur général et coordinateur, Ingérence étrangère.

Monsieur Vigneault, vous et vos collègues disposerez d'un maximum de 10 minutes pour faire vos déclarations préliminaires, après quoi nous passerons à nos séries de questions.

Soyez les bienvenus à la séance du Comité.

Je vous remercie de votre présence, monsieur Vigneault. La parole est à vous.

[Français]

**M. David Vigneault (directeur, Service canadien du renseignement de sécurité):** Merci beaucoup, monsieur le président.

Mesdames et messieurs les membres du Comité, bonjour.

Je vous remercie de m'avoir invité à témoigner aujourd'hui.

**Le président:** Monsieur Vigneault, veuillez attendre un instant, s'il vous plaît.

[Traduction]

Nous avons un problème d'interprétation.

D'accord. Le problème semble avoir été résolu.

[Français]

Nous vous écoutons, monsieur Vigneault.

**M. David Vigneault:** Merci, monsieur le président.

Les problèmes liés à la cybersécurité, leur lien avec la sécurité nationale et les tentatives des adversaires pour s'immiscer dans les affaires du Canada deviennent sans cesse plus complexes. Ces problèmes requièrent l'attention du gouvernement canadien et de tous les Canadiens.

De plus en plus, les menaces qui pèsent sur la sécurité du Canada revêtent la forme de cybermenaces. Les cyberactivités malveillantes visant le Canada prennent de l'ampleur et gagnent en complexité et en technicité, les cyberintervenants cherchant à servir leurs propres intérêts économiques, politiques, idéologiques et liés à la sécurité, au détriment du Canada et de ses alliés. Bref, l'écosystème numérique a transformé la nature et la conduite de la guerre, de l'espionnage, de la diplomatie et du commerce.

[Traduction]

Les auteurs de cybermenaces peuvent être des acteurs étatiques, qui obéissent aux ordres des forces armées et des services de renseignement d'États étrangers, ou des acteurs non étatiques.

Le SCRS fait activement enquête sur toute une gamme de cyberintervenants, notamment ceux qui proviennent de la Chine, de la Russie, de l'Iran et de l'Inde ou qui sont associés à ces États. Quelle que soit la personne qui dirige leurs activités, les auteurs de cybermenaces emploient un large éventail de technologies et de techniques pour exploiter les points faibles des systèmes d'information, pour prendre des personnes pour cible afin d'accéder sans autorisation à des systèmes ou des réseaux, ou pour tirer parti de l'infrastructure canadienne pour atteindre leurs grands objectifs stratégiques et géopolitiques au détriment du Canada.

Le mandat du SCRS consiste à recueillir des renseignements sur les menaces envers la sécurité du Canada, à conseiller le gouvernement à cet égard et, au besoin, à prendre des mesures en vue de les réduire. Cela comprend les cybermenaces.

Plus précisément, lorsque le SCRS détecte des cybermenaces pour la sécurité nationale du Canada, il emploie diverses méthodes d'enquête, dont la mise à contribution de sources humaines et la collecte de renseignements autorisée par mandat, afin de déterminer l'ampleur, les cibles et la source de la menace ainsi que les motivations de son auteur.

[Français]

Le vaste dialogue instauré par le Service canadien du renseignement de sécurité, le SCRS, avec le secteur privé, le milieu universitaire, les différents paliers gouvernementaux et les groupes autochtones aide à renforcer la vigilance et la résilience des Canadiens relativement à l'intensification des menaces. Par exemple, depuis 2021 seulement, plus de 70 séances d'information sur l'ingérence étrangère et l'espionnage ont été offertes aux parlementaires. Au cours de celles-ci, la sensibilisation à la sécurité, notamment les mesures de cybersécurité, était un des principaux éléments de discussion.

De plus, le SCRS fournit régulièrement des évaluations du renseignement à ses partenaires gouvernementaux, ce qui leur permet de prendre des décisions stratégiques et opérationnelles éclairées. Il diffuse aussi ces évaluations et des pistes d'enquête à ses partenaires étrangers de confiance, afin de les aider à garantir l'intégrité de l'infrastructure mondiale de l'information, qui est essentielle à la sécurité.

[Traduction]

Cependant, j'aimerais également signaler que le SCRS fait partie d'un groupe de ministères et d'organismes qui cherchent à protéger le Canada contre les cybermenaces. Même si le SCRS joue un rôle essentiel au sein de ce groupe, il collabore étroitement avec d'autres intervenants de premier plan, comme les spécialistes en cybersécurité du Centre de la sécurité des télécommunications, ou CST, du Centre canadien pour la cybersécurité, de Sécurité publique Canada et de la Gendarmerie royale du Canada, pour n'en nommer que quelques-uns. Ensemble, nous nous employons à protéger le Canada et ses actifs, ses informations et sa sécurité nationale contre une grande quantité de cybermenaces.

En ce qui concerne l'étude particulière que le Comité mène, nos collègues et les spécialistes en cybersécurité du CST ont établi conjointement la chronologie des événements qui détaille les interactions entre nos deux organisations et la Chambre des communes.

Je tiens à mentionner que le CST nous a indiqué en janvier 2021 que le système informatique de la Chambre des communes éprouvait des problèmes. Par la suite, le SCRS a donné une séance d'information directement au personnel des TI de la Chambre des communes en collaboration avec le CST. Nous avons ensuite travaillé de concert avec le CST et la Chambre des communes de janvier à avril 2021 dans le cadre de l'enquête qui a suivi.

Il a été déterminé que des membres de l'Alliance interparlementaire sur la Chine, ou IPAC, étaient visés. Mais, fait important, aucune compromission des systèmes ni aucune activité de suivi n'ont été recensées.

Le SCRS a largement diffusé à des clients de l'ensemble du gouvernement du Canada des produits de renseignement portant sur les tentatives de pistage de courriels que le groupe ATP31 a dirigées contre des membres de l'IPAC au Canada. Le SCRS a commencé à travailler avec la Chambre des communes avant que le FBI ne transmette des informations au SCRS et au CST ou que les États-Unis ne rendent des informations publiques en 2024.

• (1110)

Lorsque l'incident a été signalé au début de 2021, le SCRS a suivi le protocole en vigueur à cette époque. Il a travaillé directement avec le CST et la Chambre des communes afin de mieux comprendre l'incident et ses répercussions. Notre enquête, en parallèle

avec le travail du CST, a permis de renseigner la Chambre des communes sur les mesures techniques précises qui pouvaient être prises pour atténuer les répercussions de l'incident.

[Français]

En 2023, le premier ministre a transmis des directives ministérielles au SCRS qui précisent le rôle et les responsabilités de celui-ci pour ce qui est d'enquêter sur les menaces dirigées contre les parlementaires, de les informer et de trouver des façons d'atténuer ces menaces. Dans les directives, il est précisé que le SCRS doit, dans la mesure du possible tout en respectant la loi, veiller à ce que les parlementaires soient informés des menaces à la sécurité qui sont dirigées contre eux.

Le SCRS avance en territoire inconnu. C'est l'occasion de réfléchir, d'apprendre et de nous améliorer. Aujourd'hui, ce qui diffère, c'est que les directives que nous recevons nous obligent à nous entretenir avec nos partenaires quant à la meilleure façon de nous assurer que les parlementaires sont informés des menaces qui pèsent sur eux. Ce n'est pas nécessairement le SCRS qui les informe; il se peut que ce soit l'organisation responsable du dossier. Toutefois, comme c'est le SCRS qui a reçu les directives ministérielles, nous dirigeons les discussions sur le processus à suivre.

[Traduction]

Monsieur le président, je pense que je vais passer sous silence la récapitulation de la chronologie des événements pour gagner du temps. Je parlerai rapidement de certains pouvoirs législatifs.

Mesdames et messieurs les membres du Comité, je crois que vous comprenez tous que la loi qui régit le mandat du SCRS a été adoptée il y a près de 40 ans. Compte tenu de l'évolution rapide de la technologie et de la complexité croissante de l'écosystème de la cybersécurité, les lacunes relatives aux pouvoirs du SCRS pèsent toujours plus lourd. Elles limitent de plus en plus la capacité du SCRS à détecter les activités d'ingérence étrangère, à enquêter sur celles-ci et à lutter contre elles, y compris en échangeant des renseignements.

Heureusement, le projet de loi C-70, que la Chambre étudie à l'heure actuelle, propose une série de modifications bien précises qui amélioreront les mesures opérationnelles que le SCRS peut prendre pour lutter contre l'ingérence étrangère.

Les modifications proposées permettront notamment de communiquer des informations à des entités autres que le gouvernement fédéral dans le but de renforcer la résilience face aux menaces pour la sécurité nationale, dont l'ingérence étrangère. Il sera ainsi possible de renforcer la résilience avant même que les menaces ne se concrétisent. De plus, cela aidera les parlementaires à prendre des décisions plus éclairées.

De manière générale, le projet de loi C-70 vise à ce que les enquêtes du SCRS soient souples et adaptées, ce qui lui permettra d'améliorer la collecte de renseignements et de donner de meilleurs conseils, y compris aux parlementaires.

La dernière chose que je voudrais dire, monsieur le président, c'est qu'en réfléchissant à cette situation pour me préparer à cette comparution, j'estime que l'analyse à laquelle je me suis livré avec mes collègues a indiqué que tout le monde avait fait le travail qu'il était censé faire. Cependant, avec le recul, je pense que tout le monde sera maintenant d'accord pour dire que le résultat pour les parlementaires n'était pas ce qui aurait été souhaité.

Je salue le travail de votre comité et celui que le SCRS peut réaliser pour s'assurer qu'à l'avenir, nous tirions des enseignements de cette affaire et que le résultat pour les parlementaires et les Canadiens soit différent.

[Français]

Je vous remercie.

**Le président:** Merci beaucoup, monsieur Vigneault.

[Traduction]

Chers témoins, nous allons maintenant passer aux séries de questions. Pour votre gouverne, je précise que les représentants de chaque parti politique présents aujourd'hui disposeront de six minutes pour vous interroger. Nous passerons ensuite à des séries d'interventions légèrement plus brèves.

Cela dit, monsieur Cooper, vous avez la parole pendant six minutes.

**M. Michael Cooper (St. Albert—Edmonton, PCC):** Merci, monsieur le président.

Monsieur Vigneault, le 19 novembre 2021, le SCRS a remis à 35 clients du gouvernement du Canada un résumé analytique classifié portant sur la campagne de cyberattaques dirigée par Pékin que le groupe APT31 a menée. La conseillère à la sécurité nationale et au renseignement du premier ministre faisait-elle partie des 35 clients du gouvernement du Canada qui ont reçu la note d'information?

• (1115)

**M. David Vigneault:** Monsieur le président, je n'ai pas en main la liste de distribution particulière de ce document. D'une manière générale, je peux dire qu'un tel produit serait en effet distribué au Bureau du Conseil privé, et cela inclurait la conseillère à la sécurité nationale et au renseignement. C'est la pratique générale, mais je vais devoir vérifier ce point précis.

**M. Michael Cooper:** Est-il probable que la liste de distribution comprenait certains ministres, ministères et sous-ministres?

**M. David Vigneault:** Monsieur le président, la distribution des renseignements se fait de la manière suivante: au nom de leur unité du renseignement, les ministères sont chargés de mettre ces renseignements à la disposition de leur ministre. Toutefois, il me serait difficile de savoir s'ils l'ont fait.

**M. Michael Cooper:** La façon la plus simple de procéder est peut-être de demander à M. Vigneault de fournir au Comité une liste des 35 clients du gouvernement du Canada qui ont été informés de cette affaire?

**M. David Vigneault:** Je le ferai, monsieur le président.

**M. Michael Cooper:** Merci.

Pouvez-vous nous donner des précisions au sujet de cette séance d'information?

**M. David Vigneault:** Monsieur le président, je ne dispose pas des détails de cette séance d'information. Ce que je peux dire, c'est que, comme je l'ai mentionné dans ma déclaration préliminaire, en tant que membres du service du renseignement qui travaillent avec leurs partenaires au Canada ainsi qu'à l'étranger, nous avons constaté une augmentation du perfectionnement et du caractère agressif du cyberciblage par la Chine, y compris par le groupe APT31.

**M. Michael Cooper:** Je vous remercie beaucoup de votre réponse.

Le 25 août 2023, le SCRS a publié une deuxième note d'information, c'est-à-dire une évaluation du renseignement classifiée, à l'intention de ce qui est décrit dans le calendrier comme des clients pertinents du gouvernement du Canada, et cette note fait allusion aux cyberattaques menées par le groupe ATP31. Ces clients comprenaient-ils la conseillère à la sécurité nationale et au renseignement du premier ministre ou le BCP? Savez-vous qui sont ces clients pertinents?

**M. David Vigneault:** Monsieur le président, ma réponse est la même. Je peux obtenir la liste de distribution. Je suppose que oui, mais je le confirmerai au Comité.

**M. Michael Cooper:** Vous vous engagez à fournir une liste des clients pertinents du gouvernement du Canada. Merci beaucoup.

Je note que la date du 25 août 2023 est postérieure à la publication, le 16 mai 2023, de la directive ministérielle à laquelle vous avez fait allusion.

Cette directive prévoit que le SCRS veillera « à ce que les parlementaires soient informés des menaces à la sécurité du Canada qui sont dirigées contre eux ». Pourquoi les parlementaires n'ont-ils pas été informés comme l'exigeait cette directive ministérielle?

**M. David Vigneault:** Monsieur le président, je pense que nous touchons là au cœur du problème.

Comme je l'ai mentionné, l'écosystème cybernétique comprend différents acteurs dotés de responsabilités et de mandats différents. Nous avons tous travaillé en collaboration, mais aussi, dans une certaine mesure, en parallèle.

Les renseignements initiaux ne provenaient pas du SCRS, mais de nos collègues du CST. Nous collaborons avec eux dans le cadre de notre travail avec la Chambre des communes.

Le député veut savoir si la directive ministérielle pourrait s'appliquer au SCRS, et dans quelles conditions. C'est une question intéressante. Nous sommes en train de nous pencher sur le sujet et d'adapter la directive ministérielle.

**M. Michael Cooper:** Désolé de vous interrompre, mais...

**M. David Vigneault:** Monsieur le président, j'aimerais terminer et dire que le point essentiel ici est qu'à l'époque, l'évaluation indiquait que les renseignements avaient été communiqués à la Chambre des communes pour atténuer cette menace.

**M. Michael Cooper:** Ils n'ont pas été communiqués aux députés, ce qui était l'idée principale de la directive. Le SCRS informait toutefois les clients du gouvernement du Canada jugés pertinents, vraisemblablement le ministère du premier ministre, le BCP. Vous aviez dit que, bien que d'autres organismes ou ministères puissent être mieux placés pour informer les députés, le SCRS aurait pour rôle de mener ou de diriger les discussions sur l'organisation de ces séances d'information.

Cela s'est-il produit?

**M. David Vigneault:** Monsieur le président, je ne pense pas que le rôle du SCRS ait été d'organiser ce type de séance d'information. Il est toutefois clair, avec le recul, que le résultat pour les parlementaires n'a pas été celui que l'on espérait. Je m'engage donc auprès du Comité à tirer des leçons de ce constat, à travailler avec le Comité et à tirer des leçons des résultats de son travail.

Nous et nos partenaires — je peux vous dire que j'ai parlé à mes partenaires du CST — avons tous le même objectif, qui est de veiller à ce qu'à l'avenir, nous obtenions un résultat différent pour les parlementaires.

Je pense que c'est l'un des rôles... Je dirais, en toute franchise, que la collaboration avec les parlementaires par l'intermédiaire de la Chambre des communes est un domaine dans lequel nous devons tous nous améliorer. Nous passons normalement par la Chambre des communes. Je ne veux pas que les députés pensent que nous esquivons nos responsabilités en disant que nous avons communiqué les renseignements à la Chambre des communes et que nous nous lavons les mains du problème. Ce n'était pas du tout notre intention ni notre approche.

Cependant, pour les personnes visées par une cyberattaque de la part du groupe MPA 31, le résultat n'a évidemment pas été celui auquel elles s'attendaient. Je m'engage devant ce comité à ce que mes collègues et moi-même tirions des enseignements de cette expérience et nous assurions, avec nos partenaires, d'obtenir des résultats différents à l'avenir.

• (1120)

**Le président:** Merci beaucoup.

Merci, monsieur Cooper.

[Français]

Madame Fortier, vous avez la parole pour six minutes.

**L'hon. Mona Fortier (Ottawa—Vanier, Lib.):** Merci beaucoup.

Je veux, moi aussi, tenter de comprendre comment cela s'est déroulé. Nous pourrions ensuite voir ce que nous devrions faire si nous devions revivre une telle expérience.

D'abord, le calendrier que le Centre de la sécurité des télécommunications, ou CST, a fourni aux membres du Comité indique que, le 18 février 2021, il a été décidé que le SCRS s'engagerait auprès de la Chambre des communes.

L'équipe de gestion des incidents du Centre canadien pour la cybersécurité a fourni au SCRS une liste de questions techniques pour l'aider à analyser l'activité suspecte.

Pourquoi a-t-il été décidé que le SCRS jouerait un rôle d'intermédiaire entre le CST et la Chambre des communes?

**M. David Vigneault:** Monsieur le président, je n'ai pas de réponse précise en ce qui concerne le rôle d'intermédiaire, sinon que chaque service entretient des relations avec la Chambre des communes. Tant l'administration centrale que les régions travaillent étroitement avec la Chambre. Je présume qu'un certain lien a pu être utilisé à ce niveau.

Je vais demander à M. Madou de répondre.

**M. Peter Madou (directeur adjoint, Exigences, Service canadien du renseignement de sécurité):** En effet, c'est sans doute dû au fait que, depuis plusieurs années, nous avons beaucoup de rapports avec la Chambre des communes. C'était sans doute une solution plus simple. Quand une analyse plus stratégique du problème est nécessaire, c'est souvent notre service qui la fait. Nos collègues du CST font plutôt des analyses techniques.

**L'hon. Mona Fortier:** Selon vous, qui est chargé d'informer les parlementaires des tentatives de cyberattaque, comme celle qui s'est produite, par exemple?

**M. David Vigneault:** Le SCRS, en partenariat avec ses collègues, a tenu pour acquis qu'à partir du moment où on travaillerait avec la Chambre des communes, les responsables de la Chambre allaient informer aux députés. Cette approche n'a pas fonctionné pour différentes raisons.

Je sais que les conditions dans lesquelles cela s'est passé n'étaient pas simples; c'était pendant la pandémie de COVID-19. Il y avait beaucoup de restrictions pour les gens qui étaient au bureau, ce qui compliquait les rencontres. C'était avant l'arrivée du vaccin. Les employés du Service canadien du renseignement de sécurité ont été présents au bureau pendant tout le temps qu'a duré la pandémie. Cela a contribué à créer un peu de confusion dans la répartition des tâches.

Cela dit, nous devrions tous aborder cette question avec humilité et nous demander ce que nous pouvons mieux faire à l'avenir.

**L'hon. Mona Fortier:** Ce que je constate, c'est qu'il y a parfois beaucoup de chefs à la cuisine. Nous pourrions tenter de voir quelle recette nous voulons et établir qui fait quoi. Je crois que c'est ce que nous tentons de comprendre par rapport à la menace qui a pesé sur nous.

**M. David Vigneault:** Monsieur le président, c'est effectivement le cas.

Lorsqu'il s'agit d'enjeux liés à la sécurité nationale, le SCRS est généralement en première ligne. Dans le cas qui nous occupe, la menace à la sécurité nationale a été détectée par nos partenaires du Centre canadien pour la cybersécurité. Par conséquent, au départ, l'analyse a été plutôt technique.

Encore une fois, nous avons tenu pour acquis que, lorsque les autorités de la Chambre des communes seraient informées, elles seraient le vecteur par lequel les parlementaires seraient avertis. Cela n'a pas été le cas.

Nous nous fierons aux conclusions des travaux au Comité et nous ferons en sorte, en tant qu'agence, et non seulement dans notre sphère d'activité, d'analyser la façon de travailler en collaboration avec nos partenaires pour faire en sorte d'obtenir un bon résultat, peu importe qui a fait le travail.

• (1125)

**L'hon. Mona Fortier:** Pensez-vous que seulement une de ces trois organisations peut parler aux parlementaires? Y aurait-il des situations dans lesquelles ces trois organisations, ou deux d'entre elles, devraient pouvoir partager leurs informations avec eux dans le but de les appuyer?

**M. David Vigneault:** Monsieur le président, entre 2021 et 2024, la discussion entourant la sécurité nationale et l'ingérence étrangère a grandement évolué au Canada.

Je ne devrais pas émettre d'hypothèse, mais à l'avenir, il pourrait effectivement y avoir une entité responsable de communiquer de telles informations aux parlementaires. Ce pourrait être la Chambre des communes, compte tenu de sa relation privilégiée avec les parlementaires, de concert avec le SCRS et le CST, qui pourraient aussi être présents. Cela permettrait que la meilleure information soit communiquée aux parlementaires dans les meilleurs délais, pour qu'ils puissent non seulement se protéger, mais également prendre les décisions qui leur incombent.

**L'hon. Mona Fortier:** En terminant, pour ce qui est des parlementaires eux-mêmes, lorsque la personne n'a pas été jointe de la bonne façon, par exemple, en êtes-vous informé? L'avez-vous été, dans la situation en question? Faites-vous un suivi auprès des parlementaires après un incident, peu importe ce qui s'est passé? Pensez-vous que c'est important?

**M. David Vigneault:** Comme je l'ai mentionné, dans le cas qui vous intéresse, lorsque des parlementaires ont été visés par une cyberattaque de la part du groupe MPA 31, le travail n'a pas été fait ainsi. Comme je l'ai mentionné dans mon mot d'ouverture, nous allons donc travailler avec nos partenaires pour nous assurer que nous aurons tous appris de cette situation.

**Le président:** Merci, madame Fortier.

**L'hon. Mona Fortier:** Merci beaucoup.

**Le président:** Madame Gaudreau, vous avez la parole pour six minutes.

**Mme Marie-Hélène Gaudreau (Laurentides—Labelle, BQ):** Je pense qu'on vient de mettre le doigt sur quelque chose, grâce aux questions précédentes. Il n'y a pas d'entité qui prend les commandes pour empêcher que se produise ce qu'on a vécu. On dit que ce ne sont que des hypothèses, mais je trouve cela indispensable.

À plusieurs reprises, monsieur le président, M. Vigneault a dit « nous avons tenu pour acquis ». Or il ne faut rien tenir pour acquis. Je le dis constamment.

Monsieur Vigneault, pouvez-vous me rassurer et me dire que, depuis cet incident, des notes de service sont systématiquement envoyées au ministre responsable?

**M. David Vigneault:** Oui.

**Mme Marie-Hélène Gaudreau:** Alors, si quelqu'un est en vacances, par exemple, cela ne va pas se retrouver à la poubelle. S'il y a une note de service importante, on va la lire et on ne la traitera pas comme une petite alerte. Rassurez-moi à cet égard.

**M. David Vigneault:** Monsieur le président, je peux assurer à la députée que le SCRS travaille en partenariat avec le ministère de la Sécurité publique pour le garantir. Le ministre a été très clair à ce sujet.

**Mme Marie-Hélène Gaudreau:** De notre côté, notre rôle est de légiférer, et je constate que la loi contient plusieurs éléments qui vous freinent. Pour que nous puissions faire notre travail, nous devons savoir ce dont vous avez besoin.

Prenez quelques instants pour nous en parler. Vous y avez réfléchi, j'en suis convaincue.

**M. David Vigneault:** Monsieur le président, comme je l'ai mentionné dans mon allocution d'ouverture, effectivement, la Chambre étudie actuellement un projet de loi visant à moderniser certains aspects de la Loi sur le Service canadien du renseignement de sécurité, le projet de loi C-70.

Il est intéressant de prendre un peu de recul. Cette loi a été promulguée en 1984, en pleine guerre froide, à la suite d'une commission d'enquête qui avait pour but de réviser certaines des activités de l'organisation qui était responsable de la sécurité nationale à l'époque. C'était donc un projet de loi plutôt défensif, à mon avis. Il visait à empêcher que certains écarts ne se reproduisent.

À mon humble avis, les circonstances qui existaient en 1984 n'ont plus cours, en 2024. Le monde a changé. Le visage du Canada a changé et les menaces auxquelles nous faisons face ont changé;

elles ont changé pour ce qui est de la complexité, du nombre d'acteurs qui en sont responsables et des répercussions qu'elles ont au quotidien sur les Canadiens et les Québécois.

Les modifications liées au partage de l'information proposées par le projet de loi C-70, qui est présentement étudié par le Parlement, sont absolument essentielles. Elles visent à simplifier une partie de notre régime relatif aux données, ainsi que la façon dont nous obtenons des mandats de la Cour fédérale, tout en conservant les autorisations judiciaires. Je suis certain que ces changements auront un effet très direct sur les Canadiens.

Je reprends les propos du ministre LeBlanc, qui a mentionné que c'était un premier pas et que d'autres efforts allaient être nécessaires à l'avenir pour moderniser la Loi sur le Service canadien du renseignement de sécurité. Encore une fois, quand vient le temps de protéger les Canadiens contre les menaces, il faut savoir que les moyens employés par ceux qui les trament évoluent très rapidement. Nous devons donc nous assurer de ne pas être à la remorque de ces changements.

● (1130)

**Mme Marie-Hélène Gaudreau:** Je m'inquiète un peu des délais du processus législatif. Nous sommes en train de travailler au projet de loi C-70. On peut se demander si, au moment où les modifications à la loi entreront en vigueur, celle-ci sera encore efficace et si elle répondra toujours à nos besoins.

En ce moment, il est urgent de prendre des mesures. Je crois que nous sommes tous d'accord là-dessus. Pouvons-nous réussir à prévoir des mesures le plus rapidement possible pour que vous ayez les outils nécessaires à votre disposition?

Lors des dernières rencontres que nous avons eues, des témoins nous ont dit que chacun était limité à son carré de sable, dans un carcan, sans pouvoir parler aux autres. J'ai même dit à certains, la semaine dernière, que j'aimerais être leur cliente, parce que cela me permettrait d'avoir de l'information. Je ne l'apprends pas de l'Administration de la Chambre des communes, je ne sais pas si elle va nous informer.

Nous avons besoin de recommandations, parce que, mon avis, le projet de loi C-70 sera périmé au moment où il sera adopté.

Qu'en pensez-vous?

**M. David Vigneault:** Je pense que Mme Gaudreau met le doigt sur quelque chose d'assez important.

Comme fonctionnaire, je vais me permettre de faire le commentaire suivant.

Lorsqu'on aborde les questions de sécurité nationale, il est important, dans la mesure du possible, de ne pas les politiser. Il faut chercher la façon d'arriver le plus rapidement possible à moderniser les différentes lois en faisant preuve de souplesse.

Les changements technologiques s'accroissent et nous dépendons grandement des systèmes de communication. Certaines compagnies changent leurs protocoles et leurs façons de faire. Par ailleurs, beaucoup de travail se fait sur l'accès aux données des télécommunications.

Ce que je souhaite, c'est qu'un comité parlementaire, plutôt qu'étudier des projets omnibus un peu complexes, invite régulièrement des témoins à comparaître et les interroge sur les banques de données, sur les avancées en matière de lutte contre la menace et sur la façon dont nous pouvons combler les besoins le plus rapidement possible. C'est le souhait que je veux transmettre au Comité.

**Mme Marie-Hélène Gaudreau:** Merci beaucoup, monsieur le président. Je vais m'arrêter ici.

**Le président:** Merci, madame Gaudreau.

[Traduction]

Madame Mathysen, vous avez la parole pour six minutes.

**Mme Lindsay Mathysen (London—Fanshawe, NPD):** Merci aux témoins d'être présents aujourd'hui.

Nous voyons clairement — vous l'avez dit vous-même, monsieur Vigneault — qu'une évaluation a été faite à l'époque, que les renseignements ont été transmis et qu'il y a eu une communication de haut niveau. Cependant, nous apprenons constamment, dans cet environnement qui évolue très rapidement, que... Il s'agit clairement d'une question importante à soulever pour montrer que les processus doivent changer. Je salue le travail continu qui est accompli à cet égard.

À l'avenir, nous devons réfléchir à des questions plus larges. Je sais que c'est ce sur quoi je me concentre. J'ai une idée claire de l'orientation que doit prendre ce comité, mais les questions que je me pose s'inscrivent dans un cadre plus large.

J'aimerais parler du rapport du CPSNR.

Il confirmait le fait choquant que des mandataires du gouvernement de Modi s'étaient ingérés dans deux récentes élections conservatrices... Ces renseignements ne sont pas nouveaux. Il y a deux ans, The Bureau a publié un article sur une évaluation de 2022 réalisée par le SCRS.

On y lit ce qui suit:

Des agents du gouvernement indien semblent avoir interféré dans la course à la direction du Parti conservateur en 2022 en achetant des adhésions pour un candidat tout en en sapant un autre, et se sont également vantés de financer « un certain nombre de politiciens à tous les niveaux du gouvernement, »

La même semaine, Baaz a rapporté qu'un représentant du gouvernement indien avait communiqué avec un député conservateur pour retirer son soutien à l'un des candidats.

Pouvez-vous dire à ce comité si les renseignements recueillis par le SCRS ont été communiqués pour le rapport du CPSNR, ou le confirmer?

• (1135)

**M. David Vigneault:** Monsieur le président, avec tout le respect que je dois à la députée, je ne suis pas en mesure de m'exprimer sur les fuites de renseignements dans les médias. Je peux toutefois assurer à la députée que nous avons témoigné et communiquer tous les renseignements permanents pour l'étude du Comité.

Je vais demander à M. Basler, qui est notre coordinateur de la lutte contre l'ingérence étrangère, de parler du volume et de la portée des renseignements que nous avons communiqués.

**M. Bo Basler (directeur général et coordinateur, Ingérence étrangère, Service canadien du renseignement de sécurité):** Merci, monsieur.

Oui, le CPSNR a pu accéder à tous les renseignements des services, à l'exception de ceux qui ont été expurgés pour des raisons de confidentialité, mais nous avons communiqué tous nos renseignements classifiés au Comité. En outre, un certain nombre de fonctionnaires ont comparu devant le Comité pour être interrogés et répondre à des questions directes tout au long de l'étude. Ils disposaient également de tous les renseignements fournis au rapporteur spécial indépendamment lors de son examen. Ces mêmes renseignements ont été transmis à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, ainsi qu'à l'enquête publique.

Je crois que, selon les derniers chiffres du Service, les quatre comités d'examen distincts ont pu accéder à plus de 8 000 documents.

**Mme Lindsay Mathysen:** Au début de cette année, PressProgress a rapporté que le SCRS enquêtait sur l'ingérence étrangère dans la course à l'investiture d'un candidat d'Oxford. L'article indiquait que des responsables locaux du Parti conservateur avaient été interrogés par le SCRS et que des militants conservateurs locaux avaient reçu la visite de responsables du SCRS.

Je pose les mêmes questions et j'aimerais savoir si ces renseignements ont été communiqués au CPSNR. Je comprends que l'on ne veuille pas s'exprimer sur les fuites de renseignements, mais le fait que ces fuites continuent de se produire doit être préoccupant. Je ne vous demande pas de détails, mais dans l'ensemble, nous parlons de ces processus, nous parlons des fuites et des améliorations apportées. Pouvez-vous répondre à la première partie de la question et à la seconde?

**M. David Vigneault:** Monsieur le président, dans ce cas précis, nous avons estimé qu'il s'agissait de journalisme d'enquête et non d'une fuite.

Je ne donnerai évidemment pas de détails sur nos techniques d'enquête ou les sujets de nos enquêtes. Nous avons toutefois dit publiquement dans nos rapports annuels, dans nos discours, lors de nos comparutions devant ce comité et d'autres comités de la Chambre et du Sénat, que le SCRS se préoccupe de l'ingérence étrangère depuis de très nombreuses années. Cette question fait partie de notre travail. Nous enquêtons sur ce problème, mais ces dernières années, nous avons constaté une agressivité accrue de la part d'un certain nombre de pays.

La rapidité et la complexité avec lesquelles la menace d'ingérence étrangère s'abat sur les Canadiens, oui, dans le cadre des processus démocratiques, des élections, mais aussi sur les Canadiens de différentes diasporas dont les droits démocratiques sont bafoués par des nations étrangères, est une question qui préoccupe vivement le SCRS. Voilà pourquoi nous en avons parlé publiquement et de façon confidentielle au gouvernement. Je pense que grâce au travail de ce comité et d'autres comités, du CPSNR, de l'OSSNR et de la commission d'enquête, les Canadiens ont maintenant une meilleure idée de ce qui est nécessaire.



J'aimerais conclure en disant que l'une des meilleures façons de lutter contre l'ingérence étrangère est de faire ce que nous faisons en ce moment, c'est-à-dire en parler en public. Je ne peux évidemment pas vous communiquer de renseignements classifiés, mais en discutant publiquement de ces questions dans différents endroits avec différentes personnes, nous augmenterons la résistance contre ces acteurs. Le SCRS, la GRC ou autres ne peuvent pas toujours attraper les responsables. Nous espérons obtenir de bons résultats, mais ce sont les Canadiens qui, dans leurs activités quotidiennes, vont signaler ces problèmes et vont se dire: « Il se passe quelque chose ici. Je devrais peut-être en parler ».

• (1140)

**Le président:** Merci beaucoup, madame Mathyssen.

Chers collègues, nous passons maintenant au deuxième tour.

Monsieur Cooper, vous avez la parole pour cinq minutes.

**M. Michael Cooper:** Merci, monsieur le président.

En ce qui concerne le rapport du CPSNR, la note 63 de la page 18 indique que le SCRS a informé le premier ministre le 9 février 2021 des activités d'ingérence étrangère du régime de Pékin, plus particulièrement des efforts visant à manipuler les médias canadiens. La RPC avait notamment « payé pour faire publier sans attribution des articles dans les médias, parrainé des voyages médiatiques en Chine, fait pression sur des journalistes pour faire retirer des articles et créé de faux comptes sur les médias sociaux pour faire de la désinformation ».

Avez-vous informé le premier ministre le 9 février 2021? Est-ce que c'était vous?

**M. David Vigneault:** Monsieur le président, je n'ai pas le rapport sous les yeux, mais je vais croire le député sur parole que la référence est effectivement exacte.

Je ne me souviens pas de cette séance d'information particulière. Il faudra que je vérifie si c'était moi-même, un membre de mon équipe ou quelqu'un d'autre qui a informé le premier ministre.

**M. Michael Cooper:** Je vous remercie. Pourriez-vous vérifier également si le premier ministre a été informé avant le 9 février 2021 sur le même sujet?

**M. David Vigneault:** Monsieur le président, nous allons examiner ce point. Nous allons voir ce que nous pouvons faire. Dans les différents comités...

**M. Michael Cooper:** Je vous en serais reconnaissant. Merci.

**M. David Vigneault:** ... nous avons fourni un certain nombre de chronologies. Nous allons voir ce que nous pouvons faire.

**M. Michael Cooper:** Merci.

À la page 19 du rapport du CPSNR, on peut lire que le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections a observé, lors des élections de 2021, une campagne concertée visant à « dissuader les Canadiens, particulièrement les personnes d'origine chinoise, de soutenir le Parti conservateur du Canada ». On lit ensuite ce qui suit: « D'ailleurs, divers organes d'information d'expression chinoise établis au Canada ont repris l'énoncé d'un article publié dans un média étatique chinois sans en indiquer la provenance. De plus, la plupart de ces organes d'information étaient liés à la RPC au titre d'une entente de partenariat conclue avec le service China News, principal média du Parti communiste chinois ».

Si un registre de l'ingérence étrangère avait été mis en place à l'époque, ces médias auraient dû s'inscrire publiquement à la lumière de leurs accords de partenariat avec la RPC. Est-ce exact?

**M. David Vigneault:** Monsieur le président, je me tourne vers mon collègue ici présent pour savoir s'il souhaite donner son avis sur la question.

Je vais devoir renvoyer la question à mes collègues de Sécurité publique Canada, qui sont en train de préparer le registre actuel. Je n'ai pas de réponse définitive à fournir à ce comité.

**M. Michael Cooper:** Je pense que la réponse est oui, dans la mesure où il s'agit d'un accord. Un contrat de partenariat serait un accord avec une entité étrangère, n'est-ce pas?

**M. David Vigneault:** Monsieur le président, il semble que ce soit le cas, mais encore une fois, je ne veux pas spéculer. Je ne suis pas l'expert de ce registre. Nos collègues de Sécurité publique pourront nous éclairer.

**M. Bo Basler:** Je ne pense pas que nous puissions en dire davantage sur la nature et la portée de l'entrée en vigueur d'un accord de partenariat dans le cadre de la législation proposée actuellement. Je pense qu'il serait difficile pour moi de me prononcer à ce sujet.

**M. Michael Cooper:** D'accord. Je me rends compte que vous n'êtes peut-être pas l'autorité en la matière, mais si l'on examine le projet de loi, cette situation correspondrait assez clairement à la définition d'un accord. J'aimerais simplement souligner qu'à la lumière du rapport du CPSNR et d'autres renseignements, y compris ceux transmis par Affaires mondiales Canada et dans les rapports sur le mécanisme d'intervention rapide, il est bien documenté que, pendant les élections de 2021, le régime de Pékin a mené une campagne de désinformation visant à décourager les communautés de la diaspora chinoise de voter pour les conservateurs. Vous seriez d'accord avec cette affirmation.

**M. David Vigneault:** Monsieur le président, par l'entremise de la commission d'enquête présidée par le juge Hogue, le SCRS, en partenariat avec ses collègues, a publié certains résumés d'information, y compris sur ce sujet. Pour répondre le plus précisément possible à la question du député, je renvoie le Comité à ce résumé, qui se base sur l'ensemble des renseignements classifiés et des renseignements publics pour fournir la meilleure réponse possible.

Je pense qu'il s'agit là de la version définitive de cette réponse, monsieur le président.

• (1145)

**M. Michael Cooper:** Me reste-t-il 15 secondes?

**Le président:** Non. Votre temps est écoulé.

**M. Michael Cooper:** D'accord. Merci, monsieur le président.

**Le président:** Merci beaucoup, monsieur Cooper.

Monsieur Gerretsen, vous avez la parole pour cinq minutes.

**M. Mark Gerretsen (Kingston et les Îles, Lib.):** Merci, monsieur le président.

On parle beaucoup de l'ingérence étrangère ces derniers temps, et il semble que vous pensiez que c'est une bonne chose. Comme vous l'avez dit tout à l'heure, les Canadiens doivent être conscients du problème. Qu'il s'agisse de votre travail, de la commission Hogue ou du CPSNR, cette question est à l'avant-scène du débat public. Peut-on dire que c'est en partie dû au travail en cours et à l'importance accrue de ce travail ces dernières années, monsieur Vigneault?

**M. David Vigneault:** Monsieur le président, c'est une question très intéressante. Nous y réfléchissons.

Je pense que le SCRS et ses partenaires consacrent plus de ressources et d'attention à cette question, car la menace s'est accrue au cours des dernières années. Un certain nombre d'acteurs agissent de manière bien plus agressive et font des choses que nous n'avions pas vues auparavant.

**M. Mark Gerretsen:** La connaissance, c'est le pouvoir, donc. La connaissance, c'est le pouvoir. Le fait de disposer de ces renseignements nous donne, ainsi qu'à vous et aux responsables, le pouvoir de lutter contre ce phénomène.

**M. David Vigneault:** Oui, en effet. C'est pourquoi, tout en respectant, dans notre cas, la Loi sur la protection de l'information et les accords conclus avec nos partenaires pour protéger l'information, nous parlons publiquement depuis plusieurs années de l'ingérence étrangère. C'est pourquoi je pense que le fait de mener une discussion plus organisée sur ces questions rendra les Canadiens plus résilients.

**M. Mark Gerretsen:** Certains renseignements sont publics et peuvent faire l'objet de discussion en public, mais d'autres ne le peuvent pas. Quelques rapports sont classifiés pour diverses raisons, mais certaines personnes peuvent y avoir accès, comme le premier ministre, les membres du Cabinet et les chefs officiels de chaque parti politique, bien entendu. S'ils disposent de renseignements issus de ces sources classifiées, peuvent-ils agir en conséquence ou sont-ils limités dans leur action parce que ces renseignements sont classifiés?

**M. David Vigneault:** Monsieur le président, j'ai témoigné à ce sujet il y a quelques jours devant un autre comité, et je formulerai deux ou trois observations en réaction à cette question.

Premièrement, nous sommes en territoire inconnu. Nous ne l'avons jamais exploré avant, alors nous apprenons tous ensemble.

Deuxièmement, je pense que les personnes qui ont la cote de sécurité requise, qui ont besoin de savoir, peuvent effectivement obtenir des séances d'information sur ces questions.

Troisièmement, je pense que, tout en respectant la loi, les gens ont la possibilité et la capacité de prendre des décisions sur la foi de ces renseignements sans avoir à les révéler publiquement.

**M. Mark Gerretsen:** Voilà où je voulais en venir. C'est intéressant. Vous avez fait ce commentaire devant un autre comité, et il en a été question au cours d'un échange à CTV le 9 juin, il y a quelques jours à peine.

En parlant du chef du Parti conservateur, l'animateur a dit: « ce n'est pas parce que votre chef reçoit de l'information à ce sujet qu'il ne peut pas agir. » C'est ce que vous venez de dire. Il a poursuivi en disant: « En fait, il pourrait agir sur la foi de cette information. Quand nous avons fait une entrevue la semaine dernière — l'entrevue était avec M. Chong —, vous pensiez que ce n'était pas le cas. »

M. Chong a répondu: « Je pense qu'il — en faisant ici référence à vous — était dans l'erreur en faisant cette affirmation. Voici pourquoi: le premier ministre demande essentiellement à M. Poilievre de se lier les mains derrière le dos. Voici pourquoi. Il demande à M. Poilievre de passer en revue la politique du Secrétariat du Conseil du Trésor sur la sécurité du gouvernement. C'est le même processus que d'autres personnes — comme les membres du CPSNR, par exemple — ont suivi. Ce processus obligerait M. Poilievre à signer un engagement et à prêter un serment du secret afin

de ne pas divulguer cette information à qui que ce soit. Il ne pourrait donc pas dire à quiconque d'agir sur la foi de ces informations afin de demander des comptes à quelqu'un. »

L'animateur de l'émission a alors respectueusement demandé à son invité s'il était censé le croire, lui, plutôt que le directeur du SCRS.

Michael Chong a répondu par l'affirmative.

Je ne vais pas vous demander de faire des commentaires à ce sujet, parce que je sais que vous ne vous prononcerez pas sur la question, mais vous avez très distinctement affirmé aujourd'hui que si on reçoit de l'information, même si elle est classifiée, on peut l'utiliser pour prendre des décisions, même si on n'est pas autorisé à la divulguer.

• (1150)

**M. David Vigneault:** Monsieur le président, c'est ce que je comprends.

J'ai beaucoup de respect pour M. Chong et ses observations. Je serais heureux d'en discuter avec lui pour peut-être avoir l'occasion de mieux comprendre son point de vue.

**M. Mark Gerretsen:** Je vous remercie.

**Le président:** Merci beaucoup, monsieur Gerretsen.

[Français]

Madame Gaudreau, vous avez la parole pour deux minutes et demie.

**Mme Marie-Hélène Gaudreau:** Monsieur Vigneault, revenons à votre souhait.

J'étais même en train d'imaginer un comité parlementaire qui assurerait une vigie sans trop de pouvoir, mais suffisamment pour laisser tomber la partisanerie afin d'éviter les fuites dans les journaux, entre autres choses.

Pouvez-vous fournir davantage de commentaires sur ce sujet?

**M. David Vigneault:** Monsieur le président, en réfléchissant à la question de la députée, j'ai en tête différents modèles.

Par exemple, nos partenaires de l'Australie ont notamment recours, à intervalles réguliers de quelques années, à un tiers de l'extérieur du gouvernement qui revoit toutes les ententes et les lois qui régissent la sécurité nationale. L'objectif est de s'assurer que, selon l'état de la menace, les fameux outils dans la boîte à outils sont les bons et qu'ils sont tenus à jour. Ce type d'exercice vise à faire état de la situation en dehors des périodes électorales.

J'ai dit à plusieurs reprises, au cours des dernières années, que le Canada a été chanceux et que les menaces auxquelles il a été confronté ont été différentes de celles d'autres pays. Grâce à notre géographie, aux trois océans qui bordent le pays et au fait que nous avons les États-Unis comme partenaire économique et militaire, nous avons échappé à l'intensité des menaces que certains autres pays ont vécues.

Ainsi, les Canadiens, avec raison — je m'en réjouis —, n'ont pas eu à réfléchir à ces questions de la même façon et avec la même intensité que d'autres. Par contre, le monde a changé, et toutes les tendances qui ont fait du Canada un pays prospère, sécuritaire et souverain vont dans la mauvaise direction depuis quelques années. Je crois fermement que de trouver une façon différente de discuter de ces menaces, y compris au Parlement, est une approche très raisonnée.

**Mme Marie-Hélène Gaudreau:** En résumé, si je comprends bien, il faut vraiment faire une analyse des modèles du Groupe des cinq, afin de se créer un modèle et d'être fins prêts à faire face aux menaces.

Mon temps de parole est écoulé.

Merci.

**Le président:** Merci beaucoup, madame Gaudreau.

[Traduction]

Madame Mathysen, vous disposez de deux minutes et demie.

**Mme Lindsay Mathysen:** Je vous remercie.

Pour faire suite à la question de M. Gerretsen, le premier ministre a-t-il le rapport complet non caviardé du CPSNR depuis maintenant 11 semaines?

**M. David Vigneault:** Monsieur le président, je croirais la députée sur parole, mais chose certaine, il l'a depuis une certaine période.

**Mme Lindsay Mathysen:** Mais il n'a rien fait. D'accord. Je ne faisais que vérifier.

Dans le temps dont je dispose, j'aimerais donner avis d'une motion, monsieur le président. Ce n'est qu'un avis, que nous distribuons sous peu:

Compte tenu des conclusions récentes du rapport spécial du CPSNR sur l'ingérence étrangère dans les processus et les institutions démocratiques du Canada, le Comité permanent de la procédure et des affaires de la Chambre ordonne la production de toutes les notes de service, les notes d'information, les courriels et les comptes rendus de conversation pertinents ainsi que de tout autre document pertinent en possession du Service canadien du renseignement de sécurité et du Centre de la sécurité des télécommunications Canada, concernant l'impact de l'ingérence étrangère sur les courses à la direction du Parti conservateur du Canada en 2020 et 2022, à condition que:

(i) les deux organismes chargés de recueillir ces documents y appliquent des caviardages conformément à la Loi sur l'accès à l'information et à la Loi sur la protection des renseignements personnels;

(ii) les documents caviardés soient déposés aussitôt que possible, mais au plus tard le dimanche 23 juin 2024, auprès du greffier du Comité pour être communiqués à tous les membres du Comité dans les deux langues officielles.

**Le président:** Nous prenons acte de la motion.

Je crois comprendre que vous choisissez de ne pas proposer cette motion, madame Mathysen. Il reste donc...

**Mme Lindsay Mathysen:** Je donne un avis de motion. Je dois...

**Le président:** Oui, d'accord. Il vous reste 45 secondes pour poser vos questions, si vous le souhaitez.

**Mme Lindsay Mathysen:** En fait, je n'aurais pas d'objection à poursuivre dans la même veine que Mme Gaudreau.

Lorsque j'étais en voyage à Taïwan, il a été énormément question des aléas que subissent les Taïwanais, avec les bombardements et l'ingérence étrangère, et de l'éducation prodiguée à la population. Avez-vous travaillé avec le gouvernement de Taïwan pour tirer des

enseignements de cette situation, éduquer la population ou même envisager l'idée d'un ministre des Affaires numériques?

• (1155)

**M. David Vigneault:** Monsieur le président, je répondrai très brièvement que je ne ferai pas de commentaire précis sur les interactions du SCRS avec des partenaires, mais je peux rassurer la députée en affirmant qu'un certain nombre de partenaires au sein du gouvernement se sont effectivement penchés sur ces questions précises avec des partenaires à Taïwan.

**Le président:** D'accord.

Merci beaucoup, madame Mathysen.

[Français]

Monsieur Berthold, vous avez maintenant la parole pour cinq minutes.

**M. Luc Berthold (Mégantic—L'Érable, PCC):** Merci beaucoup, monsieur le président.

Je trouve très ironique, encore une fois, de voir le NPD se lancer à la défense du gouvernement alors que nous avons présenté, à plusieurs reprises, des motions pour la production de documents, et ce, pendant des semaines. Chaque fois, le NPD a voté comme le gouvernement pour empêcher la production de documents. Je trouve donc plutôt ironique que ma collègue du NPD présente une motion aujourd'hui.

Monsieur Vigneault, dans votre déclaration d'ouverture, vous avez parlé de l'importance de ne pas politiser les questions de sécurité nationale. Je dois y revenir, car il est important de mentionner que, politiser les questions de sécurité nationale, cela ne signifie pas qu'il ne faut pas en parler; cela ne veut pas dire que l'opposition ne peut pas en parler ou poser des questions auxquelles il est difficile de répondre. En fait, cela signifie plutôt qu'on se sert de certaines informations pour mettre en avant ses intérêts partisans.

Est-ce bien ce que vous vouliez dire quand vous parliez de politiser les questions de sécurité nationale?

**M. David Vigneault:** Monsieur le président, dans une large mesure, c'est exactement ce que je voulais dire.

Je rappelle que le poste que j'occupe implique un devoir de réserve. Cela dit, lorsque des intérêts partisans sont pris en compte, ce qui est normal dans une démocratie — nous sommes heureux de vivre dans une démocratie —, les questions fondamentales sont peut-être un peu occultées. De mon point de vue, cela devient effectivement plus compliqué lorsque c'est politisé.

**M. Luc Berthold:** Si le gouvernement ferme les yeux sur certaines informations, s'il refuse de voir des informations classifiées pour ne pas se mettre dans l'embarras vis-à-vis son parti, s'il refuse d'agir quand il a de l'information sur un candidat qui aurait reçu l'appui d'une puissance étrangère hostile, s'il rejette le blâme sur une autre association ou s'il ne prend tout simplement pas ses responsabilités, cela revient à politiser le débat sur la sécurité nationale.

Est-ce exact?

**M. David Vigneault:** Monsieur le président, je pense que personne ne se surprendra du fait que je ne ferai pas de commentaire sur les propos du député.

Par contre, je peux dire que la discussion qui a lieu en ce moment et les travaux de ce comité sont essentiels pour que les Canadiens soient mieux protégés contre l'ingérence étrangère et les nombreuses autres menaces.

**M. Luc Berthold:** Permettez-moi, monsieur Vigneault, d'insister là-dessus.

Je ne voudrais pas que, dans l'esprit des gens, le débat politique autour des questions dont nous parlons actuellement se limite uniquement aux travaux du Comité ou ne se tienne qu'à la suite de fuites. Les décisions pouvant être prises au sein d'un gouvernement qui a des intérêts partisans peuvent aussi politiser la question de la sécurité nationale. On ne peut pas dire le contraire.

**M. David Vigneault:** Monsieur le président, je vais exercer un devoir de réserve sur ces commentaires, mais j'apprécie la question du député.

**M. Luc Berthold:** Monsieur Vigneault, qui, dans l'appareil gouvernemental, peut décider de déclassifier une information jugée confidentielle ou ultra-secrète? Je ne sais pas comment cela fonctionne, mais qui peut décider qu'une information, hier secrète, est aujourd'hui publique?

**M. David Vigneault:** Monsieur le président, en fait, c'est une très bonne question à laquelle il n'y a malheureusement pas de très bonne réponse, dans la mesure où il n'y a pas de politique de déclassification.

Prenons pour exemple le Service canadien du renseignement de sécurité. L'information qui émane du Service est gouvernée non seulement par la Loi sur le Service canadien du renseignement de sécurité et par la Loi sur la protection de l'information, mais aussi par nos pratiques et nos engagements. Il n'y a donc pas de politique au sein du gouvernement ni d'autorité qui peut ordonner cette déclassification.

**M. Luc Berthold:** Est-il exact que, dans le cas d'une question grave de sécurité nationale, le premier ministre peut utiliser l'information et la rendre publique?

**M. David Vigneault:** Généralement, d'après mon expérience, la divulgation de l'information se fait en collaboration avec les agences.

Je vais vous donner un exemple très concret. La première fois que nous avons mentionné le nom de certains pays qui étaient impliqués dans cette affaire, il s'agissait d'une information classifiée. Nous avons fait le travail nécessaire qui nous permettrait de dire que, maintenant, selon l'information connue publiquement et l'impact sur nos opérations, nous pouvons commencer à en dire un peu plus.

C'est donc un processus itératif, mais il n'est pas basé sur une politique du gouvernement.

- (1200)

**M. Luc Berthold:** Je n'ai pas beaucoup de temps, alors soyons brefs. C'est quand même une directive du premier ministre qui vous a permis de dévoiler l'information à des députés qui avaient été visés par l'ingérence étrangère, de divulguer ces informations auparavant secrètes à ces députés.

**M. David Vigneault:** Monsieur le président, pour être plus précis, nous nous sommes prévalus de l'article 12.1 de la Loi sur le Service canadien du renseignement de sécurité, qui porte sur la mesure sur l'atténuation des menaces. C'est ce processus, basé sur la

loi sur le SCRS, qui m'a permis d'avoir la première discussion avec le M. Chong.

**M. Luc Berthold:** Vous aviez bien parlé, tout à l'heure...

**Le président:** Malheureusement, monsieur Berthold, c'est tout le temps dont vous disposez. Je suis désolé.

Madame Romanado, vous avez la parole pour cinq minutes.

[Traduction]

**Mme Sherry Romanado (Longueuil—Charles-LeMoine, Lib.):** Merci beaucoup, monsieur le président. Par votre entremise, je remercie les témoins de leur présence.

Monsieur Vigneault, vous avez indiqué que votre équipe a rencontré plus de 70 députés pour les informer au cours des deux dernières années. Est-ce exact?

**M. David Vigneault:** Oui, monsieur le président, c'est juste. Nous avons rencontré 70 parlementaires, et je pense qu'en ce qui concerne les Canadiens, nous avons rencontré plus de 1 000 personnes.

**Mme Sherry Romanado:** Pouvez-vous confirmer que vous avez rencontré les parlementaires victimes de cette cyberattaque?

**M. David Vigneault:** Monsieur le président, je vais devoir vérifier cette information pour vous confirmer ce qu'il en est.

**Mme Sherry Romanado:** Vous engagez-vous à le faire? La directive de mai 2023 était claire: tous les parlementaires ciblés doivent être mis au courant. Je voudrais donc m'assurer que tous les parlementaires... Certains viendront témoigner jeudi, et nous leur demanderons si le SCRS les a rencontrés pour les informer.

**M. David Vigneault:** Monsieur le président, je m'engage à confirmer si les députés ont été rencontrés. Cependant, je pense qu'il était très clair, dans mon témoignage et les informations présentées au Comité, que lorsque nous avons communiqué l'information, nous nous attendions à ce que la Chambre des communes transmette les informations précises. En outre, la directive ministérielle envoyée au SCRS est arrivée environ deux ans plus tard que... l'incident. Je pense donc qu'il est important de garder ces deux points à l'esprit lorsqu'on réfléchit à ce qui a été fait ici.

**Mme Sherry Romanado:** Monsieur Vigneault, vous avez eu deux ans pour informer les gens. Vous avez eu plus d'un an, depuis la directive de 2023, pour communiquer avec les députés et les sénateurs touchés. Lorsque j'examine ce que nous avons entendu au cours de cette étude, c'est presque nous avons communiqué l'information, nous nous attendions à ce que la Chambre des communes transmette les informations précises. En outre, la directive ministérielle envoyée au SCRS est arrivée environ deux ans plus tard que... l'incident. Je pense donc qu'il est important de garder ces deux points à l'esprit lorsqu'on réfléchit à ce qui a été fait ici.

Face à ce qui semble être une véritable défaillance, personne ne veut assumer la responsabilité du fait que les parlementaires — ceux-là mêmes qui, selon vous, sont la cible d'ingérence étrangère — ne sont pas informés. C'est fort préoccupant pour nous. Je comprends que vous voulez tirer des leçons de l'affaire, mais en attendant, nos adversaires qui ciblent des parlementaires s'en tirent à bon compte.

Quelle structure faut-il mettre en place pour assurer un dialogue constant avec les personnes ciblées, que ce soit par des acteurs étatiques ou non étatiques? J'ai peut-être des renseignements que vous n'avez pas. Il semble y avoir un manque. Quand on dit que c'est à la Chambre des communes qu'il incombait d'informer les parlementaires, qu'en est-il du Sénat? Le groupe des TI de la Chambre des communes est-il également responsable du Sénat? Il semble y avoir beaucoup de « ce n'est pas mon problème » ou « j'ai joué mon rôle dans la chaîne de montage », mais au bout du compte, le travail ne s'effectue pas. Que devons-nous faire pour qu'il se fasse?

**M. David Vigneault:** Monsieur le président, dans mon exposé et mes commentaires précédents, je pense avoir dit clairement que le résultat observé ici n'est pas celui que les députés ou les sénateurs membres de l'AIPC auraient souhaité. Ce n'est certainement pas celui que nous aurions souhaité, car notre travail en matière de sécurité nationale consiste à nous assurer que nous permettons aux gens de se défendre et que nous accomplissons notre travail.

Par conséquent, je me suis engagé envers le Comité à tirer des leçons de cette affaire avec mes partenaires du SCRS, du CST, de la Chambre des communes et du Sénat et à chercher à voir comment nous harmonisons les différentes autorités, puisque nous devons également respecter les mandats et les lois qui régissent nos actions. Comment pouvons-nous combiner ces éléments pour nous assurer que le résultat soit différent à l'avenir?

J'étais très sincère, monsieur le président, lorsque j'ai fait cette offre auparavant. C'est probablement la meilleure réponse que je puisse donner à la députée.

• (1205)

**Mme Sherry Romanado:** Mon temps est écoulé. Je poserai donc d'autres questions pendant la séance à huis clos.

Je vous remercie.

**Le président:** Merci beaucoup, madame Romanado.

Chers collègues, nous allons suspendre la séance...

**M. Blaine Calkins (Red Deer—Lacombe, PCC):** Monsieur le président, puis-je auparavant poser une question à mes collègues du Comité?

**Le président:** Invoquez-vous le Règlement, monsieur Calkins?

**M. Blaine Calkins:** J'aimerais savoir pourquoi et à quelle fin nous nous réunissons à huis clos. Le directeur a essentiellement dit que nous devons tenir une conversation publique avec le...

**Le président:** Monsieur Calkins, je suis désolé de vous interrompre, mais je vais suspendre la séance.

Nous pourrions en discuter pendant la brève intermission.

Le Comité a convenu de siéger à huis clos. Il est très inhabituel pour nous de discuter de la possibilité de modifier cette pratique. Nous pourrions, bien sûr...

**M. Blaine Calkins:** Nous pouvons en parler, n'est-ce pas?

**Le président:** ... proposer une motion, si vous le souhaitez, afin de modifier...

**M. Blaine Calkins:** Je propose que nous poursuivions la séance en public.

**Le président:** ... nos paramètres, mais je vais suspendre brièvement la séance pour que nous puissions en parler entre collègues...

**M. Eric Duncan (Stormont—Dundas—South Glengarry, PCC):** Nous venons de proposer quelque chose.

**Le président:** Je vais suspendre brièvement la séance pour que nous puissions discuter entre collègues, puis nous déciderons ce que nous voulons faire.

*[La séance se poursuit à huis clos.]*





Publié en conformité de l'autorité  
du Président de la Chambre des communes

---

### PERMISSION DU PRÉSIDENT

---

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

---

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante :  
<https://www.noscommunes.ca>

Published under the authority of the Speaker of  
the House of Commons

---

### SPEAKER'S PERMISSION

---

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

---

Also available on the House of Commons website at the following address: <https://www.ourcommons.ca>