CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

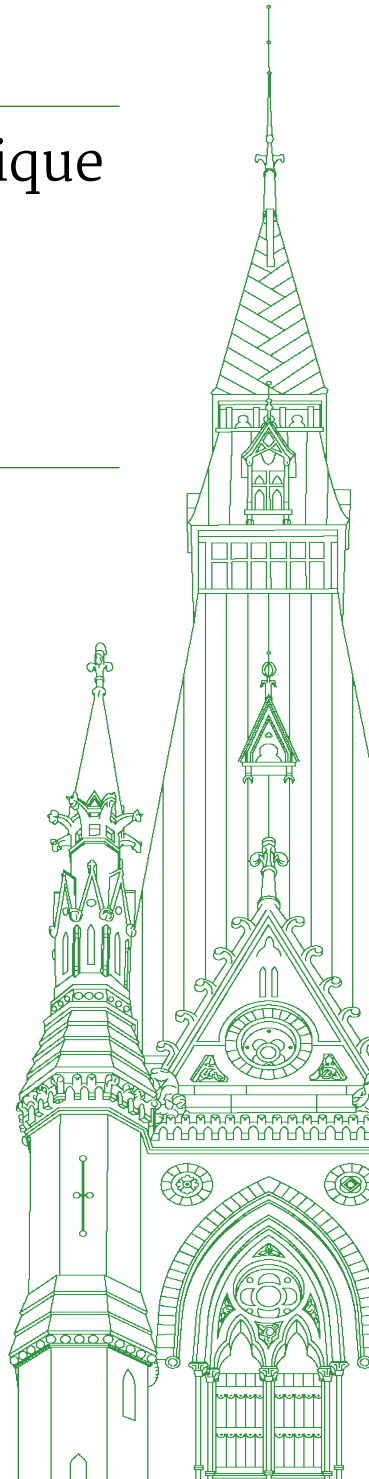
45e LÉGISLATURE, 1re SESSION

Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 051

Le mercredi 21 octobre 2026



Président : Jean-Yves Duclos

Comité permanent de la sécurité publique et nationale

Le mercredi 21 octobre 2026

● (1630)

[*Français*]

Le président (L'hon. Jean-Yves Duclos (Québec-Centre, Lib.)): Nous ouvrons maintenant la séance.

Bonjour, tout le monde. Je vous remercie de vous être déplacés en personne pour participer à la 51e réunion du Comité permanent de la sécurité publique et nationale de la Chambre des communes ou d'y assister virtuellement.

Conformément à l'article 108(2) du Règlement, nous nous réunissons aujourd'hui pour faire l'étude du processus de contrôle de sécurité du Canada, qui découle de la motion adoptée le 17 août.

J'aimerais tout d'abord souhaiter la bienvenue aux trois témoins, qui participent tous à la réunion à distance.

Nous accueillons à titre personnel Christian Leuprecht, professeur au Collège militaire royal du Canada, et Michael Wernick, titulaire de la Chaire Jarislowsky sur la gestion dans le secteur public à l'Université d'Ottawa. De l'Agence spatiale canadienne, nous avons Jean-Claude Piedboeuf, vice-président principal responsable des programmes spatiaux.

Chaque témoin aura cinq minutes pour faire une intervention.

Vous avez la parole, monsieur Leuprecht.

Christian Leuprecht (professeur, Collège militaire royal du Canada, à titre personnel): Bonjour, mesdames et messieurs.

Monsieur le président, je vous remercie de votre intervention et de l'invitation.

Je vais intervenir en anglais et je vais répondre à vos questions dans l'une ou l'autre des deux langues officielles.

[*Traduction*]

J'ai passé deux décennies à faire des recherches et à écrire sur des questions de sécurité nationale, y compris des questions de sécurité de la recherche, que je connais particulièrement bien. J'ai également écrit un livre sur la communauté du renseignement du Groupe des cinq. En tant que professeur au Collège militaire royal qui collabore avec d'autres ministères, je suis également soumis à des processus de filtrage de sécurité.

Le système ne sera jamais infaillible. Il est plutôt conçu pour procéder à des évaluations raisonnables des risques en amont, en fonction de la personne, du poste et des tâches, puis pour faire preuve de souplesse et de réactivité lorsque des signaux d'alarme apparaissent. L'affaire à l'origine de la réunion d'aujourd'hui montre qu'il y a eu des défaillances des deux côtés: une évaluation inadéquate des risques en amont et une inaction subséquente face aux signaux faibles.

J'ai trois observations à faire à ce sujet.

En février dernier, la Jamestown Fondation a publié un rapport qui présentait le Canada comme le pays le plus corrompu par la Chine parmi les pays du G7. La Commission sur l'ingérence étrangère a documenté la portée et l'ampleur de l'ingérence étrangère et de l'influence malveillante au Canada, en particulier par le Département du travail du Front uni de la Chine. En 2024, le Comité des parlementaires sur la sécurité nationale et le renseignement a finalement publié la version caviardée de son rapport tant attendu sur l'ingérence étrangère dans les processus et les institutions démocratiques du Canada.

Sam Cooper a documenté l'étendue de l'emprise sur les élites au sein des réseaux politiques, diplomatiques, d'affaires et d'entreprises du Canada à l'échelle fédérale, régionale et locale. La portée, l'ampleur et la sophistication des activités de compromission contre le Canada sont bien documentées dans les versions non classifiées des rapports annuels du SCRS. Autrement dit, le gouvernement aurait dû être bien au courant des risques et des vulnérabilités provenant d'abord et avant tout de la Chine.

Entre 2020 et 2023, le gouvernement a triplé le nombre d'immigrants admis à près de deux millions de personnes. Aucune ressource proportionnelle supplémentaire n'a été accordée aux trois organismes — l'ASFC, IRCC et le SCRS — chargés des vérifications visant les nouveaux arrivants au pays. On peut supposer que des dizaines, voire des centaines de milliers de personnes ont été autorisées à entrer et à résider dans le pays sans vérification adéquate. De même, entre 2015 et 2024, la taille de la fonction publique a augmenté de plus de 40 %, passant de 257 000 à 368 000 employés, mais étant donné le manque de ressources supplémentaires pour les organismes de la sécurité et du renseignement, il est peu probable que bon nombre des nouveaux fonctionnaires aient fait l'objet d'une vérification rigoureuse.

Au bout du compte, les niveaux d'immigration, la taille de la fonction publique et l'affectation des ressources sont des décisions politiques. Le gouvernement de l'époque a choisi de donner la priorité à l'immigration et à la croissance de la fonction publique au détriment de la sécurité et du filtrage. Autrement dit, le gouvernement a sciemment exposé le Canada et la fonction publique à un risque de sécurité accru. Le cas tristement célèbre du contrat accordé à Nuctech pour les appareils à rayons X dans les ambassades canadiennes est un exemple probant. La mollesse de la politique du gouvernement fédéral en matière de sécurité de la recherche est un autre exemple. Le gouvernement fédéral doit trouver un meilleur équilibre entre ses politiques visant à accroître l'immigration et la fonction publique, d'une part, et la nécessité d'assurer l'intégrité des technologies et des personnes admises au pays et embauchées comme fonctionnaires, d'autre part.

Les espions étrangers savent qu'ils peuvent mener leurs activités au Canada dans une relative impunité. Les deux scientifiques chinois du laboratoire de microbiologie de niveau 4, à Winnipeg, ont étrangement été en mesure de quitter le pays pendant la pandémie, alors que les déplacements étaient très limités, au lieu d'être traduits en justice, et le gouvernement a activement supprimé les documents connexes. Mikhail Mikushin, un agent russe du GRU, a pu étudier et mener ses activités au Canada en toute quiétude, jusqu'à son arrestation par les autorités norvégiennes. Dans l'affaire à l'origine de la présente séance, qui illustre un problème classique lié aux signaux faibles, la personne visée a enfreint la politique fédérale, mais la primauté des politiques en matière d'EDI a certainement un effet dissuasif sur tout gestionnaire qui prendrait le risque de remettre en cause l'intégrité d'une jeune femme racisée.

Bref, il ne s'agit pas, en premier lieu, d'une défaillance des processus de filtrage de sécurité. Le gouvernement est bien conscient des risques associés à la Chine. Le gouvernement a choisi de ne pas optimiser les ressources en fonction de la portée et de l'ampleur de la menace. Lorsque des risques surviennent, le gouvernement préfère faire disparaître les problèmes au lieu d'agir pour assurer la sécurité du pays et de ses alliés. Il est difficile d'exagérer l'ampleur des dommages à notre réputation lorsque des espions étrangers opèrent au Canada, puis sont ensuite interpellés par nos alliés.

En fin de compte, il ne s'agit pas d'une défaillance du processus de filtrage de sécurité. Il s'agit d'un manque de volonté politique de reconnaître les menaces à l'intérêt national et à la sécurité nationale provenant d'acteurs étrangers, et de réagir en conséquence, qui est exacerbé par une culture institutionnelle qui dissuade de réagir à de faibles signaux [*difficultés techniques*]. Ce qu'il faut retenir, c'est la nécessité d'une volonté politique d'avoir conscience que la subversion et les menaces internes au sein des institutions fédérales...

● (1635)

Le président: Je suis désolé, monsieur Leuprecht. Nous allons faire une brève pause pour nous assurer que les interprètes vous entendent bien. Je crois qu'il y a des problèmes de communication.

Pouvez-vous recommencer?

Christian Leuprecht: [*Difficultés techniques.*]

Le président: C'est dommage. Je dois vous interrompre, car nous ne vous entendons pas bien.

Pendant que nous essayons de régler le problème de connexion, monsieur Leuprecht, permettez-moi de donner la parole à M. Wernick pour cinq minutes, puis à M. Piedboeuf. Nous pourrons peut-être vous redonner la parole pour la dernière minute, après la déclaration de M. Piedboeuf.

Monsieur Wernick, allez-y.

[*Français*]

Michael Wernick (titulaire de la chaire Jarislowsky en gestion du secteur public, Université d'Ottawa, à titre personnel): Je vous remercie de l'invitation.

Je me demande pourquoi j'ai été invité.

[*Traduction*]

Je n'ai pas de déclaration préliminaire à faire. Je serai ravi de répondre à vos questions et d'essayer d'aider le Comité. J'ai souvent été invité à des comités parlementaires, et je respecte le travail que vous faites.

Je tiens à préciser pour les membres du Comité, en particulier les nouveaux, que j'ai quitté la fonction publique il y a sept ans et demi. Je n'ai plus de cote de sécurité, et cela fait des années que je n'en ai pas fait le processus. Je n'ai aucun contact avec les gens du gouvernement dont vous avez discuté la semaine dernière. Je n'ai parlé de cette question à personne au sein du gouvernement, et je n'ai aucune connaissance particulière de cette affaire, si ce n'est ce que j'ai lu dans les médias.

Je pourrais peut-être vous aider à cerner les faiblesses du système actuel et, peut-être, à aborder les questions de la reddition de comptes et du fonctionnement de l'appareil gouvernemental en vue d'améliorer le système à l'avenir.

● (1640)

[*Français*]

Le président: Je vous remercie, monsieur Wernick.

Monsieur Piedboeuf, vous avez la parole pour cinq minutes.

Jean-Claude Piedboeuf (vice-président principal, Programmes spatiaux, Agence spatiale canadienne): Je vous remercie, monsieur le président.

Je suis Jean-Claude Piedboeuf, vice-président principal responsable des programmes spatiaux à l'Agence spatiale canadienne, ou ASC. Je vous remercie de me donner l'occasion de témoigner devant le Comité pour présenter l'approche et la position de l'ASC en matière de sécurité, ainsi que les mesures que nous prenons pour renforcer cette dernière.

Je comprends que le Comité pourrait être intéressé par l'incident en Belgique, mais, en raison de l'enquête en cours, je limiterai mes observations aux mécanismes de filtrage, de sécurité, de contrôle, de partage d'information et de surveillance de l'ASC.

[*Traduction*]

Le mandat de l'Agence spatiale canadienne est de promouvoir l'exploitation et l'usage pacifiques de l'espace, de faire progresser la connaissance de l'espace au moyen de la science et de faire en sorte que les Canadiens tirent profit des sciences et techniques spatiales sur les plans tant social qu'économique. Notre mandat repose sur l'innovation et la collaboration. Il exige aussi de protéger les personnes, les renseignements, les installations et les technologies qui nous sont confiés, en assurant une gestion rigoureuse des programmes et des missions spatiales qui font souvent appel à des technologies de pointe, à des renseignements scientifiques et techniques de nature délicate et à des installations spécialisées.

Ces activités sont réalisées en collaboration avec des partenaires gouvernementaux, industriels, universitaires et internationaux. Dans ce contexte, le filtrage de sécurité contribue à protéger les renseignements, les biens et les activités sensibles du gouvernement du Canada. Selon la nature des fonctions et les accès requis, les personnes concernées doivent détenir la cote ou l'autorisation de sécurité appropriée.

Le filtrage de sécurité à l'Agence spatiale canadienne s'inscrit dans le cadre établi par la Politique sur la sécurité du gouvernement et la Directive sur le filtrage de sécurité du SCT. Ces instruments établissent le cadre gouvernemental applicable au filtrage de sécurité. L'administrateur général désigne un dirigeant principal de la sécurité, qui exerce les responsabilités et les pouvoirs qui lui sont confiés en matière de filtrage de sécurité.

[*Français*]

Le filtrage de sécurité est une composante essentielle de notre approche. Il contribue à évaluer la fiabilité des personnes et leur admissibilité à l'accès à l'information requise dans le cadre de leurs fonctions. Une habilitation de sécurité ne donne pas un accès automatique à tous les renseignements d'un même niveau. L'accès est octroyé en fonction des responsabilités de la personne dans le respect du principe du besoin de connaître.

Plus concrètement, lorsqu'un employé a besoin d'accéder à des renseignements protégés, le niveau minimal de la cote de sécurité est la cote de fiabilité. À l'ASC, la plupart des postes exigent soit une cote de fiabilité ou une autorisation de sécurité de niveau Secret. Un nombre plus restreint de fonctions nécessite une autorisation de sécurité de niveau Très secret.

Le niveau requis est déterminé en fonction du poste, notamment des tâches à accomplir et de la sensibilité des renseignements, des biens, des installations et des systèmes auxquels la personne doit avoir accès.

L'ASC applique un processus structuré de filtrage de sécurité qui comprend le consentement de la personne, la vérification de son identité et de ses antécédents, ainsi que les autres vérifications requises en fonction du niveau de filtrage. De plus, des recherches sur Internet sont effectuées au besoin, lorsqu'il y a des informations défavorables dans un dossier de sécurité. Par ailleurs, la mise en œuvre du programme de recherche sur Internet pour le niveau Très secret est prévue pour novembre 2026.

[*Traduction*]

Dans le cadre de ce processus, l'Agence spatiale canadienne fait appel, lorsque requis, aux partenaires fédéraux compétents, notamment la GRC et le SCRS, dans le cadre de leurs responsabilités respectives. Les résultats complets de ces vérifications d'antécédents sont évalués avant qu'une décision ne soit prise par le dirigeant principal de la sécurité et les responsables délégués autorisés, conformément à la délégation des pouvoirs en matière de filtrage de sécurité.

Au cours des dernières années, l'Agence spatiale canadienne a ajouté des ressources en sécurité pour renforcer sa capacité à soutenir ses activités. L'Agence a également accru le nombre de personnes détenant une habilitation de sécurité de niveau très secret, offert des séances de sensibilisation à la sécurité spatiale et réalisé des évaluations des menaces et des risques. Elle continuera de renforcer sa posture de sécurité de façon continue en fonction de l'évolution des menaces et des risques afin de s'assurer que les renseignements sensibles du gouvernement du Canada et de ses partenaires sont gérés selon des normes rigoureuses adaptées aux exigences de sécurité.

L'Agence spatiale canadienne assure une surveillance continue en combinant des mécanismes automatisés, des contrôles périodiques et le suivi des événements de sécurité. Elle surveille notamment les alertes de cybersécurité, les accès, améliore les systèmes de sécurité physique et surveille les changements qui pourraient modifier le niveau de risque. Les incidents et les renseignements préoccupants sont évalués et font l'objet de mesures de suivi appropriées.

● (1645)

[*Français*]

En conclusion, un filtrage de sécurité efficace est essentiel pour protéger le travail de nature délicate confié à l'ASC. Nous accordons une grande importance à la protection de nos renseignements, de nos installations et de nos personnes, ainsi qu'au maintien d'une solide culture de sécurité. Nous continuerons d'appliquer avec rigueur les exigences gouvernementales en matière de filtrage de sécurité et de travailler avec nos partenaires pour protéger les activités et les renseignements qui nous sont confiés.

Je vous remercie de m'avoir donné l'occasion de témoigner devant vous aujourd'hui. Je serai heureux de répondre aux questions du Comité.

Le président: Je vous remercie beaucoup, monsieur Piedboeuf.

[*Traduction*]

Monsieur Leuprecht, voulez-vous essayer de terminer votre intervention? Il vous reste une minute et demie.

Christian Leuprecht: Monsieur le président, à quel endroit voulez-vous que je reprenne, pour aider les interprètes?

Le président: Comme bon vous semble; il vous reste une minute et demie.

Christian Leuprecht: Je vais simplement répéter mon dernier paragraphe.

Bref, il ne s'agit pas, en premier lieu, d'une défaillance des processus de filtrage de sécurité. Le gouvernement est bien conscient des risques associés à la Chine. Le gouvernement a choisi de ne pas optimiser les ressources en fonction de la portée et de l'ampleur de la menace. Lorsque des risques surviennent, le gouvernement préfère faire disparaître les problèmes au lieu d'agir pour assurer la sécurité du pays et de ses alliés.

Il est difficile d'exagérer l'ampleur des dommages à notre réputation lorsque des espions étrangers opèrent au Canada, puis sont ensuite interpellés par nos alliés. En fin de compte, il ne s'agit pas d'une défaillance du processus de filtrage de sécurité. Il s'agit d'un manque de volonté politique de reconnaître les menaces à l'intérêt national et à la sécurité nationale provenant d'acteurs étrangers, et de réagir en conséquence, qui est exacerbé par une culture institutionnelle qui décourage toute réaction face à des signaux faibles indiquant d'éventuelles menaces internes.

Voici ce qu'il faut retenir: il faut une volonté politique. Il faut prendre conscience que la subversion et les menaces internes sont omniprésentes au sein des institutions fédérales. Il faut doter les organismes de sécurité et de renseignement des ressources nécessaires, et demander des comptes aux gestionnaires.

Le Comité pourrait se poser la question suivante: a-t-on exigé des comptes aux gestionnaires, aux sous-ministres ou aux ministres responsables dans le cas qui nous occupe, ou dans d'autres cas de menaces internes au sein du gouvernement du Canada? Se concentrer sur le processus de filtrage de sécurité, c'est être trop près de l'arbre pour voir la forêt.

[*Français*]

Je vous remercie.

Le président: Je vous remercie beaucoup tous les trois de vos interventions, qui ont été très appréciées. Nous allons maintenant passer aux questions des députés.

Madame Kirkland, vous avez la parole pour six minutes.

[*Traduction*]

Rhonda Kirkland (Oshawa, PCC): Merci, monsieur le président.

Je remercie nos témoins de comparaître aujourd'hui. Je vous remercie de votre temps.

Je ne sais pas si vous avez suivi les travaux du Comité sur ce sujet précis, mais à titre de rappel, un représentant d'Affaires mondiales Canada a confirmé, lors d'une réunion précédente du Comité, une chose que j'ai trouvée plutôt préoccupante. J'ai posé la question de façon très générale. Aujourd'hui, on a réitéré que le Comité n'examinera pas une affaire qui fait l'objet d'une enquête en Belgique. Cependant, nous avons appris que si l'on découvre qu'une personne a commis une fraude dans le cadre d'un processus d'embauche fédéral, cette information n'est pas automatiquement signalée lors d'un processus de filtrage de sécurité ultérieur si la personne n'a jamais été embauchée ou n'a jamais obtenu d'habilitation de sécurité.

Nous avons par exemple le cas d'une Canadienne — c'est d'ailleurs la raison pour laquelle nous menons cette étude — qui a commis une fraude lors d'un processus d'embauche du gouvernement fédéral. Elle a obtenu un stage à l'OTAN. C'est ce que nous savons. Nous savons qu'elle fait l'objet de graves accusations d'espionnage en Belgique.

Monsieur Wernick, je vous remercie d'être ici aujourd'hui et d'être disposé à répondre à nos questions. J'espère tirer des enseignements de votre expérience en tant qu'ancien haut fonctionnaire.

Cela vous préoccupe-t-il que l'on puisse découvrir qu'une personne a commis une fraude lors d'un processus d'embauche fédéral, mais que cette information ne parvienne jamais aux responsables chargés de sa prochaine vérification de sécurité?

Michael Wernick: C'est un grave problème. Il s'agit d'une grave faiblesse du processus de filtrage, et cela pose problème pour d'autres aspects liés au personnel. J'ai eu l'occasion d'aborder cette question, par écrit et verbalement, dans d'autres contextes.

Il y a un écart entre le point de vue de la sécurité... Dans le cadre d'une vérification de sécurité, les organismes tendent à se concentrer sur la vulnérabilité au chantage, la vulnérabilité à l'influence étrangère, les liens avec des criminels, la dépendance aux drogues et à l'alcool, les contacts suspects, la famille élargie et les partenaires d'affaires, etc. Ce sont des méthodologies relativement simples qu'utilisent la GRC, le SCRS et les autres organismes.

Cependant, l'un des autres critères, qui est lié à la fiabilité et la loyauté, est la conduite personnelle des fonctionnaires. Cela comprend une multitude de problèmes, notamment l'inconduite, les actes répréhensibles et d'autres comportements qui ne sont pas systématiquement recensés dans l'ensemble de la fonction publique. Je crois savoir que certains de ces problèmes ont été constatés dans certains des cas: fausse déclaration relative aux titres de compétences; conduite inappropriée au travail, harcèlement, intimidation, harcèlement sexuel, tricherie lors d'examens et autres choses du genre.

Il n'y a pas de répertoire unique pour cela. Une personne pourrait échapper aux conséquences en passant d'un ministère ou d'un organisme à un autre. On compte près de 300 organismes fédéraux dans la fonction publique centrale. La liste se trouve dans l'InfoBase du GC.

Je pense qu'il est temps que le Secrétariat du Conseil du Trésor du Canada force la création d'une sorte de répertoire central — j'ignore quel serait le bon terme —, un centre d'information, un lieu où toute l'information relative à... Eh bien, je pense qu'il faudrait probablement diviser cela en deux parties. La partie sécurisée comprendrait les renseignements strictement liés aux vérifications de sécurité et pouvant être communiqués aux agents de sécurité ministériels. L'idée est d'éviter d'inonder l'autre partie, à mon avis, qui contiendrait les renseignements sur les mesures disciplinaires, les manquements prouvés, les conclusions des divers organismes de surveillance, etc.

Les renseignements ne sont pas...

● (1650)

Rhonda Kirkland: Je suis désolée de vous interrompre...

Michael Wernick: ... systématiquement réunis au même endroit, mais ils devraient l'être.

Rhonda Kirkland: D'accord. C'est exactement là où je voulais en venir.

Je suis d'accord. Il n'est pas nécessaire que ce soit tout, mais si une personne commet une fraude, il me semble qu'il devrait y avoir un signalement automatique. Tous les noms que cette personne a utilisés, y compris son vrai nom, devraient se retrouver dans une base de données permettant à tout responsable de l'embauche dans la fonction publique de savoir que cette personne a commis un acte qui n'est certainement pas digne de confiance et qu'elle ne devrait peut-être pas avoir une cote de sécurité assez élevée pour occuper un poste à l'OTAN.

Selon votre expérience, dans ce cas, qui devrait avoir la responsabilité de s'assurer qu'un facteur aussi important qu'une conclusion de fraude reste dans le dossier d'une personne en vue d'un futur processus fédéral d'embauche et de vérification de sécurité? En fin de compte, qui est responsable de veiller à régler ce problème pour l'avenir?

Michael Wernick: Le président du Conseil du Trésor et le Secrétariat du Conseil du Trésor du Canada. Le poste qui se rapproche le plus d'un conseil de gestion ou d'un chef de l'exploitation au gouvernement du Canada — et ce n'est pas entièrement fonctionnel —, c'est celui de président du Conseil du Trésor. Le Conseil du Trésor dispose de tous les outils pour la gestion financière, la gestion des ressources humaines, la gestion de l'information et les politiques linguistiques et, comme vous l'avez vu, c'est lui qui émet la directive sur le filtrage de sécurité.

Rhonda Kirkland: Comment pouvons-nous faire en sorte qu'il...

Michael Wernick: Il a les leviers nécessaires. Vous pourriez notamment recommander que le gouvernement adopte un modèle clair de guichet unique pour le filtrage de sécurité — nous tendons vers ce modèle pour la cybersécurité — et que le président du Conseil du Trésor fasse rapport au Comité, tous les six mois, des mesures prises pour combler les lacunes et éliminer les cloisonnements.

Rhonda Kirkland: Je pense que c'est une excellente idée, mais au bout du compte, le ministère de la Sécurité publique... Le président du Conseil du Trésor, bien sûr... mais, au bout du compte, quel ministre doit veiller à ce que le président du Conseil du Trésor...

Michael Wernick: Le président du Conseil du Trésor est le directeur des opérations...

Le président: Je suis désolé de vous interrompre, monsieur Wernick. Nous posons souvent d'excellentes questions au Comité, mais nous avons rarement le temps d'entendre les excellentes réponses qui devraient y faire suite. Nous y reviendrons peut-être plus tard.

Nous passons maintenant à Mme Sodhi.

Madame Sodhi, vous avez six minutes.

Amandeep Sodhi (Brampton-Centre, Lib.): Merci, monsieur le président, ainsi qu'à nos chers collègues et à tous nos témoins d'être ici aujourd'hui.

J'aimerais commencer par vous, monsieur Leuprecht.

Comme vous le savez, une évaluation de sécurité exhaustive ne se résume pas à recueillir des renseignements auprès d'un demandeur. Les ministères doivent également déterminer si ces renseignements sont complets, exacts et suffisants pour prendre une décision fiable, comme ils le font. Selon vous, y a-t-il des vérifications que le gouvernement devrait renforcer pour que les problèmes potentiels de sécurité soient cernés avant d'accorder une habilitation de sécurité?

● (1655)

Christian Leuprecht: Il est question de deux problèmes distincts ici. Le premier concerne la façon de réagir aux menaces internes. Le cas qui nous occupe constitue sans contredit un problème de menace interne. Il est possible que des candidats soient tout à fait admissibles à la cote de fiabilité, de niveau secret ou de niveau très secret, puis qu'ils adoptent un comportement qui corrompe fondamentalement les conditions de fiabilité liées à leur embauche. Il faut notamment se poser cette question: comment détecter les menaces internes? Puis, demandons-nous: comment détecter les personnes dont le comportement vise manifestement à tromper et à contourner le processus en place pour être embauchées par le gouvernement?

Ce problème ne concerne pas seulement le gouvernement. Aujourd'hui même, j'ai rencontré des représentants de banques canadiennes. Eux non plus ne disposent d'aucun mécanisme efficace pour empêcher un employé qui se livre à un comportement inapproprié de traverser la rue et d'en faire autant comme employé de la banque voisine. Ce problème ne touche pas seulement le gouvernement, mais bien tout le pays.

La Loi sur la protection des renseignements personnels doit faire l'objet d'un examen. Pour nous aider dans les dossiers dont nous discutons, il nous faut un cadre législatif plus solide pour échanger efficacement des renseignements personnels, tant au sein du gouvernement qu'entre les principales organisations canadiennes chargées des infrastructures essentielles.

Par ailleurs, il faut donner suite à ces renseignements. Dans ce cas particulier, le gouvernement et le gestionnaire auraient eu la possibilité de mener une enquête administrative. Si cette enquête administrative avait conclu... à la fraude — l'ancien greffier pourra me corriger si je me trompe —, cela aurait été un motif pour empêcher cette personne d'être employée de la fonction publique fédérale.

À la lumière de ces faits, j'ai l'impression que le gestionnaire n'a pas utilisé les outils à sa disposition dans leur pleine mesure. Je crois avoir expliqué dans ma déclaration liminaire pourquoi il en est ainsi: on n'incite pas les gestionnaires à agir lorsqu'ils ont ces renseignements, et ils ont tendance à ne pas passer à l'action. Chacun sait à quel point il est plus facile de faire disparaître un problème que d'en assumer la responsabilité.

Amandeep Sodhi: Je vous remercie de votre réponse.

Monsieur Wernick, vous avez déjà proposé de créer un registre unique qui recenserait les constats d'inconduite ou de mauvaise gestion relevés par les organismes de surveillance et qui suivrait les employés d'un ministère à l'autre. Un tel registre pourrait aider à éviter qu'on laisse passer des renseignements importants lorsqu'un employé change de poste.

Concrètement, quelle forme prendrait ce registre et comment le gouvernement pourrait-il s'assurer que les constats pertinents soient adéquatement consignés, vérifiés et pris en compte pendant le processus de filtrage de sécurité?

Michael Wernick: Vous me posez une question qui dépasse mes connaissances technologiques. Il me semble qu'il pourrait s'agir d'un logiciel relativement simple.

Il faudrait également un registre semblable pour les entrepreneurs. Il y a environ 300 000 employés. Cependant — et je pense voir des hochements de tête —, les entrepreneurs et leurs employés représentent un grand risque, puisque leurs services sont retenus pour des approvisionnements très délicats et des infrastructures de défense, notamment.

Il me semble — encore une fois, je ne suis pas un expert — qu'un tel registre serait un projet parfait pour l'IA, capable d'examiner de grandes bases de données, de faire des signalements et de dégager des tendances et des liens.

Nous devons rattraper notre retard en matière de reddition de comptes de base. Le gouvernement devrait publier au moins une fois par année un rapport sur le processus d'habilitation de sécurité du personnel et des entrepreneurs qui rendrait compte du nombre de demandes, des niveaux, des délais et des organisations. C'est le mécanisme fondamental par lequel assurer une reddition de comptes. Le modèle n'est pas parfait.

Les administrateurs généraux et les dirigeants des organismes sont les piliers du modèle canadien de reddition de comptes. Ils ont beaucoup de pouvoirs, mais ils sont également responsables en vertu d'une quarantaine de lois: la Loi sur la gestion des finances publiques, la Loi fédérale sur la responsabilité et la loi sur les ressources humaines, par exemple. Ils sont guidés et encadrés par les politiques du Conseil du Trésor, et environ 14 organismes de surveillance les chapeautent.

Ce modèle fonctionne la plupart du temps, mais pas toujours. Je pense que, dans les circonstances actuelles, le Conseil du Trésor doit avoir plus de moyens d'intervenir. Il nous faut des façons plus modernes et dignes du XXI^{e} siècle d'échanger des renseignements pour empêcher que des employés malhonnêtes migrent d'un secteur de la fonction publique à un autre.

J'ajouterais également, avant que le président ne m'interrompe, que le problème touche d'autres organismes fédéraux qui sont essentiels à la démocratie. Regardez du côté d'Élections Canada, du réseau des directeurs de scrutin, de l'administration des tribunaux, des employés du Parlement et du personnel de nos agents du Parlement. Notre approche pour le filtrage de sécurité du personnel et des entrepreneurs doit être cohérente, comme elle l'est pour la cybersécurité.

● (1700)

[*Français*]

Le président: Merci beaucoup.

Madame DeBellefeuille, vous avez la parole pour six minutes.

Claude DeBellefeuille (Vallée-du-Haut-Saint-Laurent, BQ): Merci beaucoup, monsieur le président.

Je remercie les témoins d'être présents.

Monsieur Wernick, votre introduction m'a surprise tantôt quand vous nous avez dit que vous ne saviez pas ce que vous faisiez ici et que vous vous demandiez pourquoi nous vous avions invité.

Je suis tombée sur un article paru en août dans le journal *Ottawa Citizen*et dans lequel vous réagissiez au cas de Mme Zhang. Vous avez dit qu'une des raisons pour lesquelles ça ne fonctionnait pas, c'est qu'il y avait un manque de financement chronique depuis longtemps.

Est-ce que vous maintenez cette affirmation, que vous avez faite au mois d'août dans le journal *Ottawa Citizen*?

Michael Wernick: Oui.

Claude DeBellefeuille: D'accord.

Vous parlez de financement, mais on sait que ce n'est pas nécessairement en ajoutant de l'argent qu'on atteint toujours ses objectifs.

Dans votre jargon d'homme extrêmement expérimenté dans la gestion de l'État, qu'est-ce que ça veut dire, du financement supplémentaire? Quel est le réajustement à faire? Qu'est-ce qu'il faudrait ajouter pour que nous puissions avoir de meilleures mesures, être mieux outillés pour effectuer les filtrages de sécurité et éviter ce qui s'est passé cet été?

Michael Wernick: Je pense que ce serait une combinaison du nombre d'employés affectés à cette fonction, de la technologie, soit la plateforme et les logiciels — j'ai mentionné la possibilité d'améliorer ça —, et de la formation. Ce serait une combinaison de ces trois éléments.

Claude DeBellefeuille: Vous êtes un peu d'accord avec M. Leuprecht, qui dit que, dans le fond, ce n'est pas juste une question de processus, mais que c'est aussi une question de volonté politique: si le politique décidait de prendre cette question au sérieux, il y mettrait les ressources nécessaires et ferait tout en son pouvoir pour éviter une telle situation, bien qu'on sache que le risque zéro n'existe pas.

Alors, ce que je comprends, c'est que s'il y avait une volonté politique et un ajout de ressources, et que le problème était vraiment pris au sérieux, peut-être qu'on construirait un processus plus robuste pour contrer l'espionnage dont on fait l'objet. J'ai été surprise de voir que le Canada était le pays le plus infiltré au monde par la Chine. Donc, on a besoin de cette robustesse.

Vous qui avez beaucoup d'expérience, comment pouvez-vous expliquer ce manque de volonté politique d'ajouter des ressources en 2026, compte tenu de tout ce que nous savons maintenant concernant l'espionnage que le Canada subit de la part de la Chine ou d'autres pays?

Michael Wernick: Comme j'ai quitté l'appareil de l'État il y a longtemps, tout ce que je peux dire, c'est que chaque budget, chaque année, est un choix de priorités. Il y aura un autre budget dans quelques semaines, et le ministre des Finances doit faire face à une gamme de pressions tous azimuts, y compris en ce qui concerne le sujet dont nous discutons aujourd'hui.

Claude DeBellefeuille: Je pense que votre témoignage est plus que crédible. Selon ce que vous nous dites, lors du prochain budget, compte tenu des conditions actuelles d'espionnage contre le Canada, on pourrait s'attendre à ce que de meilleures ressources soient données pour le filtrage de sécurité afin qu'il soit plus robuste et qu'il puisse mieux protéger l'appareil gouvernemental, ses sociétés et ses agences.

Michael Wernick: Oui, absolument. C'est une recommandation que ce comité parlementaire pourrait faire à ses collègues dans le gouvernement et au ministre des Finances, qui est dans les dernières semaines de préparation du prochain budget.

Claude DeBellefeuille: Ça pourrait être aussi une recommandation du commissaire à la transparence en matière d'influence étrangère, que nous n'avons pas encore eu le privilège de recevoir à notre comité. Il a peut-être aussi fait cette recommandation au gouvernement.

Vous qui étiez un haut fonctionnaire, vous savez que les employés de la fonction publique sont syndiqués. Ils ont une convention collective. Or j'ai parfois l'impression que les conventions collectives ne permettent pas le partage des données de ressources humaines ou la création d'un registre central de ressources humaines.

Est-ce que vous pouvez m'expliquer si je fais fausse route ou si mes doutes sont fondés?

● (1705)

Michael Wernick: Je ne sais pas s'il y a de tels éléments dans les conventions collectives.

Ce qui compte, c'est la base législative. Or, c'est vous, les députés, qui contrôlez la base législative. En ce qui concerne l'équilibre entre la protection de la vie privée et les besoins de sécurité, c'est votre tâche, comme parlementaires, de trouver le juste équilibre.

Claude DeBellefeuille: Il faut comprendre que la Commission de la fonction publique nous a expliqué qu'il n'était pas si simple de créer un registre, puisqu'il y a non seulement la question des conventions collectives, mais aussi une question de droit à une forme de protection. Par exemple, si une personne fait une fraude, ça peut rester inscrit à son dossier pendant deux ou trois ans, puis ça s'efface.

Jusqu'où pensez-vous qu'on peut aller dans ce registre?

Michael Wernick: Je pense que ce sont des excuses. Les questions d'espionnage et d'ingérence sont assez graves. Il faut agir maintenant et créer quelque chose qui est, évidemment, très sécurisé: on ne veut pas créer une base de données qui pourrait devenir une cible.

Cependant, je pense qu'on peut déterminer des mesures de protection et de recours. On pourrait tout à fait présenter rapidement un projet de loi que ce comité pourrait étudier afin de trouver un équilibre, comme on le fait dans d'autres domaines.

Le président: Merci beaucoup, madame DeBellefeuille.

[*Traduction*]

Monsieur Lloyd, nous vous écoutons.

Dane Lloyd (Parkland, PCC): Merci, monsieur le président.

Je remercie les témoins.

Je vais d'abord m'adresser à M. Wernick. Lorsque vous étiez aux plus hauts échelons de la fonction publique, craigniez-vous que la fonction publique ou les entrepreneurs du gouvernement du Canada soient infiltrés par des éléments du crime organisé ou par des groupes se livrant à de l'ingérence étrangère?

Michael Wernick: C'est toujours une préoccupation générale, et il faut s'assurer que des systèmes de protection et de filtrage sont en place. Je ne me souviens que de quelques cas précis qui sont survenus lorsque j'étais sous-ministre au ministère des Affaires autochtones ou au Conseil privé. On les a traités conformément aux conseils du conseiller à la sécurité nationale et des agents de sécurité ministériels.

Dane Lloyd: Quel processus a permis de porter ces cas à l'attention des autorités?

Michael Wernick: C'était dans le cadre de séances d'information sur le renseignement.

Dane Lloyd: Qui les organisait?

Michael Wernick: Cela dépendait. Chaque ministère compte un agent de sécurité ministériel. Ensuite, lorsque j'étais au Bureau du Conseil privé — mon dernier poste —, c'était le service du renseignement de sécurité nationale... Comment s'appelait-il?

Dane Lloyd: Sans entrer dans les détails de ces dossiers, qu'est-ce qui déclenchait habituellement ces enquêtes?

Michael Wernick: Chaque dossier était différent. C'était habituellement les interactions de la personne avec des gouvernements étrangers, des entités étrangères, qui mettaient la puce à l'oreille. C'est le genre de situations qu'on voyait, si je me souviens bien.

Dane Lloyd: Merci.

Je vais m'adresser à M. Leuprecht. Vous avez parlé d'échec politique. Depuis que je suis député, j'entends des témoins dire qu'il y a un problème, que des éléments du crime organisé infiltrent le gouvernement dans le but de transmettre des renseignements qui pourraient être utiles aux organisations criminelles. Je sais qu'il y a eu des allégations liées au vol de voitures voulant que des numéros d'enregistrement de chauffeurs aient été transmis au crime organisé afin de faciliter le vol de véhicules.

Pouvez-vous nous dire ce que nous devrions surveiller dans la fonction publique?

Christian Leuprecht: Sans vouloir dénigrer mon collègue, je dirai que, pendant son mandat, nous avons connu le fiasco le plus colossal en matière de filtrage de sécurité au pays: l'arrestation du directeur général du renseignement criminel de la GRC, Cameron Ortis, qui a été reconnu coupable d'accusations très graves.

Nous assistons à une tendance où des personnes se livrent à des activités de menace interne, et le gouvernement n'est pas prêt à faire face au problème: les politiques ne sont pas conçues pour y remédier, et on ne confie pas les responsabilités qui s'imposent aux gestionnaires. Si nous ne cherchons pas ces activités, nous ne les trouverons pas.

Le processus en place est le même que l'on voit trop souvent au gouvernement. Les gestionnaires cochent des cases sur une feuille de calcul et se disent: « J'ai coché toutes les cases, alors j'ai bien fait mon travail de gestionnaire parce que j'ai fait preuve de diligence raisonnable. » Je pense que nous devons changer substantiellement la culture institutionnelle, étant donné que le Canada se trouve dans un contexte très instable et qu'il n'a jamais été aussi important de protéger l'intérêt national et la souveraineté nationale contre les éléments malveillants qui cherchent à nous diviser, à nous miner et à nous corrompre.

● (1710)

Dane Lloyd: Merci.

Vous savez, je pense que, à bien des égards, lorsque nous discutons de ces cas, nous cherchons surtout à empêcher les acteurs malveillants d'entrer au gouvernement. Nous voulons ériger de grands murs pour empêcher les auteurs de menaces d'occuper des postes d'influence. Cependant, que fait-on pour les gens qui sont déjà...? Il se peut qu'ils ne soient pas corrompus lors de leur arrivée. Il se peut qu'ils travaillent déjà à certains dossiers et qu'ils se fassent corrompre plus tard. Que pouvons-nous faire pour nous protéger de l'intérieur?

Christian Leuprecht: M. Wernick a fait allusion à ce que nous faisons du côté de la cybersécurité. Dans ce domaine, nous avons depuis longtemps abandonné le modèle du château, c'est-à-dire l'idée que l'érection de grands murs tiendra l'adversaire à l'écart. Nous savons que l'adversaire est à l'intérieur du château, mais il semble que le processus de filtrage de sécurité repose toujours sur l'idée que, d'une manière ou d'une autre, un mur suffisamment haut et imposant tiendra l'adversaire à l'écart.

Je dirais que nous devons adopter exactement la même approche que pour la cybersécurité. Nous devons supposer que suffisamment de preuves indiquent que l'adversaire se trouve à l'intérieur du château. Par conséquent, nous devons nous doter de processus pour cerner les risques, pour remédier à ces risques efficacement et en temps opportun, et pour veiller à ce que l'information et le renseignement soient communiqués efficacement. Le régime actuel nous permet de faire des signalements, mais il ne nous permet pas du tout de transformer ces signalements en renseignements exploitables et de les communiquer à l'ensemble de la fonction publique fédérale.

Dane Lloyd: Pensez-vous que le...

Michael Wernick: Je peux peut-être renchérir sur cette réponse. Je pense que mon commentaire sera utile. Les habilitations ne sont pas des laissez-passer à vie. Elles sont limitées dans le temps. Lorsque les employés changent d'emploi ou accèdent à un emploi dont les exigences relatives à l'information sont différentes...

Dane Lloyd: Merci.

Michael Wernick: ... leurs habilitations peuvent être mises à niveau, réduites ou révoquées.

Dane Lloyd: Oui. Merci. Je comprends.

Je...

Le président: Je suis désolé, monsieur Lloyd.

Dane Lloyd: Il a pris mon temps.

Le président: J'imagine que vous avez bien d'autres points à ajouter. Avec un peu de chance, vous en aurez l'occasion plus tard.

[*Français*]

Madame Dandurand, vous avez la parole pour cinq minutes.

Marianne Dandurand (Compton—Stanstead, Lib.): Merci beaucoup, monsieur le président.

Je remercie les témoins d'être là.

Monsieur Wernick, j'aimerais vous permettre de finir la pensée que vous étiez en train d'exprimer.

Michael Wernick: Laquelle?

Marianne Dandurand: Celle dont vous venez tout juste de parler, à propos du processus.

Michael Wernick: Je voulais juste dire que ce ne sont pas des approbations permanentes. Il faut les renouveler, selon le niveau, tous les cinq ou dix ans. Si on change d'emploi ou si le contexte change de sorte qu'on doit avoir plus d'accès ou moins d'accès à des renseignements secrets, il y a tout un processus d'octroi et de révocation de la cote de sécurité, ainsi que d'augmentation ou de baisse du niveau de sécurité.

Je pense que ce serait une bonne idée que le gouvernement publie, au moins pour un an, les chiffres sur le volume de ces opérations.

[*Traduction*]

Je pense qu'il serait très utile que le gouvernement offre au Comité des parlementaires sur la sécurité nationale et le renseignement, ou CPSNR, une séance d'information classifiée sur le nombre d'habilitations de sécurité qui ont été rejetées, réduites ou révoquées. Les membres du CPSNR auraient un portrait de la tendance. Ils sauraient ainsi quelles vulnérabilités sont susceptibles de fragiliser le système.

[*Français*]

Marianne Dandurand: Merci beaucoup.

Vous avez longtemps travaillé dans la fonction publique. Vous avez aussi été responsable au Conseil du Trésor, qui a la charge en bonne partie…

Michael Wernick: Non.

Marianne Dandurand: Non? Excusez-moi.

Donc, vous avez longtemps travaillé dans la fonction publique, où vous avez eu la charge d'initiatives comme celle-là.

À votre avis, à quel point devrait-on centraliser le processus de filtrage de sécurité? À quel point est-ce que ça devrait être la responsabilité d'une entité centrale plutôt que de chacun des ministères? C'est une discussion que nous avons depuis le début de cette étude. Quelle liberté chaque ministère devrait-il avoir à cet égard?

Michael Wernick: Je pense que ce sera toujours une combinaison des deux. C'est un équilibre. L'expertise en matière d'enquêtes est à la Gendarmerie royale du Canada, au Service canadien du renseignement de sécurité et aux agences de sécurité et du renseignement. Ces organismes ont la formation et la compétence pour faire le filtrage. Cependant, je pense que les dirigeants d'organismes ont une meilleure connaissance du contexte de leur institution. La Garde côtière canadienne est différente d'un laboratoire de science, par exemple. C'est un dialogue entre les deux qui fonctionne bien.

Ce qui manque de temps en temps, c'est un échange ponctuel d'informations. Je pense qu'il faut plus de centralisation et plus de cohérence. Je pense notamment à une base électronique de données qui rassemblerait toutes les organisations fédérales. C'est le temps de le faire.

Il y a un problème dans la fonction publique. C'est une sorte de syndrome « pas dans ma cour ». Les organismes se pensent spéciaux et veulent faire leurs propres affaires. J'ai toujours été en faveur d'un modèle où le centre, surtout le Conseil du Trésor, jouerait un rôle plus directif envers les autres agences et ministères.

● (1715)

Marianne Dandurand: Je suis curieuse de votre avis sur le niveau de responsabilité du gouvernement par rapport à celui de l'administration publique. J'ai l'impression que les grandes directives doivent probablement venir du politique, mais qu'ensuite, les organismes doivent utiliser leur jugement pour les appliquer.

Selon votre perspective, est-ce que les consignes du gouvernement devraient être plus strictes ou est-ce que l'administration est en mesure d'assurer la sécurité avec les règles actuelles?

Michael Wernick: Je ne peux pas commenter en détail. Je sais qu'il y a eu une mise à jour de la politique du Conseil du Trésor il y a deux ans, je pense, et qu'un représentant du Conseil du Trésor a témoigné la semaine passée. On lui a posé cette question.

Je pense que ce genre de politique du Conseil du Trésor fait toujours l'objet d'un processus de révision et de renouvellement. Ces politiques ont une durée de trois, quatre ou cinq ans, puis elles sont renouvelées. Elles découlent de décisions d'un comité du Cabinet. Elles sont très officielles. Ce sont des directives que les autres agences et les autres ministères doivent suivre. Il y a des conséquences si elles ne sont pas suivies.

Le président: Merci beaucoup, madame Dandurand.

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

Claude DeBellefeuille: Merci, monsieur le président.

Monsieur Leuprecht, dans votre allocution, vous avez dit qu'il y avait une culture institutionnelle qui empêchait de dénoncer des faiblesses dans le processus ou d'être à l'affût des signaux qui se manifestent. Qu'est-ce que vous vouliez dire? J'aimerais que vous preniez deux minutes pour nous l'expliquer concrètement.

Christian Leuprecht: Certainement, madame. C'est une très bonne question.

J'aimerais juste apporter une correction au sujet du rapport que vous avez évoqué. Le Canada est le pays du G7 le plus infiltré par la Chine.

En gros, le Canada a une posture assez homéopathique quant à la sécurité nationale, y compris quant aux enjeux de sécurité nationale au sein du gouvernement. Dans le cas qui nous intéresse, on a eu un problème de faiblesse des signaux en particulier. Maintenant, il faut responsabiliser les gestionnaires.

Je vous donne l'exemple du harcèlement sexuel dans la fonction publique. Par exemple, au sein des forces armées, plein de preuves ont démontré que la façon la plus facile de se débarrasser de quelqu'un qui avait eu une conduite inacceptable était de lui trouver un autre poste ou même d'assurer sa promotion afin qu'on n'ait plus ce problème dans son unité. Or, maintenant, les forces armées ont complètement changé d'approche. Les gestionnaires sont dorénavant responsables de la conduite des personnes qui relèvent d'eux. C'est cette approche qu'il faut adopter partout dans la fonction publique.

Le problème, c'est qu'on a créé une culture où les gestionnaires n'assument plus la responsabilité de leur travail ni de leurs employés. Au lieu de prendre des décisions difficiles, ils poussent ces décisions difficiles plus haut dans la chaîne de commandement.

Claude DeBellefeuille: En ce qui concerne la sécurité, dans l'exemple présent, où croyez-vous qu'il y a eu défaillance dans la chaîne des responsabilités?

Christian Leuprecht: À mon avis, il serait intéressant pour le Comité de voir qui, dans la fonction publique, a été tenu responsable de la conduite de la personne qui est à l'origine de la discussion d'aujourd'hui.

J'estime que probablement personne dans la fonction publique n'a vraiment pris la responsabilité du fait que quelqu'un avait effectivement essayé de commettre une fraude. On a plutôt dit que ce n'était pas si grave que ça et on a laissé tomber la question. On l'a fait pour les raisons que j'ai expliquées, à savoir que les politiques de diversité, qui, en principe, sont de bonnes politiques, ont dissuadé les gestionnaires de prendre des mesures contre une jeune femme racisée.

● (1720)

Le président: Merci beaucoup, madame DeBellefeuille.

Monsieur Lloyd, vous avez la parole pour cinq minutes.

[*Traduction*]

Dane Lloyd: Je serai bref.

Ma question s'adresse à M. Leuprecht et à M. Wernick. J'essaie d'être systématique.

Le Service des poursuites pénales du Canada est-il outillé pour juger les affaires de sécurité nationale? A-t-il ce dont il a besoin? A-t-il l'expertise nécessaire?

Enfin, les enquêtes et les procès de sécurité nationale sont-ils trop secrets, ou estimez-vous que ce niveau de secret est justifié, compte tenu de la nature des affaires?

Merci.

Christian Leuprecht: Je pense que nous devons séparer — et l'ancien greffier pourra me corriger sur ce point — les procédures criminelles des procédures disciplinaires. Les gestionnaires disposent d'une foule de mesures disciplinaires, selon le type d'infraction qu'on soupçonne l'employé — motifs raisonnables à l'appui — d'avoir commise, et ces mesures commencent généralement par une enquête. Le type d'enquête dépend de l'infraction soupçonnée et peut se solder, dans le pire des cas, par le congédiement de l'employé.

Les enquêtes permettent de déterminer, au début, s'il y a soupçon de comportement criminel et, à la fin, si ces soupçons sont avérés. Soit l'enquête est confiée à la GRC pour enquête criminelle, avec la participation du SPPC... Nous avons appris des erreurs du passé et nous savons maintenant que nous devons faire appel au SPPC beaucoup plus tôt, mais l'enquête est bien sûr menée par la GRC en coordination avec le SPPC.

L'enquête ne serait pas confiée au SPPC en soi, mais il y a probablement lieu de se demander à quel moment et dans quelles circonstances des enquêtes criminelles doivent être lancées, afin de bien recueillir les preuves. Je crains que, dans le cas dont nous discutons, par exemple, s'il y avait eu des soupçons de comportement criminel, l'enquête n'aurait pas mené à des preuves recevables dans le cadre d'une procédure pénale.

Dane Lloyd: Monsieur Wernick, nous vous écoutons.

Michael Wernick: Je n'ai pas grand-chose à ajouter sur le SPPC. Je sais que leurs ressources sont rajustées lorsque de nouvelles lois s'appliquent. Un autre comité étudie le projet de loi sur l'Agence contre les crimes financiers, qui aura une incidence sur la charge de travail du SPPC. L'organisation discutera donc de ses ressources avec le ministre des Finances.

Je dirais qu'il y a deux problèmes récurrents.

Des entrepreneurs nous ont donné beaucoup de fil à retordre lorsque j'étais sous-ministre des Affaires autochtones et, dans de nombreux cas, nous avons renvoyé des dossiers à la GRC pour qu'elle enquête sur des fraudes potentielles. Il fallait souvent attendre de deux à trois ans avant d'avoir des nouvelles, et la GRC abandonnait souvent l'affaire parce qu'il était tout simplement trop difficile de recueillir quelque preuve que ce soit. Étant donné ces délais, le sous-ministre se demande vraiment ce qu'il doit faire avec l'entrepreneur ou l'employé visé par l'enquête.

Je n'ai pas de solutions à vous proposer pour accélérer les enquêtes. Parfois, elles concluent qu'aucun acte malveillant n'a été commis. Il faut faire preuve de prudence quant aux paramètres établis.

Je voudrais simplement souligner un autre point dont le Comité n'est peut-être pas au courant: si un emploi exige une cote de sécurité de niveau très secret ou de niveau secret, et qu'un employé se voit révoquer cette cote de sécurité, il est, dans les faits, congédié.

Frank Caputo: Merci. Je vais poursuivre dans la même veine.

Monsieur Piedboeuf, pourriez-vous nous dire...? Vous avez dit ne pas pouvoir faire de commentaires parce qu'une enquête est en cours. Quelle enquête est en cours?

[*Français*]

Jean-Claude Piedboeuf: Il s'agit du cas survenu en Belgique.

[*Traduction*]

Frank Caputo: Je comprends que l'enquête en Belgique est en cours, mais qui mène l'enquête qui vous empêche de faire des commentaires?

[*Français*]

Jean-Claude Piedboeuf: C'est la Belgique.

[*Traduction*]

Frank Caputo: D'accord. C'est la Belgique. Aucune enquête n'est menée par votre organisation en ce moment.

Jean-Claude Piedboeuf: Non. Nous ne pouvons pas formuler de commentaires sur une affaire qui fait l'objet d'une enquête en Belgique.

● (1725)

Frank Caputo: Je comprends. Je ne vous demande pas de formuler de commentaires.

Comprenez-moi bien. Je veux savoir si votre agence compte mener une enquête sur une employée visée par des allégations d'espionnage. Ne serait-ce pas normal que votre agence mène sa propre enquête?

[*Français*]

Jean-Claude Piedboeuf: Je ne peux pas commenter la situation.

[*Traduction*]

Michael Wernick: Non. Pas du tout. Dès qu'une affaire est mise entre les mains de la police, on ne peut pas poursuivre sa propre enquête, car on risquerait de nuire à l'enquête policière.

Frank Caputo: Bien respectueusement, je ne demandais pas si quelqu'un avait communiqué avec la police ou entrepris d'autres démarches du même genre. Je demandais au dirigeant de l'Agence spatiale canadienne si une enquête était menée dans son organisation pour déterminer ce qui s'était passé, étant donné qu'une employée est visée par des allégations d'espionnage pour le compte de la Chine.

Une enquête est-elle menée sur ce qui s'est passé à l'Agence spatiale canadienne? Répondez par oui ou par non s'il vous plaît.

[*Français*]

Jean-Claude Piedboeuf: Malheureusement, je ne peux pas commenter la situation parce qu'elle fait l'objet d'une enquête.

[*Traduction*]

Frank Caputo: Aucune enquête n'est menée, mais...

Le président: Je suis désolé, monsieur Caputo. Je n'aime pas vous interrompre, mais nous devons passer à M. Powlowski pour cinq minutes.

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): Loin de moi l'envie de défendre la bureaucratie. J'ai souvent été critique envers notre propre bureaucratie, mais puisque vous avez tenu des propos incendiaires à ce sujet, je me demandais si vous pouviez les étayer.

Corrigez-moi si je me trompe — je prenais des notes lorsque vous avez prononcé ces mots —, mais vous avez indiqué qu'entre 2015 et 2024, la taille de la fonction publique avait augmenté de 40 %. Vous avez dit qu'il était « peu probable » que pour bon nombre de fonctionnaires, un filtrage de sécurité ait été effectué. Avez-vous des preuves pour étayer vos dires?

La deuxième chose que vous avez dite — corrigez-moi si je vous cite mal — est que la bureaucratie avait « sciemment exposé » le pays à un risque. Voilà une autre déclaration très sévère. Vous avez employé le terme « sciemment ». Avez-vous des preuves que les fonctionnaires ont exposé en connaissance de cause le pays à un risque?

Christian Leuprecht: Je vais commencer, si vous me le permettez, en parlant de mon collègue de l'Agence spatiale canadienne. Le cas dont nous sommes saisis est le deuxième à survenir à l'Agence spatiale canadienne.

Je dois admettre que M. Wanping Zheng a été reconnu non coupable. Je vois se dessiner, dans cet exemple même, une tendance qui se rattache en toute apparence à la menace interne.

Marcus Powlowski: Attendez. Un seul cas ne constitue pas une tendance. C'est un exemple, je suppose, mais ce n'est pas forcément...

Christian Leuprecht: C'est pour cette raison que j'ai fait remarquer qu'au moins un deuxième cas avait été signalé ces dernières années.

Ce que je soulignais dans ma déclaration était que le filtrage de sécurité n'avait pas été mené à un niveau approprié et proportionnel au risque, comme cela aurait été nécessaire. J'en déduis que l'expansion de la fonction publique n'a pas été proportionnelle aux ressources allouées aux organismes chargés de mener une évaluation plus approfondie lorsque des cas déclenchent des signaux d'alarme.

Je n'ai pas dit que des filtrages de sécurité n'avaient pas été faits. J'ai mentionné que les ressources n'étaient pas proportionnées.

Je n'ai pas dit que la bureaucratie avait « sciemment exposé » le pays au risque. Vous consulterez ma déclaration écrite, que j'ai remise au greffier. J'ai dit que la décision politique avait été prise de ne pas allouer les ressources qui auraient été appropriées étant donné l'augmentation de la taille de la fonction publique et les vulnérabilités bien connues du Canada, particulièrement par rapport à un acteur adverse très agressif et doté de capacités avancées qu'est la Chine.

Marcus Powlowski: Vous niez avoir dit que la bureaucratie avait « sciemment exposé » le pays à des risques. Vous rétractez-vous?

Christian Leuprecht: Vous avez ma déclaration écrite sous les yeux, et je l'ai lue.

Je pourrais retrouver le passage en question, mais je disais en substance que des décisions politiques avaient sciemment exposé la fonction publique à un risque. Les ressources en sécurité qui ont été allouées n'étaient pas suffisantes pour effectuer le filtrage de sécurité des nouveaux fonctionnaires qui ont augmenté les effectifs de 50 %, y compris les vérifications plus poussées que nécessitent certains cas.

Je peux affirmer avec un degré de certitude raisonnablement élevé que dans certains cas, des décisions ont été prises précipitamment, étant donné l'augmentation de la taille de la fonction publique.

Je répète depuis des années que le Canada, dans la fonction publique fédérale et à l'échelle du pays, fait preuve de mollesse concernant la sécurité nationale. Les nombreux rapports que je cite dans ma déclaration en témoignent, notamment en ce qui concerne la Chine.

● (1730)

Marcus Powlowski: D'accord. Je vais vous demander de clarifier un autre point.

Corrigez-moi au besoin, mais vous avez dit à propos de Mme Zhang que le fait de ne pas avoir signalé la vulnérabilité d'une « jeune femme racisée » constituait une faille de sécurité. Affirmez-vous ou sous-entendez-vous que les personnes issues des minorités visibles sont plus susceptibles de commettre un acte de trahison et qu'elles devraient faire l'objet de vérifications plus approfondies?

Christian Leuprecht: Ce n'est pas ce que j'ai dit et ce n'est pas ce qu'il faut déduire de mes propos.

J'ai souligné que dans un gouvernement fédéral qui accorde visiblement la priorité aux politiques de diversité, les gestionnaires — surtout s'ils sont jeunes — qui signalent une personne doivent arriver avec une preuve béton et se préparer à de forts vents de face.

Ce que je dis, c'est que nous devons créer un environnement où même les signaux faibles sont pris au sérieux et que les gestionnaires devraient être en mesure de les rapporter sans craindre de représailles lorsque la personne visée par ces signaux se trouve à être une personne favorisée par les priorités et les politiques du gouvernement.

Marcus Powlowski: L'appartenance à une minorité est-elle un faible signal de risque?

Le président: Je suis désolé, monsieur Powlowski. Je déteste vous interrompre, mais votre temps est écoulé.

[*Français*]

C'est le moment de remercier les trois témoins d'avoir pris le temps d'être avec nous, d'avoir fait l'effort de se préparer et d'avoir été présents à la réunion d'aujourd'hui.

Messieurs Leuprecht, Wernick et Piedboeuf, nous vous exprimons notre gratitude et nous espérons que vous avez passé une bonne fin de journée.

Je m'adresse maintenant aux membres du Comité. Nous allons suspendre la séance pendant cinq minutes avant de reprendre avec trois autres témoins.

Merci.

● (1730)

_____(Pause)_____

● (1735)

Le président: Nous reprenons la séance.

Je vous remercie de revenir pour la deuxième heure de cette réunion, pour laquelle nous avons trois témoins.

Nous accueillons à titre personnel M. Wesley Wark, chercheur principal au Centre pour l'innovation dans la gouvernance internationale. De Cinchy Incorporated, nous accueillons J. Paul Haynes, président-directeur général. Enfin, du Bureau du Conseil privé, nous accueillons David Morrison, conseiller principal en affaires diplomatiques et internationales auprès du premier ministre.

Vous avez chacun cinq minutes pour faire votre intervention.

Nous allons commencer par M. Wark.

● (1740)

[*Traduction*]

Wesley Wark (chercheur principal, Centre for International Governance Innovation, à titre personnel): Monsieur le président, mesdames et messieurs, merci de m'avoir invité à témoigner dans le cadre de votre étude sur le processus de contrôle de sécurité au Canada.

Je vais traiter du sujet sous un autre angle et susciter peut-être chez vous des craintes différentes de celles qui ont été soulevées dans les témoignages précédents. Je vais commencer par quelques éléments factuels.

Tout d'abord, le processus de contrôle de sécurité du gouvernement du Canada est décrit en détail dans une directive relativement récente sur le filtrage de sécurité, qui est entrée en vigueur le 6 janvier 2025. Le deuxième point est que le SCRS s'acquitte de la majeure partie du fardeau du filtrage de sécurité pour le gouvernement du Canada. Je reviendrai plus tard sur ce point. Affaires mondiales Canada joue un rôle secondaire dans la conduite des contrôles de sécurité du personnel embauché sur place et des représentants d'autres gouvernements faisant partie des missions canadiennes à l'étranger. Le filtrage de sécurité du SCRS repose en substance sur l'évaluation de la « loyauté des personnes envers le Canada et, dans la mesure où elle s'y rapporte, leur fiabilité. »

À propos de la finalité de l'évaluation du filtrage de sécurité du SCRS, je cite un passage de la directive du Conseil du Trésor:

> Évaluer, lorsque les renseignements disponibles sont suffisants, s'il existe des motifs raisonnables de croire que la personne s'est livrée, se livre ou pourrait se livrer à des activités qui constituent une « menace envers la sécurité du Canada » au sens de l'article 2 de la Loi sur le Service canadien du renseignement de sécurité [...]

Le troisième point que je veux soulever est que le SCRS est responsable de la prestation de conseils dans deux volets distincts du contrôle de sécurité. L'un concerne les dossiers d'immigration signalés par Immigration, Citoyenneté et Réfugiés Canada, par l'Agence des services frontaliers du Canada, ou par les deux. L'autre porte sur l'octroi de cotes de sécurité par le gouvernement du Canada à différents niveaux d'accès à l'information.

Le SCRS fournit des avis sur le filtrage de sécurité conformément aux critères que j'ai mentionnés. Ce sont des avis discrétionnaires fondés sur les informations à sa disposition. Comme l'a mentionné M. Wernick, le refus d'une cote de sécurité a de graves répercussions pour le demandeur. Cette décision entraîne essentiellement un congédiement. La personne concernée peut toutefois déposer une plainte, qui sera traitée par l'Office de surveillance des activités en matière de sécurité nationale et de renseignement.

Ces avis de filtrage de sécurité, qui sont toujours discrétionnaires, peuvent être influencés par des informations incomplètes ou par une gestion inadéquate des données. Il est toujours difficile, voire impossible, de déterminer si une personne pourrait constituer une menace interne en prédisant son comportement futur.

L'affaire à l'origine de l'étude du Comité peut constituer ou non un cas d'espionnage. Je ne me prononcerai pas avant la fin de la procédure judiciaire en Belgique. Une arrestation a eu lieu, et l'affaire est devant les tribunaux belges, comme vous le savez. D'ailleurs, l'accès à certains documents clés compliquera sans doute l'étude du Comité.

Je veux élargir la perspective au-delà de ce cas précis et dire au Comité que le système actuel de filtrage de sécurité au Canada n'est tout simplement pas viable. Le double fardeau de l'évaluation des demandes d'immigration et du filtrage de sécurité est trop lourd pour le SCRS. De mon point de vue, cette structure risque de nuire à l'efficacité opérationnelle du SCRS dans le cadre de ses missions principales. Les services de renseignement ne devraient pas être des centres de filtrage de sécurité.

Examinons les statistiques. En 2025, selon le *Rapport public du SCRS*, le service aurait reçu 129 130 demandes dans le cadre du programme de filtrage de sécurité du gouvernement et 438 600 demandes de contrôle d'immigration et de sécurité. Au total, le service reçoit 567 730 demandes — 1 555 demandes par jour, en supposant qu'elles arrivent de manière ordonnée, ce qui n'est évidemment pas le cas. Noyées dans cette montagne de demandes se trouvaient 360 demandes de ce qui s'appelle le « filtrage pour d'autres pays », qui désigne les « évaluations de sécurité fournies à des gouvernements étrangers ainsi qu'à des organisations internationales lorsque des Canadiens souhaitent obtenir un emploi qui nécessite une autorisation d'accès à des informations ou à des sites sensibles dans un autre pays. » Malgré ces chiffres relativement modestes, le rapport du SCRS indique un arriéré causé par l'incapacité du service à les traiter.

Un autre modèle est déjà en place au sein du gouvernement d'un de nos alliés, le Royaume-Uni, qui s'est doté d'un organisme distinct et centralisé responsable des cotes de sécurité — les Britanniques emploient le terme « security vetting » — qui dessert tous les ministères. Ce modèle a été établi en 2017. Il relève depuis 2020 du bureau du conseil des ministres, et non pas du MI5 ou du MI6 ou d'un organisme de sécurité.

À mon avis — et c'est ce que je suggérerais au Comité d'examiner —, le Canada devrait étudier et adopter le modèle britannique, et créer un organisme distinct et centralisé qui se chargerait du filtrage de sécurité et qui délesterait de cette lourde responsabilité les organismes de renseignement.

● (1745)

Une restructuration fondamentale comme celle-là permettrait également, à mon avis, de mettre en place des processus plus cohérents et d'améliorer la gestion des données.

Si nous nous en tenons au modèle actuel, le recours à l'IA et à des consultants externes s'accroîtra et le SCRS restera aux prises avec un fardeau dont il est impossible de s'acquitter. Laquelle des deux options préférez-vous?

Merci.

[*Français*]

Le président: Merci beaucoup, monsieur Wark.

Monsieur Haynes, vous avez la parole pour cinq minutes.

[*Traduction*]

J. Paul Haynes (président-directeur général, Cinchy Inc.): Merci, monsieur le président.

Merci, mesdames et messieurs.

Je m'appelle J. Paul Haynes. Mon entreprise, Cinchy, fournit des solutions de sécurité dans le domaine de l'IA. J'ai accumulé avant Cinchy de nombreuses années d'expérience dans la cybersécurité de première ligne au sein d'une organisation qui est probablement une des plus grandes au pays dans le secteur privé. Je me sens donc un peu comme un poisson sorti de son bocal, mais j'espère que mes observations vous seront utiles.

Je ne vais pas entrer dans les détails du cas survenu en Belgique. Je vais plutôt traiter du système et des méthodes qui ont fait leurs preuves dans le secteur privé. Il y a quelques points clés, dont certains ont déjà été mentionnés.

Le système est solide, mais il est statique. La durée des cotes de sécurité, de 5 ans ou de 10 ans, sans vérifications dans l'intervalle, ne correspond pas aux façons de faire dans le secteur privé. Quiconque accède à des dossiers financiers ou en assure la sécurité dans les banques, aux États-Unis ou ailleurs, fait l'objet de vérifications de solvabilité et de casier judiciaire chaque année. Les gens modifient leur comportement s'ils ont un problème de solvabilité, par exemple. C'est la raison principale pour laquelle nous avons cette façon de faire.

Le point suivant est la notion de « faire confiance, mais vérifier », que j'ai appliquée dans le secteur privé. Selon ce principe, lorsqu'il est nécessaire de resserrer la surveillance à l'égard de quelqu'un, on ne peut pas cibler uniquement la personne. Il faut faire confiance, mais vérifier tous les membres de l'équipe, ce qui va à l'encontre du procédé qui consiste à repérer les signaux, puis à mener une enquête sur les signaux en question. Du point de vue des droits de la personne, les équipes de RH du secteur privé nous incitent à cibler tout le monde, et non pas une personne en particulier. Faire confiance et vérifier... C'est facile à dire, mais assez difficile à mettre en pratique.

Les systèmes de signalement utilisés par les équipes de cybersécurité pour repérer des comportements humains, la synchronisation des vérifications et la conciliation de la gestion du personnel et de la cybersécurité, comme d'autres témoins l'ont mentionné, je crois, ces choses doivent être coordonnées.

De plus, les informations existent, mais elles ne sont pas en orbite. C'est quelque chose que j'ai relevé nombre de fois au gouvernement. Nous avons pensé qu'un document d'intégrité transférable qui servirait de passeport aux titulaires d'une cote de sécurité renouvelable pourrait être mis en œuvre — par voie électronique, bien sûr — afin que ces données importantes parviennent aux gestionnaires d'embauche des nouveaux organismes où seront transférés les fonctionnaires.

Quant à la protection de la vie privée, il faut trouver le juste équilibre, et non pas la maximiser. Au cours d'une opération en Irlande, nous avons vu des situations où les règles de protection de la vie privée étaient tellement strictes qu'il était impossible d'obliger les employés à se soumettre à une vérification de solvabilité et de casier judiciaire, exception faite de ceux qui travaillent avec des personnes vulnérables ou des enfants, ou dans un service de police. L'Irlande s'est ainsi privée d'importantes occasions économiques dans l'aérospatiale et d'autres secteurs de la sécurité. Il faut trouver le juste équilibre.

L'autre difficulté qui a été soulevée aujourd'hui, que je vais formuler autrement, est le caractère limité des antécédents vérifiables des nouveaux Canadiens. Pour certains d'entre eux, il est impossible d'obtenir 10 ans d'antécédents, même si leur profil est idéal pour un poste donné. À quel point peut-on faire confiance à un organisme gouvernemental étranger, surtout s'il n'a pas nécessairement intérêt à fournir un portrait complet du demandeur ou à aider le Canada? Ce sont des défis intéressants à relever. Comme je le disais, il faut évaluer le niveau de risque et mettre en place des mesures d'atténuation proportionnelles.

Les recommandations que je formulerais — dont j'ai déjà fourni un avant-goût — seraient de mettre en place une évaluation continue, comme le font les banques. Cette méthode est éprouvée. Elle ne règle pas tous les problèmes, mais elle n'est pas très coûteuse ni compliquée à mettre en œuvre. De nombreuses entreprises privées l'appliquent. Je suis certain que le gouvernement possède lui aussi les capacités nécessaires pour le faire.

Un dossier d'intégrité partagé qui ferait le lien entre les rôles de la Commission de la fonction publique, de l'Agence des services frontaliers du Canada et de la Gendarmerie royale du Canada contribuerait grandement à accélérer le processus et à procurer un portrait complet des demandeurs. Si cette structure est en place dans le secteur privé, je ne vois pas pourquoi elle ne pourrait pas l'être dans la fonction publique fédérale.

Quant à la connexion entre le risque interne et la sécurité des TI, le pire scénario à éviter est une histoire à la Snowden. C'est ce qui nous vient à l'esprit et c'est ce dont nous parlons aujourd'hui. Edward Snowden était un consultant de la compagnie Booz Allen. Il avait un accès étendu aux systèmes. Des choses comme le téléchargement massif de données auquel s'est livré M. Snowden seraient signalées si elles étaient décelées. Il faut relever ce type de comportement et exercer une surveillance supplémentaire des consultants externes similaires au cas dont nous parlons.

● (1750)

Je peux conclure là-dessus. Le système canadien a été conçu de manière à vérifier la fiabilité une seule fois et la tenir pour acquise par la suite, mais vous savez ce qui se passe lorsque l'on tient quelque chose pour acquis. C'est en associant la sécurité du personnel et la cybersécurité que l'on obtiendra les meilleurs résultats.

Je serai heureux de répondre à vos questions.

Merci, monsieur le président.

[*Français*]

Le président: Merci beaucoup, monsieur Haynes.

Monsieur Morrison, la parole est à vous pour cinq minutes.

[*Traduction*]

David Morrison (conseiller principal en affaires diplomatiques et internationales auprès du premier ministre, Bureau du Conseil privé): Monsieur le président, mesdames et messieurs les membres du Comité, je vous remercie de me donner l'occasion de m'adresser à vous aujourd'hui.

En tant que conseiller principal en affaires diplomatiques et internationales auprès du premier ministre, je co-dirige la Direction générale de la sécurité nationale, du renseignement et des affaires internationales au Bureau du Conseil privé. Au sein du Bureau du Conseil privé, ma direction fournit un soutien stratégique au premier ministre, au greffier du Conseil privé, aux ministres et aux ministères sur les questions relatives aux affaires étrangères, à la politique de défense, à la sécurité nationale et au renseignement, et nous contribuons à la coordination de tous ces domaines dans l'ensemble du gouvernement.

Comme vous le savez sans doute d'après les témoignages précédents, au Canada, notre système prévoit que chaque ministère est responsable de la décision d'accorder des habilitations de sécurité en fonction d'exigences communes et en s'appuyant sur une expertise centralisée. Le Secrétariat du Conseil du Trésor établit le cadre stratégique. Le portefeuille de la sécurité publique, par l'entremise de la GRC et du SCRS, s'occupe des vérifications de casier judiciaire et des évaluations relatives à la sécurité nationale. Enfin, chaque ministère recueille les renseignements pertinents, évalue les risques et décide d'accorder ou non une habilitation de sécurité en vertu des pouvoirs qui lui sont délégués, les administrateurs généraux demeurant responsables de l'intégrité de ces programmes au sein de leur organisation.

[*Français*]

Les allégations visant une citoyenne canadienne employée par l'Organisation du Traité de l'Atlantique Nord ont naturellement soulevé des questions sur le régime de sécurité du personnel du Canada et les enseignements qui peuvent en être tirés.

Alors que les autorités belges continuent de diriger l'enquête criminelle et que le Canada poursuit sa pleine coopération à ce processus, les ministères concernés ont mené des examens et formulé des recommandations visant d'éventuelles améliorations au cadre de sécurité du personnel.

Ayant occupé les fonctions de sous-ministre des Affaires étrangères au moment où l'habilitation de sécurité en question a été accordée, je souligne qu'Affaires mondiales Canada a indiqué au Comité que son examen n'avait relevé aucun manquement aux politiques ou aux procédures alors en vigueur.

Cela étant dit, cette affaire met en lumière l'importance de s'assurer continuellement que les décideurs disposent de l'information, des outils, des mécanismes de gouvernance et des garanties nécessaires pour prendre les meilleures décisions possibles en matière de sécurité dans un environnement de menaces en constante évolution.

[*Traduction*]

Le ministre de la Sécurité publique vous a dit qu'il avait demandé aux ministères d'examiner l'affaire pour laquelle nous sommes tous ici et de proposer des améliorations au processus. Dans le même esprit, et compte tenu de mon rôle au Conseil privé consistant à soutenir la coordination de la sécurité nationale, du renseignement et des affaires internationales, j'aimerais formuler quelques observations qui, je l'espère, vous seront utiles dans le cadre de votre étude.

Premièrement, un répertoire ou un registre pangouvernemental regroupant les renseignements relatifs aux habilitations de sécurité permettrait d'améliorer l'efficacité du système, de réduire les dédoublements et d'aider les ministères à localiser les renseignements pertinents sur la sécurité du personnel qui pourraient déjà exister.

Deuxièmement, les renseignements relatifs aux ressources humaines qui sont utiles pour évaluer la fiabilité ou la loyauté d'une personne devraient être mis à la disposition des responsables devant prendre les décisions en matière de sécurité du personnel sans toutefois compromettre la protection des renseignements personnels ni l'équité procédurale.

Troisièmement, la vérification des sources ouvertes devrait être utilisée de manière plus systématique dans l'ensemble du gouvernement pour un plus large éventail de niveaux d'habilitation de sécurité. Elle pourrait également bénéficier de normes en matière de formation, de méthodologies et d'outils communs à tous les ministères.

Quatrièmement, un programme rigoureux de sécurité du personnel devrait s'appliquer à toute la durée de l'emploi d'une personne par l'entremise de programmes de gestion des risques internes, de l'assurance continue de la sécurité du personnel, de contrôles périodiques, d'obligations en matière de déclaration et de mesures de sensibilisation à la sécurité, comme l'a indiqué le témoin qui m'a précédé. Ces mesures contribueraient à cerner les nouveaux risques, à garantir que les titulaires d'habilitations de sécurité restent fiables et loyaux et à faire en sorte que les habilitations de sécurité reflètent les renseignements à jour.

Enfin, je suis au courant des propositions qui ont été faites au Comité selon lesquelles le SCRS — voire le ministre de la Sécurité publique — devrait avoir le dernier mot lorsque les dossiers sont complexes. Je pense que ce serait une erreur. Dans notre système de Westminster, la responsabilité des décisions relatives au personnel incombe à l'administrateur général. C'est ainsi que le système a été conçu et ce principe a été codifié dans la Loi sur la gestion des finances publiques.

● (1755)

J'ajouterais, aux fins du compte rendu, qu'en près de six ans en tant que sous-ministre à Affaires mondiales et bientôt près de quatre ans au Bureau du Conseil privé — dans le cadre de deux mandats différents —, je n'ai pas entendu parler d'un seul cas où une habilitation de sécurité aurait été accordée alors que des doutes subsistaient quant à la loyauté ou la fiabilité d'un fonctionnaire.

Les sous-ministres travaillent en collaboration avec les services de sécurité. Lorsqu'un cas est complexe, je suis convaincu que l'habilitation serait soit refusée soit, dans un cas extrême, accordée sous réserve de mesures d'atténuation convenues avec les services de sécurité.

Aujourd'hui, je ne peux pas me prononcer sur des cas particuliers. Je serai toutefois heureux de discuter du cadre général de sécurité du personnel, des questions touchant la gouvernance et des efforts déployés pour renforcer le système canadien de sécurité du personnel.

Merci. Je suis prêt à répondre à vos questions.

[*Français*]

Le président: Merci beaucoup, monsieur Morrison.

Cela nous permet de passer à Mme Kirkland pour six minutes.

Pardonnez-moi, c'est en fait au tour de M. Caputo.

[*Traduction*]

Frank Caputo: Merci beaucoup, monsieur le président.

Je remercie les témoins de comparaître au sujet de cette question très importante.

Par votre entremise, monsieur le président, je vais adresser mes questions à M. Morrison.

L'affaire Zhang a montré et montre encore l'inefficacité de notre système de renseignement. N'est-ce pas?

David Morrison: Je ne peux pas me prononcer sur un cas particulier.

Frank Caputo: D'accord. Examinons la question de façon générale. Nous pourrons ensuite passer à des hypothèses.

Je pense que vous pourriez nous donner votre avis, monsieur, sur cette situation: si une personne se rendait dans un pays étranger au nom du Canada parce que celui-ci lui avait donné une habilitation de sécurité, mais qu'au moment où elle a obtenu cette habilitation de sécurité, elle avait des antécédents de fraude documentés au Canada, nous serions devant un échec en matière de renseignement, n'est-ce pas?

David Morrison: Je dirais que, dans cette situation hypothétique, toutes les règles et tous les protocoles applicables à l'époque auraient pu être respectés. Cela dit, les systèmes peuvent toujours être renforcés.

En théorie, même si les renseignements dont disposent les décideurs étaient traités de manière appropriée et que les décisions étaient prises comme il se doit, nous pourrions faire face à des résultats imprévus. C'est pourquoi je dis que certains systèmes peuvent être améliorés et que j'ai suggéré quatre façons de le faire.

Frank Caputo: J'en suis conscient. Ce que je dis, c'est que lorsque nous sommes confrontés à des situations où il y a des antécédents de fraude documentés, pour moi, le débat est clos, car la fraude est une infraction qui touche à l'intégrité. C'est une infraction qui en dit long sur votre personne. On ne commet pas une fraude sur un coup de tête. Je sais que vous ne pouvez pas vous prononcer sur un cas précis, mais il reste que le Canada a octroyé une habilitation de sécurité à une personne qui avait commis une fraude.

Je vais vous dire ceci. Nous avons la chance d'avoir une stagiaire dans notre bureau. Elle est stagiaire depuis deux semaines et elle a réussi à trouver la décision de la Cour fédérale concernant l'affaire Zhang. Comme elle me l'a fait remarquer, avant de rencontrer une personne pour la première fois, on se renseigne sur cette personne. On fait une recherche sur Google pour trouver ce genre de renseignement et je pense qu'on le trouve.

Je vais répéter ce que j'ai dit. Le fait de donner une habilitation de sécurité — une habilitation de sécurité de niveau élevé, en l'occurrence — alors que des renseignements de ce genre sont accessibles au public témoigne de failles dans le domaine du renseignement. Avez-vous quelque chose à dire à ce sujet?

● (1800)

David Morrison: Mon commentaire fait écho à celui de mon ancienne collègue, Mme Tara Denham, qui, si je me souviens bien, a témoigné ici le 7 octobre. Elle a expliqué aux membres du Comité comment Affaires mondiales Canada interviendrait dans une telle affaire. Je crois que Mme Denham a également déclaré que, même si cela n'était pas nécessaire au moment où l'habilitation a été accordée — ainsi, tous les protocoles avaient été respectés —, Affaires mondiales Canada effectuerait désormais, pour tout cas similaire, une recherche dans des sources ouvertes.

Frank Caputo: Je l'espère bien. Je pense que la question de la recherche dans des sources ouvertes représente à elle seule une défaillance sur le plan de la sécurité. Lorsque j'étais procureur, nos services de sécurité avaient effectué une recherche dans des sources ouvertes à mon sujet, simplement pour s'assurer de ma sécurité, et on parle ici d'une personne qui représente le Canada.

En somme, le Canada a accordé une habilitation de sécurité à une espionne présumée. Ce n'est pas le Canada, mais bien la Belgique qui l'a découvert. Tout à l'heure, un témoin nous a dit que le Canada est le pays le plus infiltré au monde par des agents étrangers. On savait qu'il y avait eu fraude. Malgré la constatation de fraude et la décision rendue à ce sujet, comme l'a confirmé une révision judiciaire, Mme Zhang a continué à travailler pour Emploi et Développement social Canada.

Un journal français a qualifié cette situation de honteuse pour le Canada. Cela ne nuit-il pas à notre réputation sur la scène internationale, auprès de nos alliés du Groupe des cinq et du G7?

David Morrison: Je tiens à préciser que je suis d'accord avec l'honorable député au sujet de l'utilisation des sources ouvertes... Google, ou peu importe comment vous voulez appeler cela. Je pense que cela devrait faire partie intégrante de notre processus de vérification.

Je suis également d'accord — et j'ai tenté de le dire dans ma déclaration — pour affirmer que les renseignements personnels relatifs à l'intégrité d'une personne devraient faire partie du système. Ce n'était pas le cas à l'époque, mais selon mes collègues d'Affaires mondiales Canada, cette situation a depuis été rectifiée...

Frank Caputo: Je ne veux pas vous interrompre, mais il ne nous reste que 40 secondes.

Je me suis trompé lorsque j'ai dit que le Canada était le pays le plus infiltré au monde par des agents étrangers. J'aurais plutôt dû dire qu'il était le pays le plus infiltré du G7.

Vous avez comparu en comité en 2023 en raison de l'ingérence étrangère. Vous êtes très au fait de ce phénomène. Mon collègue Michael Cooper vous a posé des questions au sujet de l'ingérence étrangère en lien avec M. Chong et un rapport qui n'avait pas été transmis. Vous avez déclaré: « Il y a l'ingérence étrangère. Nous avons ce que la stratégie indo-pacifique appelle — je n'ai peut-être pas le libellé exact — une Chine de plus en plus affirmée. »

Les gens étaient au courant de cette situation, mais quelqu'un a réussi à s'infiltrer jusqu'au plus haut niveau. Comment ne peut-on pas parler d'un échec colossal de nos services de renseignement?

Le président: Veuillez répondre très brièvement.

David Morrison: Je crois avoir essayé de répondre à cette question. Tous les protocoles et procédures qui s'imposent ont été suivis.

Dans le cas hypothétique auquel j'essaie de répondre, si tous les protocoles sont respectés, mais que nous aboutissons à un résultat imprévu, cela démontre clairement que les protocoles doivent être renforcés. C'est dans cet esprit que je me présente devant votre comité aujourd'hui. Je veux vous offrir des suggestions sur la façon d'apporter des améliorations.

Le président: Merci, monsieur Caputo.

[*Français*]

Monsieur Ramsay, vous avez la parole pour six minutes.

Jacques Ramsay (La Prairie—Atateken, Lib.): Je remercie les trois témoins.

Si on me le permet, je vais commencer par une note un peu philosophique: je pense qu'il faut reconnaître que notre système fonctionne très bien dans plus de 99 % et que les cas que l'on analyse aujourd'hui sont plutôt rares. Cela dit, je suis le premier à vouloir améliorer le système. Nous avons quelques suggestions de la part des témoins aujourd'hui. En effet, je pense qu'il faut améliorer le système, mais il faut quand même se méfier afin de ne pas créer un monstre bureaucratique. On sait que 500 000 vérifications sont faites chaque année au Canada, dont près de 130 000 pour la fonction publique et 400 000 pour l'immigration.

Monsieur Wark, vous nous avez dit que la solution pour vous est le modèle anglais qui sépare deux entités. En tout respect, je pense que c'est un peu cosmétique. Ce n'est pas de créer une autre agence. Ça pourrait être ça, mais ce n'est pas si simple que ça de créer une autre agence qui, de fait, va se priver des connaissances du Service canadien du renseignement de sécurité, qui est capable d'apporter une contribution.

Monsieur Haynes, vous nous avez suggéré certaines mesures. Vous nous avez quand même dit qu'il y avait des nuances pour ce qui est de la confidentialité et du respect de la vie privée. Vous nous avez parlé du modèle américain.

Dans le fond, ma question à vous deux, messieurs Wark et Haynes, est la suivante: comment fait-on pour avoir un système efficace qui améliore ce qu'on fait déjà, sans créer un monstre bureaucratique, avec une surveillance qui va demander des ressources incroyables? Il faut toujours se rappeler que notre système est particulièrement efficace et qu'il échoue que dans de rares cas.

● (1805)

[*Traduction*]

Wesley Wark: Brièvement, je dirais que personne au sein du système de renseignement du Royaume-Uni ne pense avoir créé un monstre bureaucratique en mettant en place une agence centralisée et spécialisée. Je pense qu'on estime plutôt avoir fait le contraire.

Ce que j'essaie de vous faire comprendre, c'est ceci: voulez-vous vraiment un service de renseignement chargé d'examiner un large éventail de menaces, tant à l'échelle mondiale qu'à l'échelle nationale, qui est enlisé dans une bureaucratie monstrueuse à cause de ses activités de filtrage de sécurité, ce qui n'est pas sa mission première?

Nous sommes le seul pays à confier ce fardeau que représente le filtrage de sécurité à l'un de ses principaux organismes responsables de la collecte de renseignements.

[*Français*]

Jacques Ramsay: Monsieur Wark, je veux juste dire qu'il est possible d'avoir un service de renseignement qui a plusieurs départements et dont les gens ont différentes fonctions. On ne demande pas au service de contre-espionnage de faire la vérification. On peut quand même établir certaines nuances dans un service.

[*Traduction*]

Wesley Wark: C'est le même service, n'est-ce pas? Ce service, son directeur et son ministre, qui en est responsable, doivent répartir les ressources à cet effet, déterminer combien de personnes seront affectées à ce domaine, ce qu'ils doivent faire pour que ces dernières aient d'autres perspectives de carrière... Je pourrais continuer.

Il me semble insensé que le SCRS — et nous sommes les seuls à fonctionner ainsi au sein du Groupe des cinq — continue de faire ce travail. Nous pouvons maintenir ces pratiques et chercher à les améliorer, comme d'autres témoins l'ont suggéré, mais, ce faisant, je pense que nous n'arriverons jamais au type de système dont nous aurons besoin. Si nous conservons le système actuel, je crains que nous assistions à une dégradation des capacités du service dans les domaines clés où nous en avons besoin, à un recours accru à l'intelligence artificielle — une idée que vous pouvez trouver excellente ou non — et, bien franchement, à l'impartition dans le secteur privé. Est-ce bien ce que vous voulez?

J. Paul Haynes: J'ai eu des expériences intéressantes avec nos forces armées. Elles ont une force cybernétique, et nous avons eu plusieurs réunions lors desquelles nous avons essayé de déterminer comment nous pourrions faire de notre équipe chargée des opérations de sécurité une équipe de réservistes, afin qu'elle puisse être mobilisée dans les situations critiques.

La cinquième dimension du combat est désormais le cyberespace. Ce sujet fait partie de toutes les discussions militaires. Les ressources ne sont pas suffisantes. Elles permettent de gérer les opérations quotidiennes, mais, à une échelle beaucoup plus grande, elles ne suffisent pas. En période difficile ou de conflit, il faudrait se tourner vers les réservistes. Le problème, c'est que nous nous heurtons à un mur en matière d'habilitation, car nous n'avons pas réussi à mettre en place un système efficace. Comme tout le monde ici le sait sans doute, obtenir une habilitation de niveau secret ou plus élevé coûte très cher, et nous n'avons pas réussi à surmonter cette difficulté.

D'autres pays ont trouvé différentes solutions. Sur le plan de la sécurité nationale uniquement, si le secteur privé doit être intégré rapidement à notre structure de défense, le coût est très élevé. Peut-être, comme le disait M. Wark, est-ce parce que l'on utilise les meilleurs instruments de la boîte à outils pour faire le travail, qui est, en grande partie, très répétitif et banal. Il serait donc possible de réaliser des gains d'efficacité à cet égard. L'intelligence artificielle doit faire partie de la solution, cela ne fait aucun doute.

Aujourd'hui, nous avons abordé cette question dans une perspective gouvernementale. Nous pouvons toutefois réfléchir à la façon dont nous pourrions l'étendre à certains secteurs clés, ou à ceux que nous cherchons à redynamiser, comme l'aérospatiale. Ces habilitations sont importantes lorsqu'on travaille avec des pays alliés et des partenaires de formation. Intégrer le secteur privé dans le cercle, où il n'est pas présent actuellement, renforce nos capacités d'un point de vue économique. Ces éléments s'intègrent très rapidement. À l'heure actuelle, beaucoup d'acteurs sont laissés pour compte. Tous mes collègues du secteur de la cybersécurité au Canada ont eu des discussions semblables. Nous avons du mal à travailler avec notre propre gouvernement.

● (1810)

[*Français*]

Le président: Merci beaucoup, monsieur Ramsay.

Madame DeBellefeuille, vous avez la parole pour six minutes.

Claude DeBellefeuille: Merci beaucoup, monsieur le président.

Monsieur Morrison, je vous ai écouté avec attention et je suis surprise. Je suis d'accord sur toutes vos recommandations, parce que dans le fond, votre objectif, c'est de vouloir améliorer le système. Par contre, je me demande pourquoi ces recommandations ne sont pas déjà en place. Ça me surprend. Comment se fait-il qu'elles n'étaient pas en place avant l'événement Zhang? Il me semble qu'elles sont très légitimes, compte tenu du fait que c'est très documenté. D'autres témoins ont dit que le Canada est le pays du G7 le plus infiltré par la Chine.

Ce que vous nous proposez comme améliorations a du sens. Toutefois, comment se fait-il que ces recommandations ne soient pas déjà mises en place? Avec les fonctions que vous avez occupées comme sous-ministre des Affaires étrangères et les fonctions que vous occupez maintenant comme conseiller au Conseil privé, vous êtes à même de posséder toute l'information pour conseiller déjà en amont de mettre en place ce que vous nous avez proposé. C'est sur ça que je me questionne.

David Morrison: Je vous remercie de cette question.

J'ai dit dans mon allocution d'ouverture que la politique qui gouverne le fonctionnement du système, ici, au Canada, est une politique du Secrétariat du Conseil du Trésor. Je suis presque certain que d'autres témoins ici, devant ce comité, ont déjà décrit les améliorations qui ont été mises en place le 6 janvier 2025. C'était la première fois, je crois, depuis 2014, donc en 11 ans. Je crois que les circonstances qui ont mené ce comité à mener cette étude nous ont tous démontré qu'il y a plus de travail à faire.

Claude DeBellefeuille: J'ai de la difficulté à comprendre ce que vous me dites là. Dans ma tête à moi, le Conseil privé, les conseillers, ce sont des personnes qui sont très expérimentées qui conseillent le premier ministre et son gouvernement. Ça ne se peut pas que vous me disiez qu'à cause de l'événement Zhang et de notre étude, ça a provoqué des changements. Je veux dire que c'est nous donner une grande importance. Merci beaucoup, mais, dans ma tête à moi, il y a eu d'autres espions avant Mme Zhang, il y a eu d'autres événements. J'ai de la difficulté à comprendre qu'une grande institution, un pays du G7, réagisse à un événement et à une étude d'un comité. Je vais vous dire sincèrement que je trouve ça un peu gros, ce que vous me dites là.

L'autre question que j'aurais le goût de vous poser — et le temps file — c'est qu'un autre témoin, M. Wernick, du Conseil privé, nous a dit que, dans le fond, ce n'est qu'une question de volonté politique: si le gouvernement trouvait important de se protéger contre l'espionnage, il doterait ses agences et ses ministères de ressources suffisantes pour être capables de faire face à l'adversité. Il l'a dit clairement, tantôt.

Là, vous, vous êtes au Conseil privé. Vous ne pouvez pas me dévoiler de secrets, mais avec ce que nous avons entendu, moi, je m'attends à ce que dans le prochain budget, il y ait des sommes supplémentaires pour nous protéger contre l'ingérence et contre l'espionnage, et qu'on dote les ministères, les agences et les sociétés d'État des ressources nécessaires pour être capables de faire un meilleur filtrage. C'est ce que je comprends, parce que je suis un petit peu estomaquée de votre dernière réponse à ma question.

● (1815)

David Morrison: Je dirais que nous sommes en train d'améliorer tous nos systèmes de défense contre l'ingérence étrangère, contre l'espionnage, contre toutes les menaces. Dans une ou deux semaines, j'espère, nous allons avoir une nouvelle politique de sécurité nationale lancée par le gouvernement. Il y a un gros effort dans ce pays maintenant pour améliorer nos défenses contre toutes les menaces. Ce sera le thème principal de la nouvelle politique qui sera lancée sous peu.

C'est clair, du moins pour moi, et pour beaucoup d'autres témoins, parce que j'ai étudié les autres témoignages. Je crois que c'est la troisième réunion que vous tenez sur ce sujet. Il est clair que, dans le domaine des cotes de sécurité aussi, il faut faire plus de travail. Dans mon poste au Bureau du Conseil privé, je le ferai.

Le président: Merci, madame DeBellefeuille.

[*Traduction*]

La parole est d'abord à M. Caputo, puis à M. Lloyd.

Frank Caputo: Merci, monsieur le président.

Je reviens à M. Morrison.

Je voulais clarifier quelque chose, monsieur. Avez-vous bien dit, tout à l'heure, qu'au moment où Mme Zhang a obtenu sa cote de sécurité, les vérifications des sources ouvertes ne faisaient pas partie du processus d'habilitation de sécurité? Ai-je bien compris?

David Morrison: À ma connaissance, au moment où elle a reçu sa cote de sécurité, à ce niveau, les vérifications des sources ouvertes ne faisaient pas partie du processus.

Frank Caputo: D'accord. Savez-vous quelle cote de sécurité elle détenait? Je suppose qu'elle avait une cote de sécurité de niveau secret, au moins.

David Morrison: C'était une cote de niveau secret pour l'OTAN.

Frank Caputo: D'accord. Il y a la cote de fiabilité de base, la cote de fiabilité approfondie, et les cotes de niveau secret et très secret. La cote de niveau secret est assez élevée.

David Morrison: Il y a maintenant six niveaux. Il y...

Frank Caputo: Les variantes approfondies...

David Morrison: C'est essentiellement ce qui existe, mais chaque niveau comporte une variante approfondie.

Frank Caputo: D'accord. Savons-nous si, à son niveau, il lui fallait une cote approfondie de niveau secret?

David Morrison: Je ne peux pas me prononcer sur un cas précis.

Frank Caputo: D'accord. Pour quelqu'un à son niveau qui va à l'OTAN, savez-vous ce qu'il en serait?

David Morrison: Je suppose qu'une personne qui va à l'OTAN a besoin d'une cote de sécurité de niveau secret... oui

Frank Caputo: D'accord. Merci.

Pour que ce soit bien clair, savez-vous si les sources ouvertes sont désormais consultées dans le cas d'une cote de sécurité de niveau secret?

David Morrison: Oui, elles le sont.

Frank Caputo: Elles le sont. Bien. Vous ne pouvez pas faire de commentaires à ce sujet.

Je dirais, pour ma part, que lorsque l'on commence à faire les choses différemment une fois le fait accompli, cela revient, essentiellement, à avouer sa faute.

Sur ce, je cède la parole à M. Lloyd.

David Morrison: Avec tout le respect que je vous dois, il s'agit d'un resserrement, d'un renforcement du système. C'est, en gros, ce que j'ai essayé de dire dans ma déclaration préliminaire.

Frank Caputo: J'en suis conscient. Le moment choisi est toutefois révélateur du fait qu'on reconnaît qu'on ne faisait pas les choses de la meilleure façon possible s'il faut resserrer ce qui n'était pas assez rigoureux avant.

Dane Lloyd: En effet, oui.

Frank Caputo: Merci.

Dane Lloyd: Merci.

Monsieur Wark, j'aimerais parler de votre proposition de nous inspirer du modèle britannique. Je me questionne toujours quand des gens proposent de créer un nouveau secrétariat ou une nouvelle fonctionnalité.

Pourquoi ne pas simplement donner plus de ressources au SCRS pour accomplir la même chose? Quel serait l'avantage de mettre en place une entité distincte pour s'en occuper?

● (1820)

Wesley Wark: Merci, monsieur.

C'est une bonne question, et je suppose que le point de départ pour y répondre consisterait à voir pourquoi exactement le Royaume-Uni a pris cette direction et quelles pourraient être, selon les Britanniques, les forces et les faiblesses de ce modèle. Il faut tirer des leçons de l'expérience britannique. N'oubliez pas que l'approche du Canada en matière de contrôle de sécurité est unique au sein du Groupe des cinq. Savons-nous quelque chose que nos partenaires du Groupe des cinq ne savent pas sur la façon de procéder à des contrôles de sécurité? Je ne pense pas.

Vous pouvez toujours laisser cette fonction au SCRS. Or, le budget du SCRS n'a cessé d'augmenter, essentiellement depuis le 11 septembre. Le SCRS a donc pour tâche de répartir cet argent entre les diverses menaces dont il doit s'occuper. Le contrôle de sécurité ne sera jamais la priorité absolue pour lui, et ce ne devrait pas l'être non plus.

C'est donc un jeu d'équilibre très difficile pour le SCRS, de déterminer qu'il a besoin de tant de personnes pour le contrôle de sécurité s'il doit pour cela diminuer le nombre de ressources affectées au contre-espionnage, à l'ingérence étrangère ou aux postes à l'étranger. Est-ce bien ce que vous voulez?

Je pense simplement qu'il est beaucoup plus logique — et il ne s'agit pas de créer une nouvelle monstruosité bureaucratique, comme on l'a laissé entendre — de retirer l'expertise existante du SCRS, pour confier cette responsabilité à un organisme centralisé, qui serait en mesure de mettre en place les systèmes de données et les processus complets dont d'autres témoins ont parlé. Il ne s'agit pas d'alourdir la bureaucratie. Je dirais plutôt qu'il s'agit d'accroître l'efficacité, mais le point de départ serait de tirer des leçons du modèle britannique.

Dane Lloyd: Combien de temps me reste-t-il?

Le président: Il vous reste huit secondes.

Dane Lloyd: Je vous remercie. J'ai un peu l'impression d'être dans un épisode de *Yes Minister* en ce moment...

Des voix: Ah, ah!

Dane Lloyd: ... mais merci.

Le président: Je vous remercie de votre indulgence, monsieur Lloyd.

Je cède la parole à Mme Sodhi pour cinq minutes.

Amandeep Sodhi: Merci, monsieur le président.

Merci à nos témoins d'être ici aujourd'hui.

Monsieur Wark, vous avez mentionné que le Canada est le seul pays du Groupe des cinq à confier au SCRS la responsabilité d'effectuer les contrôles de sécurité, et vous avez également parlé de l'approche du Royaume-Uni. Pouvez-vous nous en dire plus sur les modèles privilégiés par les États-Unis, l'Australie et la Nouvelle-Zélande? Ont-ils également des organismes centralisés distincts pour gérer le processus de contrôle de sécurité?

Wesley Wark: Je serai très bref.

Je crois comprendre que tous nos autres partenaires du Groupe des cinq ont leurs propres processus et qu'ils ont tous adopté des méthodes différentes pour le contrôle de sécurité et la classification de sécurité. Les Australiens et les Néo-Zélandais ont des modèles assez semblables en fait, comme on pourrait s'y attendre. D'après ce que je comprends, aucun de ces pays ne demande à son service de renseignement d'effectuer le contrôle de sécurité. Ce n'est pas ce qui se passe aux États-Unis, en tout cas.

Amandeep Sodhi: Croyez-vous que le principal défi auquel le Canada est confronté en ce moment tient aux politiques, aux ressources, à l'échange de renseignements ou à la structure organisationnelle? Comment classeriez-vous ces questions?

Wesley Wark: C'est une question très vaste.

Ce que je dirais au Comité, pour l'instant, c'est que la conception du contrôle de sécurité a considérablement évolué depuis 2014, année où la première norme de contrôle de sécurité, la nouvelle norme, a été créée — comme M. Morrison l'a mentionné — jusqu'à son amélioration et quelques révisions en 2025. Ce travail s'est réalisé en grande partie sur la base de préoccupations relatives aux menaces internes. En 2014, c'était dans la foulée d'une importante affaire d'espionnage, l'affaire Jeffrey Delisle, qui avait offert ses services au GRU russe. Nous avons donc tiré des leçons de tout cela en cours de route.

Je pense que les politiques en place sont de bonnes politiques. Je dirais qu'il n'est jamais possible de mettre en place une culture de sécurité à 100 % pour contrer les menaces internes. L'une des choses qui ressortent de nombreuses études sur les menaces internes, c'est que très souvent, ces menaces se développent après qu'une personne ait obtenu un poste de confiance qui lui donne accès à des renseignements de nature délicate. On aura beau avoir les meilleurs contrôles de sécurité en place, lorsqu'on donne à une personne l'accès à un emploi et à une classification, cela pourrait ne plus nous plaire plus tard. Même là, j'attribuerais au gouvernement le mérite d'essayer de régler le problème.

Je terminerai sur ce point: nous ne nous contentons plus de nous dire que nous allons revoir la cote de sécurité de niveau très secret tous les cinq ans et la cote de sécurité de niveau secret tous les 10 ans. Il y a un processus qui s'applique depuis 2014 pour effectuer ce qu'on appelle le suivi, c'est-à-dire une surveillance continue des changements potentiels dans le comportement d'une personne ou sa situation, qui pourraient présenter des risques pour la sécurité. Il y a aussi eu un resserrement des périodes de 5 ans et de 10 ans où les habilitations de sécurité sont constamment examinées. Nous essayons de nous attaquer au problème.

Les politiques sont là. Nous avons la bonne approche. Je pense que c'est simplement confié au mauvais organisme, qui croule sous le fardeau. Il n'y a pas de solution facile et on se contente de donner plus d'argent au SCRS. Je pense qu'il faut un changement organisationnel.

● (1825)

Amandeep Sodhi: Très bien. Je vous remercie de votre réponse.

Il me reste un peu plus d'une minute. Je vais donner la parole à tous les témoins.

Si vous avez d'autres recommandations à formuler aux fins du compte rendu, n'hésitez pas à le faire.

David Morrison: Je dirais simplement que fondamentalement, c'est une question de gestion des risques. Dans un monde de plus en plus tumultueux, tous les risques ont augmenté. Cela sera expliqué en détail dans la prochaine stratégie de sécurité nationale.

Je comprends les commentaires de M. Wark selon lesquels on a appris des choses entre 2014 et 2025. Je peux vous assurer que quand il y a une défaillance du système qui a des conséquences imprévues, nous renforçons davantage le système.

[*Français*]

Le président: Merci beaucoup.

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

Claude DeBellefeuille: Merci beaucoup, monsieur le président.

Tantôt, mon collègue M. Ramsay a dit qu'on parlait d'un cas et que c'était une exception. J'ai senti une certaine banalisation du cas que nous sommes en train d'étudier, vu qu'on disait qu'il n'y en a pas tant que ça. En fait, nous ne pouvons pas savoir s'il y en a beaucoup, puisqu'il y a peut-être actuellement des espions qui ne se sont pas encore fait prendre.

Voici ce qui nous intéresse, et je comprends que c'est assez important. Vous nous l'avez dit, monsieur Morrison: le fait que l'affaire Zhang soit mise en lumière publiquement et soit étudiée au Comité a donné une espèce d'électrochoc au gouvernement. Vous avez aussi dit que tout le monde s'était mis à l'ouvrage et s'était mis à proposer des solutions pour améliorer le système, parce qu'il y a de plus en plus d'attaques, d'ingérence et d'infiltration par les pays étrangers au Canada. Ça nous a donné un électrochoc. C'est ce que j'ai senti quand vous m'avez répondu tantôt. Si le système fonctionnait, vous n'auriez pas dit que vous proposez une série d'actions à mener. Vous nous avez même donné une exclusivité — en tout cas, pour moi — en disant qu'on va lancer une politique nationale sur la sécurité nationale avant pas trop longtemps, tellement il faut réagir au niveau de risque actuel qui nous touche.

Est-ce que ma compréhension est bonne? Avez-vous vraiment eu un électrochoc en apprenant ce qui s'était passé dans l'affaire Zhang?

David Morrison: Encore une fois, je ne peux pas parler d'un cas précis.

Je dirais que ce qui peut se passer au Canada s'est déjà passé dans plusieurs autres pays. Récemment, comme M. Wark le sait très bien, il y a eu un épisode en Allemagne qui a été choquant. C'était un désastre, et il s'agissait de quelqu'un de l'intérieur.

Dans mon allocution, j'ai soulevé quelques idées pour renforcer notre système. Cependant, comme je viens de le dire, en fin de compte, c'est une question de gestion des risques.

● (1830)

[*Traduction*]

Nous ne vivons pas dans un monde à risque nul. Les systèmes peuvent toujours être renforcés. Le gouvernement et la bureaucratie sont déterminés à améliorer continuellement tous nos systèmes de sécurité nationale.

[*Français*]

Le président: Merci beaucoup.

Madame Kirkland…

Claude DeBellefeuille: Excusez-moi, monsieur le président, je voudrais remercier M. Morrison, parce qu'il a fait beaucoup d'efforts pour parler en français tout au long de son témoignage et pour répondre à mes questions.

Monsieur Morrison, ça me touche, parce que, souvent, les hauts fonctionnaires à votre niveau perdent leur français puisqu'ils travaillent beaucoup en anglais. Je voulais vous le dire. Je suis vraiment reconnaissante de vos efforts. Merci beaucoup.

David Morrison: Je suis un petit gars de Lethbridge en Alberta.

Le président: Nous avions reconnu l'accent des gens de Lethbridge.

David Morrison: Ce n'était pas évident.

Le président: C'est excellent.

Je vous remercie, madame DeBellefeuille, de vos mots toujours très généreux et pertinents.

Madame Kirkland, vous disposez de cinq minutes.

[*Traduction*]

Rhonda Kirkland: Merci, monsieur le président.

Je suis assez fasciné par le commentaire sur le « resserrement de notre système » pour ce qui est des sources ouvertes et de l'examen des sources ouvertes. Il me semble que la chose la plus sensée à faire, la première chose à faire, serait de chercher ces personnes sur Google.

Vous avez mentionné plus tôt, monsieur Morrison, que l'habilitation sera refusée si l'on juge qu'une personne n'est pas digne de confiance. Vous conviendrez, j'en suis sûr, que la fraude est un exemple de faible fiabilité.

David Morrison: Je serais d'accord, de manière hypothétique.

Rhonda Kirkland: Hypothétiquement... oui.

David Morrison: Hypothétiquement, si l'on sait parfaitement qu'un candidat s'est rendu coupable de fraude et que c'est documenté, cela en dirait long sur la fiabilité de cette personne.

Rhonda Kirkland: Vous diriez donc que s'il y avait un processus d'embauche pour l'OTAN et qu'Affaires mondiales voyait quoi que ce soit lié à de la fraude, la personne concernée ne recevrait probablement pas son habilitation de sécurité, dans la mesure où le ministère serait au courant de la chose.

David Morrison: Si les responsables d'Affaires mondiales avaient eu connaissance que quelqu'un détenait des renseignements compromettants sur l'aptitude de cette personne à protéger les secrets du Canada ou de l'OTAN et sur sa fiabilité, je suis convaincu qu'ils auraient agi en conséquence.

Rhonda Kirkland: Merci de cette réponse.

Nous avons établi qu'à une certaine période, les vérifications des sources ouvertes ne faisaient pas partie du processus d'embauche et d'octroi d'habilitations de sécurité, ce que je trouve consternant, je le répète. Vous estimez que le système a été resserré et qu'on en fait maintenant. À mon avis, si vous deviez resserrer le système, cela signifie qu'il y avait des failles. Il y avait des failles dans ce système; par conséquent, nous avons dû le resserrer pour veiller à ce que cela ne se reproduise plus.

Aidez-moi à comprendre. Je vais essayer de l'expliquer de mon mieux. Si quelqu'un a besoin d'une habilitation de sécurité et que nous savons que le processus ne comprend pas de vérifications des sources ouvertes, ne ferions-nous pas une recherche dans les dossiers des tribunaux fédéraux ou provinciaux?

David Morrison: Comme mes collègues l'ont dit devant le Comité, je crois, il y a un certain nombre d'éléments qui entrent dans l'évaluation de l'habilitation de sécurité.

Rhonda Kirkland: Oui, absolument. Je veux juste...

David Morrison: L'un de ces éléments relève du SCRS et concerne la sécurité nationale; l'autre relève de la GRC et concerne le respect de la loi. Il y a aussi des vérifications de crédit. Ce sont les procédures qui s'appliqueraient dans le cas de quelqu'un qui présente sa candidature à l'OTAN. Mes collègues d'Affaires mondiales m'ont assuré qu'ils ont ajouté à ce protocole une recherche dans les sources ouvertes.

Rhonda Kirkland: Très bien. Je suis heureuse d'apprendre que la vérification des sources ouvertes a été ajoutée au processus, mais il semble qu'il faudrait aussi fouiller dans les bases de données de la Cour fédérale ou des tribunaux provinciaux pour voir si une personne a déjà été partie à une affaire soumise à la Cour fédérale.

Je rappelle qu'en juillet 2023, Mme Zhang a déposé une demande de contrôle judiciaire, comme en fait foi un document de la Cour fédérale qui date du 22 août 2024. Elle a obtenu un poste à l'OTAN au début 2025, donc c'était assez récent. Une simple recherche pour savoir s'il y avait des documents de la Cour fédérale portant ce nom aurait dû permettre de le découvrir.

Si ce que vous dites est vrai — à savoir que de façon générale, nous vérifierions s'il y a des documents judiciaires sur une personne avant de lui octroyer une habilitation de sécurité —, c'est un exemple clair et net de défaillance du système.

● (1835)

David Morrison: Je ne pense pas avoir dit que de façon générale, nous vérifierions les documents judiciaires. J'essayais plutôt de décrire le rôle du SCRS, de la GRC et d'Affaires mondiales Canada dans l'octroi d'une habilitation de sécurité à une personne pour un poste à l'OTAN. J'ai également dit très clairement, je pense, que selon les protocoles en place à l'époque, Affaires mondiales Canada n'exigeait pas de recherche dans les sources ouvertes. Il l'exige maintenant.

Rhonda Kirkland: Je comprends la partie sur les sources ouvertes. Ce qui me préoccupe, c'est la recherche dans les documents de la Cour fédérale et la question de savoir si cela ferait partie d'une vérification de sécurité.

David Morrison: C'est la GRC qui est censée vérifier l'aspect de la conformité à la loi, si je peux le dire ainsi.

Rhonda Kirkland: La GRC aurait pu faire une vérification...

Le président: Je suis vraiment désolé de vous interrompre, madame Kirkland. C'était une bonne intervention.

Monsieur Powlowski, vous avez cinq minutes, s'il vous plaît.

Marcus Powlowski: Monsieur Wark, je suppose que vous connaissez le fonctionnement des comités. Vous avez fait une recommandation très succincte. Vous avez dit que le système actuel de contrôle de sécurité n'est pas viable. À l'heure actuelle, le SCRS doit vérifier le profil de 480 000 immigrants par année en plus de faire ces contrôles de sécurité. Il a donc 520 000 cas à traiter par année.

Le Royaume-Uni a mis en place un système de contrôle de sécurité à part. Est-ce pour tous les employés du gouvernement? Est-ce tout ce que fait l'organisme britannique?

Wesley Wark: Je vous remercie de cette question, monsieur.

Le bureau de vérification de la sécurité du Royaume-Uni, comme on l'appelle, accorde des habilitations de sécurité pour tous les ministères et organismes gouvernementaux du Royaume-Uni. Il s'agit d'une unité centralisée qui travaille au sein du Cabinet et qui sert l'ensemble du gouvernement britannique.

Marcus Powlowski: Vous proposez que nous formulions une sorte de recommandation selon laquelle le gouvernement du Canada devrait envisager de créer un organisme indépendant de contrôle de sécurité pour les employés du gouvernement. Est-ce bien ce que vous proposez?

Wesley Wark: C'est une formidable idée, monsieur.

Marcus Powlowski: Nous avons ici un membre de notre gouvernement qui est assez haut placé.

Monsieur Morrison, je suis désolé de vous mettre sur la sellette, d'une certaine façon, mais je suppose que compte tenu de votre poste, ce n'est pas la première fois que cela vous arrive.

Que pensez-vous de cette idée?

David Morrison: Je vous ai donné quatre exemples de choses qu'il pourrait être utile de mettre en oeuvre pour renforcer les systèmes actuels, selon mes collègues du Bureau du Conseil privé et moi. Je vous demanderais de porter une attention particulière à la quatrième recommandation, qui porte sur l'évaluation en continu. Les trois premières concernent le filtrage initial. La dernière recommandation, qui porte sur la surveillance en continu, les programmes de gestion des risques internes et ainsi de suite, est essentielle, et il faudrait à ce titre mettre l'accent sur l'autodéclaration. Si la situation financière d'une personne change, si une personne se marie avec une nouvelle personne ou si elle se marie tout court, ce sont des renseignements que les gens doivent divulguer, car cela pourrait changer leur profil de risque.

Pour être tout à fait honnête, je n'ai pas réfléchi à la question de savoir qui exactement devrait s'acquitter de cette responsabilité. Je viens d'expliquer que cela ne relève pas uniquement du SCRS. Cela ne relève pas uniquement de la GRC. Cela ne relève pas uniquement d'Affaires mondiales Canada. Si j'étais à votre place, je poserais la question suivante à M. Wark: le SCRS ne finira-t-il pas par faire une grande partie du travail de toute façon parce qu'un organisme centralisé devrait probablement utiliser les systèmes du SCRS?

Très franchement, je pense que la culture et le protocole de sensibilisation à la sécurité sont beaucoup plus importants que la structure elle-même. La fonction pourrait être centralisée au SCRS, mais isolée du reste. Je travaille au Bureau du Conseil privé. Je n'ai jamais été en faveur de l'idée d'élargir le BCP. Je pense que le noyau du travail devrait se faire dans les ministères responsables, mais c'est ce que les gens du Bureau du Conseil privé disent toujours.

● (1840)

Marcus Powlowski: Rapidement, j'aimerais demander à M. Wark de répondre à la suggestion de M. Morrison selon laquelle le SCRS finira par faire tout le travail de toute façon.

Wesley Wark: Je ne pense pas que ce soit l'idée. Ce ne serait pas un résultat souhaitable. On voudrait plutôt, bien sûr, comme M. Morrison l'a indiqué, un organisme central ayant accès aux données du SCRS. On voudrait un organisme central ayant accès aux bases de données criminelles de la GRC, aux données du Centre d'information de la police canadienne, et ainsi de suite. On voudrait un organisme spécial qui pourrait puiser dans ces ressources sans que le SCRS ait à déployer ses propres employés pour faire ce travail.

Le président: Merci, monsieur Powlowski.

[*Français*]

Je remercie les trois invités, MM. Wark, Haynes et Morrison, d'avoir participé et de s'être préparés pour cette réunion importante. Je leur souhaite de passer une bonne fin de journée. Nous allons maintenant les laisser quitter la réunion tranquillement.

[*Traduction*]

Nous arrivons presque à la fin de la réunion, mais je crois que M. Caputo voulait déposer un avis de motion.

Frank Caputo: Merci beaucoup, monsieur le président.

Comme les gens l'ont vu, la libération conditionnelle est au cœur de bien des questions que j'ai posées à la Chambre des communes ces derniers temps. J'ai rencontré récemment la mère de Heather Aspin-Thomas, une fillette de 10 ans assassinée, et son avocate, Rebecca Darnell. J'ai également beaucoup travaillé à d'autres dossiers de libération conditionnelle. Brock Graham est un délinquant sous responsabilité fédérale qui a été libéré récemment. J'ai fait un peu de travail à ce sujet.

Après avoir parlé avec les victimes, je crois que la motion dont je donne avis se justifie:

> Que, conformément au paragraphe 108(2) du Règlement, le Comité mène une étude portant sur les politiques, les pratiques et les procédures de la Commission des libérations conditionnelles du Canada, ainsi que sur leur incidence sur les victimes d'actes criminels violents et leurs familles.
>
> Que le Comité consacre au moins cinq séances à cette étude; qu'il invite le ministre de la Sécurité publique, la présidente de la Commission des libérations conditionnelles du Canada, l'ombudsman fédéral des victimes d'actes criminels, ainsi que tout autre témoin qu'il jugera utile d'entendre et qu'il fasse rapport de ses conclusions et recommandations à la Chambre.

Merci, monsieur le président.

[*Français*]

Le président: Merci beaucoup, monsieur Caputo. Ce sera traduit dans les deux langues officielles.

Chers membres du Comité, je vous informe que, lundi prochain, nous recevrons des témoins dans le cadre de l'étude du projet de loi C-236 de M. Lloyd. Le mercredi suivant, nous en ferons l'étude article par article. Cela dit, les amendements doivent être soumis d'ici le vendredi 23 octobre. Il y aura autre chose la semaine suivante, mais nous réserverons du temps pour en discuter.

Je vous remercie beaucoup de votre attention et de votre participation.

Bonne soirée.

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