CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

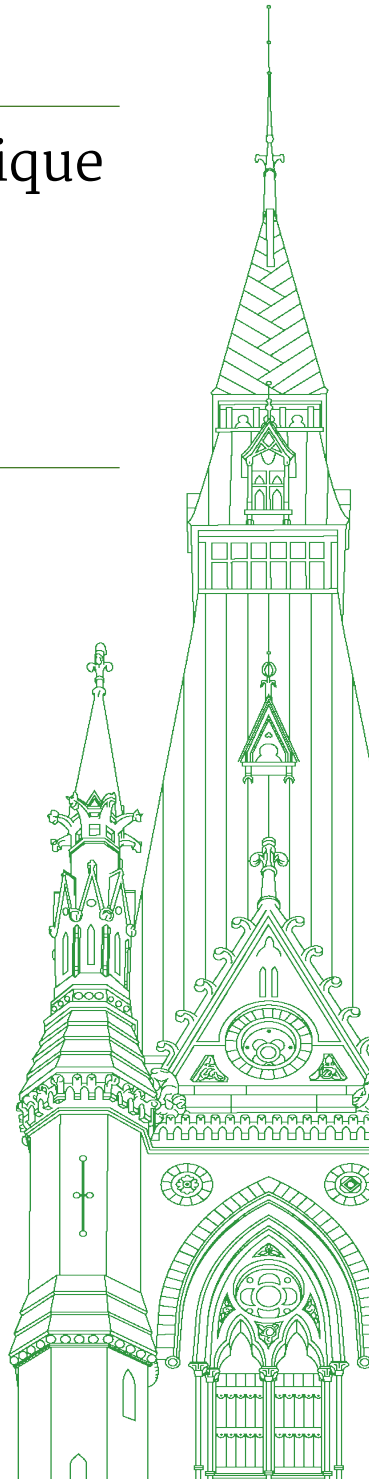
44e LÉGISLATURE, 1re SESSION

Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 095

Le jeudi 15 février 2024



Président : M. Heath MacDonald

Comité permanent de la sécurité publique et nationale

Le jeudi 15 février 2024

● (0815)

[*Traduction*]

Le président (M. Heath MacDonald (Malpeque, Lib.)): Je déclare la séance ouverte.

Bienvenue à la 95e réunion du Comité permanent de la sécurité publique et nationale.

La réunion d'aujourd'hui se déroule en mode hybride, conformément au Règlement. Les membres y participent en personne, dans la salle, et à distance à l'aide de l'application Zoom.

J'aimerais formuler quelques consignes à l'intention des témoins et des députés.

Veuillez attendre que je vous nomme avant de prendre la parole.

Afin d'éviter tout incident de retour de son pendant notre réunion, nous demandons à tous les participants d'éloigner leurs oreillettes de tout microphone. Les incidents liés au retour de son peuvent blesser gravement les interprètes et perturber les procédures.

À titre de rappel, toutes les observations doivent être adressées à la présidence.

Conformément à l'ordre de renvoi du lundi 27 mars 2023, le Comité reprend l'étude du projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois.

Nous accueillons aujourd'hui l'honorable Dominic Leblanc, député et ministre de la Sécurité publique, des Institutions démocratiques et des Affaires intergouvernementales, et l'honorable François-Philippe Champagne, député et ministre de l'Innovation, des Sciences et de l'Industrie.

Les témoins du ministère de la Sécurité publique et de la Protection civile sont Patrick Boucher, sous-ministre adjoint principal, Secteur de la sécurité et de la cybersécurité nationale, Colin MacSween, directeur général, Direction générale de la cybersécurité nationale, et Kelly-Anne Gibson, directrice par intérim, Direction générale de la cybersécurité nationale.

Les témoins du ministère de l'Industrie sont Éric Dagenais, sous-ministre adjoint principal, Secteur du spectre et des télécommunications, et Mark Schaan, sous-ministre adjoint principal, Secteur des stratégies et politiques d'innovation.

Je précise que les ministres seront avec nous pendant une heure et demie. Les fonctionnaires resteront pour le reste de la réunion afin de répondre aux questions des députés.

Chers collègues, nous devrons prendre 10 à 15 minutes à la fin de la réunion pour traiter des affaires du Comité, comme les budgets et le programme du Comité.

Bienvenue à tous.

J'invite maintenant le ministre Leblanc et le ministre Champagne à faire une déclaration préliminaire. Vous disposez de 10 minutes.

Merci.

Monsieur le ministre Leblanc, pourriez-vous commencer?

L'hon. Dominic LeBlanc (ministre de la Sécurité publique, des Institutions démocratiques et des Affaires intergouvernementales): Avec le plus grand plaisir, monsieur le président.

[*Français*]

Merci, monsieur le président.

Je vous remercie, collègues, de m'avoir invité pour parler du projet de loi C-26, qui concerne la cybersécurité.

Je suis heureux d'être ici avec mon collègue François Philippe Champagne et les autres fonctionnaires que vous avez gentiment nommés, monsieur le président.

[*Traduction*]

Les infrastructures essentielles du Canada sont de plus en plus interconnectées, interdépendantes et intégrées aux cybersystèmes. Nos infrastructures essentielles jouent un rôle vital dans la fourniture des services essentiels et des nécessités de la vie quotidienne. Afin de préserver la sécurité économique et nationale, nous devons avoir une vision plus complète des cybermenaces qui pèsent sur les Canadiens. Nous pensons que le projet de loi C-26 constitue une étape importante dans l'accomplissement de cette tâche.

Ce projet de loi protégera les Canadiens et renforcera la cybersécurité dans les secteurs des finances, des télécommunications, de l'énergie et des transports réglementés par le gouvernement fédéral. Ces secteurs contribuent tous de manière essentielle à l'économie du pays et à la sécurité des Canadiens. En raison de leur vitalité, ils sont aussi, évidemment, des cibles attrayantes pour les cyberactivités malveillantes, telles que l'espionnage, le vol de données et de propriété intellectuelle et, bien sûr, le sabotage proprement dit.

Ces préoccupations ne sont pas purement hypothétiques. Récemment, le Centre canadien pour la cybersécurité s'est joint aux partenaires opérationnels du Groupe des cinq pour émettre une mise en garde au sujet de cyberacteurs parrainés par la République populaire de Chine qui cherchent à se prépositionner en vue de mener des cyberattaques perturbatrices ou destructrices contre les infrastructures essentielles des États-Unis en cas de crise ou de conflit majeur avec notre voisin du Sud.

Des cyberincidents se produisent presque quotidiennement dans les secteurs d'infrastructures essentielles. En janvier 2023, CBC News a rapporté qu'une société territoriale et d'État, ainsi que l'unique distributeur d'énergie du Nunavut, ont été victimes d'une cyberattaque. En juin de l'an dernier, le *Calgary Herald* a rapporté que la société énergétique canadienne Suncor avait été victime d'un cyberincident majeur qui avait interrompu les opérations de débit et de crédit dans les stations-service de Petro-Canada à travers le pays. Nous nous souvenons tous des cyberincidents qui ont paralysé le système de santé de Terre-Neuve-et-Labrador en 2021.

Le projet de loi C-26 nous aiderait à défendre les infrastructures et les services essentiels dont les Canadiens et les entreprises canadiennes dépendent au quotidien. Cette nouvelle loi renforcerait la collaboration et l'échange de renseignements entre l'industrie et le gouvernement et obligerait les opérateurs désignés à signaler les incidents de cybersécurité au Centre de la sécurité des télécommunications, qui, comme nos collègues le savent, est un organisme du ministère de la Défense nationale.

En améliorant la connaissance qu'a le gouvernement des cybermenaces qui planent sur les secteurs essentiels réglementés par le gouvernement fédéral, nous pouvons avertir les exploitants des menaces et vulnérabilités potentielles afin qu'ils puissent prendre des mesures pour protéger leurs systèmes et protéger également les Canadiens.

● (0820)

[*Français*]

Toutefois, le gouvernement ne peut pas le faire seul. C'est pourquoi nous nous engageons à travailler en étroite collaboration avec nos partenaires de l'industrie, au moyen du processus réglementaire officiel, afin de créer un régime réglementaire clair, cohérent et harmonisé dans toutes les provinces et tous les territoires.

[*Traduction*]

Nous devons travailler avec nos alliés — et nous allons le faire, en particulier avec les États-Unis — pour veiller à ce que les infrastructures essentielles interconnectées soient protégées.

Le projet de loi va dans le sens des approches de nos alliés en matière de cybersécurité, et nous nous sommes engagés avec des partenaires internationaux à cerner les possibilités de collaboration future. Pas plus tard que mardi dernier, j'ai participé à une réunion téléphonique ministérielle du Groupe des cinq, au cours de laquelle M. Mayorkas, secrétaire à la Sécurité intérieure des États-Unis, a soulevé un grand nombre des questions dont nous allons parler ce matin.

[*Français*]

Nous avons constaté que les intervenants soutiennent largement l'intention du projet de loi et qu'ils conviennent que nous devons travailler de concert pour protéger nos infrastructures essentielles contre les cybermenaces. Toutefois, certains ont exprimé des inquiétudes quant à certains aspects du projet de loi. Nous avons évidemment écouté attentivement les points soulevés par nos collègues à la Chambre des communes et d'autres concernant la transparence, la responsabilité et la protection de la vie privée des Canadiens.

Fondamentalement, ce projet de loi contribuera à protéger la confidentialité des renseignements personnels des Canadiens. Les systèmes d'infrastructures critiques du Canada, bien que sécurisés, ne sont pas impénétrables. En obligeant les opérateurs d'infrastructures critiques du Canada à maintenir des niveaux élevés de cybersécurité, nous réduisons également la probabilité de violations de données personnelles sur leurs systèmes.

Je me réjouis de travailler avec vous, monsieur le président, et avec les membres du Comité sur toutes ces questions. Évidemment, si le Comité le juge nécessaire, nous serons prêts à examiner des amendements qui pourraient renforcer le projet de loi. De plus, nous souhaitons travailler avec vous afin d'assurer l'adoption de ce projet de loi et de veiller à ce que le Canada reste un pays sûr, compétitif et connecté, dans un contexte plus sécuritaire.

Je vous remercie.

J'ai bien hâte d'entendre les propos de mon collègue M. Champagne — c'est d'ailleurs la raison pour laquelle je suis venu ici ce matin — et de répondre aux questions des membres du Comité.

● (0825)

[*Traduction*]

Le président: Merci.

Monsieur Champagne, allez-y, je vous prie.

[*Français*]

L'hon. François-Philippe Champagne (ministre de l'Innovation, des Sciences et de l'Industrie): Merci, monsieur le président.

C'est un grand privilège d'être devant vous aujourd'hui. Cela fait plus de huit ans que j'ai le privilège d'être député et de témoigner devant des comités. Ce matin, cela revêt une importance particulière, d'autant plus que j'ai le privilège de témoigner avec le ministre LeBlanc. Pour les gens qui nous regardent, les Canadiens et les Canadiennes de partout au pays, cela démontre l'importance de la question.

Il faut commencer par se demander pourquoi nous sommes là ce matin. Le ministre LeBlanc a fait le tour des raisons pouvant l'expliquer. Les gens devraient être rassurés de voir le ministre LeBlanc, et son ministère, travailler de concert avec le ministère de l'Industrie sur une question qui touche non seulement l'ensemble des Canadiens et des Canadiennes, mais aussi les entreprises canadiennes partout au pays.

La question de la cybersécurité touche nos petites ou moyennes entreprises, ou PME, les familles, l'ensemble des institutions au pays et, je dirais même, à l'international. Je peux vous dire que, dans les différents forums internationaux où je suis allé, la question de la cybersécurité est d'une importance capitale, particulièrement quand on ajoute tout ce qui est du domaine des technologies quantiques et tout ce qui concerne l'intelligence artificielle. C'est pour cela que je suis fier de témoigner aujourd'hui avec le ministre LeBlanc, un grand ami qui, lui aussi, voit l'importance de voir nos deux équipes travailler main dans la main pour faire cela aujourd'hui.

Comme je le disais, je suis heureux de pouvoir discuter avec vous, chers collègues, d'un texte législatif d'une importance primordiale. Les gens au pays s'attendent à ce que l'on agisse rapidement à l'égard d'une situation qui évolue tout aussi rapidement.

L'une des choses les plus importantes que nous puissions faire en tant que législateurs est de protéger nos infrastructures essentielles partout au pays.

[*Traduction*]

En tant que ministre de l'Innovation, des Sciences et de l'Industrie, je m'intéresse particulièrement à la sécurisation du système de télécommunications du Canada. Les réseaux de télécommunications sont essentiels à la sécurité, à la prospérité et au bien-être des Canadiens. Des catastrophes frappent un peu partout au pays et les citoyens s'attendent à ce que les réseaux de télécommunications fonctionnent. C'est pourquoi il est si important d'ajouter, comme le prévoit le projet de loi, le concept de sécurité en tant qu'objectif de la Loi sur les télécommunications. Il ne s'agit pas seulement de cybersécurité, mais aussi de protéger les Canadiens dans les moments où ils en ont le plus besoin. C'est pourquoi nous nous engageons à protéger le système de télécommunications, qui sous-tend une grande partie des infrastructures essentielles du pays.

L'émergence de nouvelles technologies, telles que la technologie 5G, est l'une des raisons pour lesquelles il faut redoubler d'efforts. Comme vous le savez, le réseau 5G sera beaucoup plus décentralisé. On parle de l'Internet des objets, de la connexion de presque tout. Les objets deviendront intelligents et connectés. Si on pense aux répercussions sur le plan de la cybersécurité, on comprend l'ampleur du problème, et non seulement les pouvoirs d'urgence dont nous avons besoin, mais aussi le devoir d'agir que nous avons tous en tant que parlementaires.

[*Français*]

Les menaces qui visent ces technologies et ces systèmes sont de plus en plus nombreuses. Je parle, entre autres, des menaces sur nos chaînes d'approvisionnement et des menaces de cybersécurité émanant d'acteurs étatiques et non étatiques, évidemment.

C'est en tenant compte de ces dangers que le gouvernement a procédé à un examen approfondi de la technologie 5G. Je tiens d'ailleurs à remercier l'ensemble des fonctionnaires du ministère de l'Industrie ainsi que les fonctionnaires du ministère de la Sécurité publique et de la Protection civile qui sont ici aujourd'hui. Ils ont fait un travail exhaustif en consultant les parties prenantes partout au pays.

Nous avons examiné attentivement la question sur les plans technique et économique, comme l'a dit mon collègue le ministre LeBlanc, ainsi que sur le plan de la sécurité nationale.

[*Traduction*]

Il est évident que si cette technologie comporte des avantages considérables, elle pose également de nouveaux problèmes de sécurité que des acteurs malveillants pourraient exploiter, car les réseaux 5G sont plus interconnectés que jamais. Par conséquent, les menaces auront un impact plus important sur la sûreté et la sécurité des Canadiens, y compris sur les infrastructures essentielles, comparativement aux réseaux des générations précédentes.

C'est à la lumière de cet examen de la sécurité que le gouvernement du Canada a exprimé de sérieuses préoccupations à l'égard de fournisseurs tels que Huawei et ZTE. Vous vous souviendrez qu'en mai 2022, nous avons annoncé notre intention d'interdire aux fournisseurs canadiens de services de télécommunications d'utiliser les produits et services Huawei et ZTE dans leurs réseaux 5G et 4G.

● (0830)

[*Français*]

Notre énoncé précisait que les mesures proposées feraient l'objet d'une consultation.

Toutefois, les risques liés aux télécommunications vont bien au-delà de la cybersécurité, comme je le disais. Nous avons pris des mesures, lorsque nous avons fait cette annonce, en mai 2022.

[*Traduction*]

Les Canadiens qui nous regardent se souviendront de la célèbre panne de Rogers à l'été 2022, qui a probablement touché 12 millions de Canadiens pendant plusieurs heures. Après le passage de l'ouragan Lee au Canada atlantique en septembre 2023, mon collègue, le ministre LeBlanc, s'est vraiment impliqué dans le rétablissement des services dont les gens avaient besoin.

Je veux que mes collègues comprennent qu'il ne s'agit pas seulement de sécurité nationale. En effet, le rôle du ministre de l'Industrie est de garantir la résilience. Dans le cas de Rogers, nous avons réussi à obtenir un engagement volontaire dans le protocole d'entente que nous avons signé avec la société en septembre, mais je pense que les Canadiens seront rassurés par le fait que le ministre aura le pouvoir législatif d'obliger les entreprises à faire ce qui est juste.

Nous savons que le marché ne peut pas à lui seul atténuer ces risques. C'est pourquoi il faut établir des règles pour l'industrie, qui protègent les Canadiens, les réseaux, les entreprises et les données.

[*Français*]

Le projet de loi C-26, dont nous discutons aujourd'hui, a été conçu pour faire face à ces risques et à l'évolution des menaces. Il va permettre au gouvernement d'agir rapidement, au besoin, pour assurer la sécurité des réseaux.

À mon avis, les pouvoirs qui seraient donnés au ministre de l'Industrie lui permettraient d'agir rapidement. En situation d'urgence, il faut adopter des mesures temporaires, mais il faut le faire rapidement afin de prévenir des problèmes plus importants pour l'ensemble du réseau.

La deuxième partie du projet de loi C-26 va également renforcer la protection de nos cybersystèmes essentiels. Je pense qu'il s'agit de la partie dans laquelle le ministre LeBlanc s'est très impliqué.

[*Traduction*]

Le réseau de télécommunication est sans doute l'épine dorsale des infrastructures. Je sais que les gens à la maison pensent que les infrastructures sont des ponts qu'il faut protéger, ou peut-être des centrales nucléaires, mais le réseau de télécommunications, qui est à la base de tout le reste, est l'un des principaux réseaux clés que nous devons protéger.

Monsieur le président, nous voulons être certains de bien faire les choses. Comme l'a dit le ministre LeBlanc, c'est pourquoi nous avons écouté attentivement les débats à la Chambre des communes et les observations des intervenants et des collègues, qui sont ici parce que, lorsqu'il s'agit de sécurité nationale, on met de côté la partisanerie. C'est pourquoi nous sommes déterminés à faire en sorte que les choses se déroulent le mieux possible.

Je me réjouis de constater que le projet de loi jouit d'un vaste appui, de même que l'objectif consistant à sécuriser le réseau de télécommunications.

[*Français*]

Nous voulons travailler de manière constructive pour obtenir le meilleur projet de loi possible, mais je dois dire aussi qu'il est urgent d'agir. Les gens qui voudraient causer des dommages au Canada regardent, évidemment, les failles qu'il pourrait y avoir dans le système. Il est donc urgent de donner des pouvoirs au gouvernement pour qu'il soit en mesure de bien faire les choses. C'est important.

J'attends donc avec impatience l'adoption du projet de loi C-26 afin de mieux protéger nos infrastructures essentielles.

Monsieur le président, cela nous fera plaisir, mon collègue le ministre LeBlanc et moi, de répondre aux questions de nos collègues.

Merci.

[*Traduction*]

Le président: Je vous remercie tous les deux de vos interventions.

Nous passons directement aux questions.

Commençons avec M. Shipley. Allez-y, vous avez six minutes.

M. Doug Shipley (Barrie—Springwater—Oro-Medonte, PCC): Merci monsieur le président.

Je remercie les ministres et les fonctionnaires de leur présence aujourd'hui.

Assurément, la cybersécurité et le projet de loi C-26 sont des sujets sérieux.

Monsieur le ministre LeBlanc, Sécurité publique Canada reconnaît 10 secteurs d'infrastructures essentielles, dont l'un est le gouvernement. Dans un récent rapport du Comité des parlementaires sur la sécurité nationale et le renseignement, ou CPSNR, on signale que plusieurs ministères et sociétés d'État ne sont pas soumis aux politiques du Conseil du Trésor relatives à la cyberdéfense ou qu'ils appliquent ces politiques de cyberdéfense de manière incohérente dans leur organisation. Ils sont donc vulnérables aux cyberattaques. En fait, une atteinte importante à la sécurité des données à Affaires mondiales Canada a récemment été révélée.

Monsieur le ministre LeBlanc, pourquoi votre propre gouvernement n'adhère-t-il pas aux mêmes normes de cybersécurité que les opérateurs désignés énumérés dans le projet de loi, dont vous prévoyez de recueillir et de stocker les informations commerciales et personnelles confidentielles?

L'hon. Dominic LeBlanc: Bien entendu, nous avons pris note du travail réalisé par le CPSNR. Il s'agit là, pour notre gouvernement et notre ministère, de feuilles de route importantes pour une meilleure politique publique et une meilleure loi.

Je sais que des initiatives de passation de marchés sont en cours dans l'ensemble du gouvernement pour améliorer de nombreux systèmes d'information qui sont soit obsolètes, soit en fin de vie, et qui doivent être renforcés. C'est quelque chose que l'industrie et les entreprises font constamment. Le gouvernement a la même obligation.

En fait, vous demandez si le gouvernement du Canada a l'obligation de se tenir au moins à la norme qu'il attend de l'industrie privée, et la réponse est, bien sûr, et nous cherchons activement des moyens de le faire. Vous avez mentionné le ministère des Affaires étrangères, et je sais que, dans le portefeuille de la sécurité publique, nous investissons activement dans la modernisation des systèmes et sommes constamment à la recherche de bonnes idées et de meilleures solutions, y compris avec nos alliés.

● (0835)

M. Doug Shipley: Merci.

On est presque unanime pour dire qu'il s'agit d'un projet de loi important, mais c'est aussi un projet de loi mal rédigé. Les groupes d'entreprises, les groupes de défense des libertés civiles et les entreprises de cybersécurité s'entendent tous sur le fait que le projet de loi C-26 donne au gouvernement trop de pouvoir, presque sans surveillance. On n'exige pas de rapports réguliers, pas d'examens indépendants et pas d'exigence de production de rapports écrits. En fait, la plupart des pouvoirs prévus dans le projet de loi seraient exercés en secret.

Pensez-vous que les pouvoirs étendus que vous tentez de vous octroyer sont assortis de mécanismes de contrôle suffisants?

L'hon. Dominic LeBlanc: Nous avons évidemment pris note des préoccupations exprimées par les personnes auxquelles notre collègue a fait référence. Dans le cadre des travaux du Comité, s'il y a des amendements qui, à votre avis, répondent à certaines de ces préoccupations, nous serions bien sûr disposés à travailler avec le Comité et à veiller à ce que nous obtenions collectivement le meilleur projet de loi possible.

Nous reconnaissons qu'il s'agit, à bien des égards, de pouvoirs extraordinaires qui nécessitent un contrôle approprié, comme vous l'avez mentionné. Il existe un élément de contrôle judiciaire, mais nous sommes conscients que les menaces évoluent elles aussi, et très rapidement. D'après certaines informations que m'ont transmises des responsables de la sécurité, y compris du Service canadien du renseignement de sécurité, les auteurs de menaces, y compris les acteurs étatiques malveillants, cherchent à causer certains des dommages et à perturber certains des systèmes dont nous avons parlé. Nous devons être en mesure d'agir rapidement et de contribuer à l'identification des risques et, nous l'espérons, à la prévention des incidents. C'est pourquoi ces pouvoirs existent, mais nous reconnaissons qu'ils doivent être assortis d'une obligation de transparence dans tous les cas possibles et d'examens appropriés, y compris des examens judiciaires.

Monsieur Champagne, vous vouliez ajouter quelque chose au sujet de l'examen judiciaire.

L'hon. François-Philippe Champagne: Si vous le permettez, monsieur le président, j'aimerais ajouter que la question est importante, évidemment, et, comme je l'ai dit, que nous sommes pour la surveillance, les examens judiciaires et le concept de la proportionnalité.

J'aimerais rappeler aux députés qu'à la suite de tempêtes majeures, en particulier sur la côte Est, des premiers ministres nous ont demandé d'intervenir. Comme je l'ai dit, dans le domaine des télécommunications, bien que nous ayons signé des protocoles d'ententes volontaires avec les entreprises de télécommunications, je crois que les Canadiens et les députés voudraient que tout futur ministre de l'Industrie ait également le pouvoir d'intervenir très rapidement.

Vous vous souvenez peut-être que, dans certains cas, on nous a demandé d'ordonner aux entreprises de télécommunications de faire certaines choses. Je peux vous assurer que lorsque le 911 n'est pas accessible et qu'il y a situation d'urgence, les Canadiens sont très inquiets. Le fait que nous puissions prendre des mesures correctives ou obliger les entreprises de télécommunications à faire certaines choses — qu'elles ont maintenant accepté de faire de leur plein gré ce qui, je pense, est une bonne chose...

M. Doug Shipley: Merci.

L'hon. François-Philippe Champagne: Je ne crois pas que les Canadiens veuillent dépendre du bon vouloir des entreprises.

M. Doug Shipley: Merci.

Il ne me reste presque plus de temps, mais j'ai une dernière question à poser à M. Champagne.

De nombreux intervenants ont fait remarquer que les sanctions proposées dans le projet de loi, qui pourraient atteindre 15 millions de dollars et cinq ans d'emprisonnement, sont présentées comme visant à promouvoir le respect de la loi plutôt qu'à punir. Cependant, je pense que nous sommes tous d'accord pour dire qu'une sanction de cette nature serait très difficile à assumer pour une petite entreprise.

A-t-on pris en considération l'impact que ces sanctions importantes auraient sur les petites et moyennes entreprises?

L'hon. François-Philippe Champagne: Avec tout le respect que je dois au Comité, je dirais qu'il s'agit toujours d'une question d'équilibre. Je dirais aussi respectueusement aux membres du Comité que l'amende doit être proportionnelle, car il est évident que vous faites référence aux petites et moyennes entreprises. Soyons clairs: le risque systémique pour un réseau comprenant de très grands acteurs est le danger d'une amende trop faible, et mes collègues seraient d'accord pour dire que, si l'amende est de cette nature lorsqu'il s'agit de grands exploitants de services de télécommunications, elle n'est pas très pertinente. Je ne suis pas sûr que cela donnerait au ministre de l'Industrie le pouvoir de les contraindre à prendre des mesures.

Je ne suggère pas qu'ils le fassent, mais ils pourraient effectuer une analyse coût-bénéfice et décider d'ignorer le ministre, car, en fin de compte, l'amende est si insignifiante qu'ils poursuivraient leurs activités comme si de rien n'était.

En cas d'urgence, je peux vous dire que la panne de Rogers a touché 12 millions de Canadiens. Dans une telle situation, vous avez besoin d'une mesure punitive pour assurer le respect des règles, car vous parlez au nom de millions de personnes.

● (0840)

Le président: Merci.

C'est au tour de M. Schiefke. Allez-y, je vous prie.

[*Français*]

M. Peter Schiefke (Vaudreuil—Soulanges, Lib.): Merci beaucoup, monsieur le président.

Je remercie les ministres d'être avec nous aujourd'hui, au Comité.

Monsieur Champagne, en vous appuyant sur votre expérience, puisque vous avez travaillé avec nos partenaires économiques partout dans le monde, y compris les États-Unis et l'Europe, pouvez-vous expliquer au Comité l'importance d'adopter le projet de loi C-26 pour protéger non seulement nos entreprises, mais aussi les entreprises avec lesquelles nous travaillons chaque jour dans le cadre du libre-échange?

L'hon. François-Philippe Champagne: C'est une excellente question, monsieur Schiefke.

Nous ne voulons jamais être vus par les acteurs étatiques et non étatiques comme étant le maillon le plus faible de la chaîne, celui qui attire ce genre d'actes malicieux, qui peuvent nuire aux entreprises canadiennes ou même aux systèmes critiques. Il y a des spécialistes du renseignement et de la sécurité publique qui pourraient vous le dire.

J'essaie toujours de nous comparer aux pays du G7 et de l'Organisation de coopération et de développement économiques, ou OCDE. Comme Canadiens et Canadiennes, nous voulons être parmi les meilleurs et avoir des outils modernes. C'est une question de modernisation, pour moi. Quand j'ai constaté, par exemple, que la Loi sur les télécommunications n'avait pas pour objectif la sécurité, je trouvais que c'était un manque flagrant. Parmi nos alliés, je pense qu'il n'y a pas un pays où le ministre de l'Industrie ou la personne qui est responsable d'un réseau aussi important que celui des télécommunications n'a pas la sécurité pour objectif. C'est essentiel, aujourd'hui. Les gens savent qu'on a besoin de cela.

Le projet de loi que nous proposons va nous permettre d'être à la hauteur des attentes de nos partenaires économiques. Vous avez raison, c'est un pas dans la bonne direction.

M. Peter Schiefke: Merci beaucoup, monsieur le ministre.

[*Traduction*]

Monsieur Leblanc, je vous pose la même question.

Je me réjouis que vous ayez mentionné nos partenaires du Groupe des cinq. Puisque l'interdépendance de nos économies croît de jour en jour, dans quelle mesure est-il important que le Canada contribue aux efforts en matière de cybersécurité, en particulier en ce qui concerne le projet de loi C-26?

L'hon. Dominic LeBlanc: Le projet de loi-cadre avec les mesures mises en place par nos partenaires du Groupe des cinq. Comme je l'ai dit, les ministres de la Sécurité publique des pays du Groupe des cinq ont tenu une réunion virtuelle cette semaine. Il s'agit toujours d'une sorte de point permanent à l'ordre du jour — ce que l'on peut faire face aux cybermenaces. La nature et l'évolution des menaces sont telles que je dirais qu'un seul pays ne pourra pas avoir toutes les bonnes idées et toutes les meilleures pratiques. C'est pourquoi, comme l'a dit M. Champagne... la capacité de travailler avec les pays du G7, en particulier dans le domaine de la sécurité avec nos partenaires du Groupe des cinq... Le MI5 et le MI6 du Royaume-Uni ont effectué de nombreuses recherches dans ce domaine.

Nos alliés américains s'inquiètent évidemment de la montée de la désinformation. Ils sont en pleine année électorale. Il est possible que des acteurs étatiques malveillants puissent crypter ou paralyser les cybersystèmes aux États-Unis et y introduire de la désinformation et des logiciels malveillants. Les principes fondamentaux d'une démocratie dépendent, comme l'a dit M. Champagne, d'une série d'acteurs du secteur privé et du gouvernement pour la transmission élémentaire de l'information.

Le gouvernement du Canada pense que l'adoption du projet de loi nous placera dans une position comparable à celle de nos cinq alliés. Si nous ne sommes pas en mesure, au cours de la présente législature, d'adopter le projet de loi, je pense que cela enverra un signal à nos alliés — en particulier aux États-Unis. J'en parle parce qu'étant donné l'interdépendance de nos économies et de nos industries, que mon collègue connaît mieux que moi, les services de base aux Canadiens, sur lesquels nous comptons au quotidien, seraient, à notre avis, soumis à une menace qui peut être atténuée et contenue.

M. Peter Schiefke: Merci.

Dans la minute et demie qui me reste, je vais poser une question au ministre Champagne.

Lorsqu'il est question du projet de loi, on parle souvent de cybersécurité, bien que la partie 1 du projet de loi soit aussi très importante. Il s'agit de créer des pouvoirs pour sécuriser le réseau, qui a des applications au-delà des cybermenaces, y compris la façon dont nous répondons aux catastrophes naturelles.

C'est important pour ma collectivité, Vaudreuil—Soulanges, et pour beaucoup d'autres collectivités au pays. Dans mon cas particulier, l'année dernière, lors de la tempête de verglas au Québec, je n'ai pas pu téléphoner aux maires et à mes homologues provinciaux pour coordonner une réponse afin d'aider ceux qui n'avaient pas d'électricité et qui étaient coincés chez eux — je parle en particulier de personnes âgées.

Pouvez-vous parler de l'importance d'être en mesure de répondre et de mieux soutenir les Canadiens lorsqu'ils sont dans le besoin?

● (0845)

L'hon. François-Philippe Champagne: Oui, cela se résume à un seul mot: résilience.

L'objectif de la loi est d'assurer la résilience du réseau de télécommunications en particulier. Comme vous l'avez dit, les catastrophes naturelles sont plus fréquentes, plus violentes et se présentent sous différentes formes. Ainsi, qu'il s'agisse d'incendies de forêt, de tempêtes de grêle au Québec ou d'inondations dans le Canada atlantique, nous ne devrions pas considérer le projet de loi uniquement sous l'angle de la sécurité, mais aussi, lorsqu'il s'agit de bon nombre de ces réseaux cruciaux, sous l'angle de la résilience.

Il serait souhaitable qu'un futur ministre de l'Industrie ait certains pouvoirs. Comme je l'ai dit, la dernière fois, à la lumière de ce qui précède, nous avons signé un protocole d'entente. En gros, j'ai réuni les PDG et je leur ai dit qu'il fallait faire mieux — vous devez faire mieux pour protéger les Canadiens. C'est ce que nous avons fait.

Je pense qu'il est sage, pour une nation comme le Canada, d'avoir des lois qui lui permettent de contraindre... et de ne pas compter uniquement sur la bonne volonté des acteurs, ce qui a été fait. Comme vous l'avez dit, pour les personnes dans le besoin, ces systèmes deviennent cruciaux. Lorsqu'il est impossible d'accéder à une ligne téléphonique et qu'il y a une inondation ou une autre catastrophe naturelle, ces pouvoirs permettraient au moins d'imposer certaines mesures. Il appartiendrait évidemment aux fournisseurs de services d'appliquer ces mesures. Au moins, on disposerait d'une sorte de pouvoir, et pas seulement d'un pouvoir souple consistant à se réunir et à formuler des demandes. On pourrait alors obliger les autres à faire quelque chose.

Le président: Je remercie le ministre Champagne et le ministre Leblanc.

C'est maintenant au tour de Mme Michaud. Allez-y, je vous prie.

[*Français*]

Mme Kristina Michaud (Avignon—La Mitis—Matane—Matapédia, BQ): Merci, monsieur le président.

Merci, messieurs les ministres, d'être avec nous ce matin.

D'abord, je veux vous parler d'un texte paru dans *La Presse* intitulé « Quand Ottawa veut jouer au gérant d'estrade ». L'article a paru en 2022, peu de temps après que vous avez déposé le projet de loi C-26. Il faut dire que cela fait un petit moment, soit plus d'un an et demi, que le projet de loi a été déposé. On se dit donc que la cybersécurité n'est peut-être pas une priorité pour le gouvernement du Canada.

L'article a été écrit par Mme Célia Pinto Moreira, qui est analyste en politiques publiques à l'Institut économique de Montréal.

Elle commence son article ainsi: « Imaginez un arbitre qui, lors d'un match du Canadien, va voir un joueur pour lui expliquer comment envoyer la rondelle au filet. Il risquerait fort de perdre son emploi: ça ne fait pas partie de ses tâches ni de son champ de compétences. »

Elle poursuit en disant que c'est pourtant ce qu'Ottawa fait avec le projet de loi C-26. Elle dit: « Au lieu de s'occuper de ses affaires, le gouvernement fédéral veut s'incruster dans la mise en place des plans de sécurité numérique des entreprises. »

Elle ajoute: « En sécurité numérique, les choses vont à vitesse grand V. Lorsqu'une entreprise trouve une faille dans son système, elle sait pertinemment qu'elle a tout intérêt à la réparer rapidement, sans quoi elle s'expose à des risques juridiques, réputationnels et financiers importants [...] »

Elle dit ensuite que le gouvernement fédéral est peu rapide ou peu efficace en citant la saga des passeports.

On se rappelle cette saga. Cela fait un petit bout de temps. On peut aussi penser à Phénix, à Canada Vie, à la frontière. Je pense que le gouvernement a été peu efficace et peu rapide dans ces situations.

En somme, on peut penser que les entreprises canadiennes sont bien préparées à l'heure actuelle. Elles doivent déjà faire face à des incidents de cybersécurité. On dit qu'en 2021, les entreprises canadiennes ont investi plus de 10 milliards de dollars pour se préparer à ce type d'incident. Elles font donc déjà le travail.

Concrètement, pour les entreprises canadiennes, qu'est-ce que le projet de loi C-26 vient changer?

L'hon. François-Philippe Champagne: Je vous remercie de votre question, madame Michaud, et je remercie aussi la personne qui a écrit l'article.

Je vais vous donner un exemple qui, d'après moi, va répondre à votre question.

Vous savez que prévenir le préjudice est aussi le rôle du gouvernement. Rappelez-vous le cas de Rogers. Il y a eu 12 millions de Canadiens et de Canadiennes qui ont perdu l'accès aux services de télécommunications, ce qui les empêchait même de faire des paiements, car les services Interac étaient connectés au réseau de Rogers.

Dans ce cas, le gouvernement a été rapide. Je pense que j'étais au Japon, mais j'ai parlé au président-directeur général, ou PDG, de Rogers dans les heures qui ont suivi pour lui demander de prendre des mesures très concrètes. D'un côté, vous pouvez dire que Rogers est une grande société qui investit probablement des centaines de millions de dollars dans la cybersécurité, mais de l'autre côté, 12 millions de Canadiens et de Canadiennes n'ont pas eu de services de télécommunication pendant des heures.

À ce moment-là, j'ai interpelé non seulement le président-directeur général de Rogers, mais l'ensemble des PDG des principales entreprises de télécommunication en leur disant qu'ils devaient tous, ce jour-là, utiliser leurs équipes pour aider Rogers. Ce n'était plus une question de concurrence, mais une urgence, parce que des Canadiens et des Canadiennes ne pouvaient plus aller à l'épicerie ou mettre de l'essence dans leur véhicule. Leurs cartes de paiement ne fonctionnaient plus.

Vous allez me dire qu'il devrait y avoir de la résilience dans le système. Or, dans les audiences par la suite, on s'est rendu compte que, curieusement, il n'y avait pas autant de résilience ou de redondance dans le système qu'on le pensait. Tout le monde disait pourtant que l'opérateur des cartes Interac devait évidemment avoir un système de secours.

Je pense que les faits ont démontré que des choses devaient être améliorées. Je pense aussi que le gouvernement a le rôle d'assurer l'intérêt public.

Vous avez raison de dire que la plupart des entreprises le font bien, mais je pense que le cas de Rogers est un bel exemple du rôle que joue le gouvernement. À l'époque, on l'a fait de façon volontaire. D'ailleurs, je remercie les diverses entreprises d'avoir voulu apporter leur aide. Elles ont même signé un protocole d'entente à ce sujet. Le nombre de pages qu'il comporte prouve qu'il y avait beaucoup de choses à faire.

Je pense que, dans l'avenir, s'il y avait une situation urgente semblable, le fait d'avoir des pouvoirs dans le coffre à outils et de pouvoir dire à des entreprises qu'elles n'ont pas fait leur travail et que cela a nui à des Canadiens et à des Canadiennes, ce serait bien. Je pense que c'est justifié.

● (0850)

Mme Kristina Michaud: Merci, monsieur le ministre. Je sais que vous pouvez parler longtemps d'un sujet qui vous passionne, mais nous avons peu de temps.

Dans ce projet de loi, ce qui me marque, c'est qu'on donne énormément de pouvoirs au gouverneur en conseil et au ministre de l'Industrie, donc à vous. Vous me paraissez être un homme digne de confiance. Si vous faites tout cela dans le secret, cela peut se passer très bien, mais il y a des Canadiens qui ont des craintes, il y a des Québécois qui sont inquiets. Des questions de transparence sont soulevées.

Pouvez-vous nous expliquer pourquoi tout cela doit se passer dans le secret absolu et ce que cela peut représenter pour les petites ou moyennes entreprises?

Vous avez parlé de grandes entreprises, comme Bell et Rogers, qui peuvent se permettre de se voir infliger une amende de quelques millions de dollars par le gouvernement si elles ne se conforment pas aux exigences.

Par contre, qu'est-ce que cela représente pour une petite entreprise québécoise? Vous connaissez l'importance des petites ou moyennes entreprises pour l'économie québécoise.

Qu'est-ce que cela représente pour une petite entreprise de télécommunication qui a quelques centaines ou quelques milliers d'abonnés et qui n'offre ses services que sur une partie du territoire?

Qu'en est-il pour cette entreprise qui n'a pas la main-d'œuvre nécessaire pour mettre en place un plan de sécurité qui serait conforme à votre plan? Va-t-elle recevoir une amende de quelques millions de dollars?

Quels sont les pouvoirs que vous pouvez exercer? Des gens nous disent qu'ils peuvent lire, dans le résumé législatif, que le ministre de l'Industrie peut prendre des décrets et des arrêtés, mais qu'ils ne savent pas ce que c'est.

Pouvez-vous nous expliquer tout cela?

L'hon. François-Philippe Champagne: Je vous remercie de la confiance que vous me témoignez. Je vous en suis reconnaissant.

J'aimerais dire deux choses à ce sujet.

D'abord, j'aimerais dire que c'est soumis au contrôle judiciaire. On en a parlé, et le ministre LeBlanc l'a évoqué plus tôt. Je ne veux pas faire l'avocat devant le Comité, mais, comme vous le savez, dans le cas d'un contrôle judiciaire, il y a une question de proportionnalité dans les mesures qui sont prises.

Ensuite, il y a une raison pour laquelle, en matière de sécurité nationale, certaines de ces directives doivent être secrètes. Je vais vous donner un exemple et vous comprendrez tout de suite le problème. Si nous trouvons une faille dans un système, évidemment, nous ne voulons pas que les acteurs étatiques et non étatiques en profitent avant que nous ayons pu la réparer. C'est ce à quoi nous nous exposerions si nous publiions l'ensemble de nos directives.

Prenons le cas d'une cyberattaque. Quand il s'agit de la technologie 5G, surtout, cela va être décentralisé. Le maillon le plus faible de la chaîne pourrait être attaqué. Je pense que c'est dans l'intérêt de l'entreprise, de l'organisation et des Canadiens que nous puissions dans une telle situation donner une directive secrète et confidentielle pour indiquer ce qui doit être réparé.

Comme nous le disions, il y aura une rétroaction. Nous pourrons faire état de la situation. Il faut savoir que, dans nos démocraties, le problème, c'est que des acteurs étatiques et non étatiques qui veulent nuire au pays ne jouent pas selon les mêmes règles que nous. Alors, si je publie une information qui indique que le maillon le plus faible de notre système se trouve dans tel système ou tel service de télécommunication, j'invite quasiment les gens malveillants avant que nous ayons eu le temps de réparer cette brèche dans notre système.

Je pense que cela exposerait l'ensemble du réseau à un risque. C'est pour cela que, dans certains cas, nous devrons garder cette information secrète et confidentielle pour protéger la sécurité nationale.

[*Traduction*]

Le président: Merci.

C'est maintenant au tour de M. Julian.

[*Français*]

M. Peter Julian (New Westminster—Burnaby, NPD): Merci beaucoup, monsieur le président.

Je remercie les ministres d'être avec nous. Ils sont toujours les bienvenus au Comité.

Nous aimerions beaucoup vous voir plus souvent, monsieur LeBlanc, devant le Comité.

● (0855)

L'hon. Dominic LeBlanc: Pas autant que moi, monsieur.

M. Peter Julian: Comme vous l'avez si bien dit plus tôt, c'est une question d'importance nationale. Nous savons que le nombre de cyberattaques augmente sans cesse.

Le gouvernement a déposé ce projet de loi en juin 2022, et nous sommes encore en train de l'étudier. Tout se passe très lentement. Nous sommes en 2024, et ce projet de loi n'a pas été adopté.

Pourquoi le gouvernement ne semble-t-il pas considérer que c'est une priorité, alors que nous savons que c'est un problème monumental?

L'hon. Dominic LeBlanc: Monsieur le président, je remercie mon ami et collègue M. Julian de la question.

Je reconnais que cela n'a pas progressé aussi vite que nous l'aurions souhaité.

Monsieur Julian, vous êtes leader parlementaire et vous savez que, souvent, le processus parlementaire peut être ralenti par d'autres questions à certains moments. Je n'utilise pas du tout cela comme prétexte. Je reconnais que nous aurions aimé que le projet de loi soit adopté avant 2024, c'est sûr. Je ne suis pas en désaccord avec vous.

Nous sommes prêts à faire tout ce que nous pouvons faire, y compris travailler avec ce comité sur des amendements et nous assurer que toutes les ressources de nos ministères sont disponibles pour vous aider à avancer si le Comité décide d'aller de l'avant.

J'accepte cette critique de bonne foi. Je reconnais que c'est urgent, et nous allons faire de notre mieux. Je ne vais pas vous rappeler que je suis ministre de la Sécurité publique seulement depuis le mois de juillet. Nous avons travaillé ensemble, vous et moi, au cours de l'été. Vous êtes au courant de cela.

M. Peter Julian: Merci.

Je vais passer à une autre question.

[*Traduction*]

Au cours de son témoignage, M. John de Boer, de BlackBerry, a déclaré que, de septembre à décembre de l'année dernière, il y a eu plus de 5,2 millions de cyberattaques, dont 62 % visaient des infrastructures essentielles. L'Association des banquiers canadiens nous a dit que le nombre de cyberattaques de priorité 1 avait triplé au cours de l'année dernière.

Le gouvernement — le ministère de la Sécurité publique et celui de l'Industrie — suit-il le nombre de cyberattaques dans tous les secteurs? Disposez-vous de ces renseignements? À ce jour, nous n'avons pas été en mesure de consolider le nombre d'attaques par secteur. En fait, de nombreux témoins nous ont dit qu'ils ne recueillaient tout simplement pas ces données.

L'hon. Dominic LeBlanc: Je vous remercie d'avoir relevé ce que nous pensons être l'un des éléments positifs du projet de loi, à savoir l'obligation de faire rapport. Nous reconnaissons la bonne foi d'un grand nombre des importantes entités privées qui collaborent avec le gouvernement du Canada, mais leur bon vouloir n'est probablement pas suffisant. L'obligation véritable de faire rapport garantirait que nous disposions de données fiables et précises sur l'augmentation alarmante que vous soulevez.

Comme je l'ai mentionné au début, le Centre de la sécurité des télécommunications serait l'agence fédérale qui serait en mesure de rassembler ces données et de les communiquer à l'ensemble du gouvernement. Lors de séances d'information offertes par le ministère de la Sécurité publique et le directeur du Service canadien du renseignement de sécurité, entre autres, on m'a confirmé cette tendance alarmante.

Monsieur Boucher, vous avez peut-être des détails sur les données qui sont recueillies par notre ministère ou le Centre de la sécurité des télécommunications. Pourriez-vous fournir brièvement ces informations à M. Julian?

M. Patrick Boucher (sous-ministre adjoint principal, Secteur de la sécurité et de la cybersécurité nationale, ministère de la Sécurité publique et de la Protection civile): Pour ajouter à ce que le ministre LeBlanc a dit, à l'heure actuelle, tous les signalements sont faits sur une base volontaire. C'est formidable quand les gens le font, mais il y a évidemment des lacunes à cet égard. L'un des éléments fondamentaux de ce projet de loi, comme l'a dit le ministre LeBlanc, consiste à veiller à régulariser les signalements afin que le Centre de la sécurité des télécommunications puisse recevoir toute l'information pertinente, mettre à profit les conseils de ses experts et diffuser les constatations afin de renforcer parallèlement la résilience dans d'autres secteurs.

M. Peter Julian: Merci, mais là n'était pas ma question. Je comprends tout à fait comment le projet de loi C-26 vise à corriger ce problème. Ce que je demande, c'est quels sont les chiffres actuels? Avez-vous des chiffres à nous communiquer, même s'ils ont été transmis de façon volontaire, qui peuvent donner un aperçu de l'étendue et de la portée des cyberattaques au Canada?

M. Patrick Boucher: Nous pouvons certainement nous informer auprès de nos partenaires du Centre de la sécurité des télécommunications, un organisme qui relève du ministère de la Défense nationale, pour savoir s'il existe des données facilement accessibles à ce sujet.

M. Peter Julian: Cela serait très utile pour le Comité.

L'hon. Dominic LeBlanc: Je me ferai un plaisir de veiller à ce que nous obtenions ces informations le plus rapidement possible afin de les transmettre au Comité.

M. Peter Julian: Je vous remercie.

Monsieur LeBlanc, parmi vos dossiers, il y a celui de l'ingérence étrangère dans notre processus électoral. Nous avons parlé du Centre de la sécurité des télécommunications. À la fin de l'année dernière, cet organisme a sonné l'alarme sur le fait que les cybermenaces émanant de la Russie, de la Chine — et je pense que nous pouvons ajouter à cela des soupçons à l'égard de l'Inde — prennent diverses formes, notamment des tentatives de lancer des attaques contre les sites Web des autorités électorales, d'accéder aux renseignements personnels des électeurs ou à l'information relative aux élections, et de rechercher les vulnérabilités des systèmes électoraux en ligne.

Nous savons à quel point les conséquences de l'ingérence étrangère ont été dommageables aux États-Unis, lors de l'élection de Donald Trump, ainsi qu'au Royaume-Uni, lors du référendum sur le Brexit. En quoi le projet de loi C-26 renforcerait-il notre système électoral et notre démocratie pour nous protéger contre les cyberattaques comme celles qui ont eu un impact si tangible dans d'autres démocraties?

● (0900)

L'hon. Dominic LeBlanc: Je partage votre inquiétude. Je pense que vous avez tout à fait raison en ce qui concerne le risque. Comme je l'ai mentionné, les États-Unis sont dans une année électorale, de sorte que les mêmes acteurs qui — d'après ce que nous savons — ont connu un certain succès en 2016 seront à nouveau à l'œuvre cette année. C'est un sujet de discussion pour un autre comité, mais des amendements à la Loi électorale du Canada pourraient être proposés dans les semaines à venir. Le fait que nous ayons un système de bulletins de vote en papier est, selon le directeur général des élections, l'un des meilleurs moyens de sécuriser notre système de vote.

Nous sommes en communication avec le directeur général des élections et nous suivons ses conseils et ses recommandations. À mon avis, ce projet de loi contribuerait à renforcer notre système électoral si, par exemple, la Loi électorale du Canada permettait aux gens de demander en ligne un bulletin de vote postal — ce n'est qu'un exemple qui me vient à l'esprit —, car ces demandes passeraient par les canaux de télécommunications des particuliers, des entreprises privées auxquelles mon collègue a fait allusion. Ce n'est pas un système d'Élections Canada en soi, mais il est essentiel pour que les gens aient accès à la démocratie. Donc, si nous voulons rendre le vote plus accessible en 2024 ou 2025, il faudra nécessairement passer par Internet et les systèmes de télécommunications.

Le vote en tant que tel se fait avec un bulletin de vote en papier, mais Élections Canada est très préoccupé par cette question. Nous avons investi dans ce domaine et nous avons permis au Centre de la sécurité des télécommunications de collaborer avec Élections Canada pour renforcer les systèmes. Comme mon collègue le sait, des fonctionnaires du gouvernement du Canada sont à la disposition des partis politiques pour les aider à sécuriser leurs systèmes. C'est une source de préoccupation commune et nous sommes prêts à faire tout ce qui est en notre pouvoir à cet égard.

Le président: Merci.

Nous passons maintenant au second tour.

Monsieur Lloyd, vous avez la parole pour cinq minutes.

M. Dane Lloyd (Sturgeon River—Parkland, PCC): Merci, monsieur le président.

Je remercie les témoins de leur présence aujourd'hui.

Messieurs les ministres, renforcer la résilience face aux catastrophes naturelles, renforcer la résilience face aux menaces à la cybersécurité, voilà des enjeux que tous les Canadiens et tous les partis peuvent, je pense, soutenir. Nous savons qu'il faut investir davantage dans la cybersécurité et la résilience, mais les deux ministres ont dit quelque chose aujourd'hui et cela m'a fait réfléchir. Quand ces ministres disent que ce projet de loi vise à donner au gouvernement des « pouvoirs d'urgence » et des « pouvoirs extraordinaires » — je reprends leurs termes —, je pense que c'est très inquiétant pour les Canadiens qui veulent savoir pourquoi le gouvernement a besoin de tels pouvoirs alors que le but, en fait, est d'essayer de renforcer la résilience contre les catastrophes naturelles et d'inciter les entreprises à investir davantage dans la cybersécurité. Pourquoi le gouvernement a-t-il besoin d'une mesure législative qui lui donne le pouvoir de recourir aux tribunaux, d'annoncer des lois ou d'empêcher des personnes de faire partie du secteur des télécommunications, tout cela en secret? Pourquoi ces pouvoirs d'urgence sont-ils nécessaires alors que nous devons investir davantage dans la cybersécurité?

L'hon. François-Philippe Champagne: C'est un plaisir de répondre à votre question.

Tout d'abord, je vous remercie d'avoir dit qu'il ne s'agissait pas d'une question partisane. Je pense, comme vous l'avez souligné, que nous essayons tous de faire ce qu'il y a de mieux.

Je vais vous donner un exemple très concret. En ce qui concerne le réseau 5G, je pense que tout le monde est d'accord pour dire que ce sera très décentralisé. Quand l'on passe de la 4G à la 5G, c'est un univers différent. Ces deux réseaux sont différents l'un de l'autre. L'avenir nous amène vers des produits intelligents, de sorte que tout sera interconnecté. Si, par exemple, l'on détectait une défaillance ou une intrusion dans le réseau et que celle-ci risquait d'entraîner des répercussions dans tout le réseau, vous voudriez qu'à l'avenir le ministre de l'Industrie soit en mesure de dire à l'auteur de cette intrusion d'arrêter sa démarche, ou encore, de déconnecter cette personne ou cette entité de l'ensemble du réseau. Pour agir ainsi, il faut un pouvoir qui permet d'agir très rapidement, parce que l'on parle de...

M. Dane Lloyd: Monsieur le ministre, pourquoi le recours aux tribunaux en secret est-il nécessaire?

L'hon. François-Philippe Champagne: Je vais vous le dire. C'est très simple, parce que vous ne voudriez pas que les auteurs, ceux qui essaient d'infiltrer notre système, soient au courant que vous leur demandez de colmater la brèche...

M. Dane Lloyd: Quelles mesures de sauvegarde allez-vous mettre en place pour que ce pouvoir ne soit pas utilisé de manière abusive? De nombreux témoins nous ont fait part de leurs inquiétudes concernant ces pouvoirs, que vous avez qualifiés de « pouvoirs d'urgence ». C'est très inquiétant.

L'hon. François-Philippe Champagne: Les gens devraient être tout aussi préoccupés par le fait qu'aujourd'hui — à titre d'exemple — le ministre de l'Industrie n'a pas le pouvoir de demander à une entité en particulier de colmater la brèche de son système qui crée une vulnérabilité susceptible d'avoir un effet dans tout le réseau, risquant ainsi d'affecter des millions de Canadiens. En tant qu'avocat, je dirais que le contrepoids de ces pouvoirs serait assuré par un contrôle judiciaire. Il ne faut pas oublier que dans le cadre d'un contrôle judiciaire, le principe de la proportionnalité et la Charte des droits et libertés entrent en ligne de compte. Tous les projets de loi et mesures législatives s'appliquent.

● (0905)

M. Dane Lloyd: Le commissaire à la protection de la vie privée a déclaré que ce projet de loi n'incluait pas le principe de la proportionnalité. Que pouvons-nous faire pour inclure le principe de la proportionnalité dans ce projet de loi?

L'hon. François-Philippe Champagne: Je dirais que, dans le cadre d'un contrôle judiciaire, comme vous le savez, il est bien établi dans la jurisprudence que le gouvernement doit tenir compte du principe de la proportionnalité dans sa démarche, mais je pense qu'il faut voir cela d'une manière positive. Imaginez l'inverse; si, en l'absence de ce pouvoir, quelqu'un s'infiltrait quelque part dans le réseau et que cela entraînait des effets dommageables dans tout le réseau et pour des millions de Canadiens, tant sur le plan économique que sur d'autres plans. Pensez à l'inverse.

M. Dane Lloyd: Merci de votre réponse, monsieur le ministre.

Monsieur LeBlanc, au cours des dernières années, le Canada a été confronté à un problème important: près de 100 églises ont été incendiées ou attaquées à l'échelle du pays, la plus récente étant l'église Blessed Sacrament, à Regina. Avant Noël, quatre églises ont été incendiées en Alberta. En tant que ministre de la Sécurité publique, vous n'avez fait aucune déclaration pour dénoncer ces attaques. Je veux simplement vous donner l'occasion, aujourd'hui, de dire au peuple canadien, à la communauté chrétienne et aux autres groupes confessionnels que vous dénoncez ces attaques contre les églises au Canada.

L'hon. Dominic LeBlanc: Bien sûr, notre gouvernement, et moi-même, personnellement, et nous tous, dénonçons ce qui est une augmentation alarmante des attaques contre les communautés religieuses et culturelles. Je discute souvent avec le commissaire de la Gendarmerie royale du Canada de ce que nous pouvons faire en tant que force de police nationale, en collaboration avec les polices locales et provinciales, pour mieux protéger les communautés, y compris les exemples que notre collègue a identifiés. Nous sommes préoccupés par l'augmentation alarmante des discours et des crimes haineux. Je suis donc heureux de joindre ma voix à tous ceux qui dénoncent ces incidents particuliers.

M. Dane Lloyd: Je vous remercie, monsieur le ministre. Je suis toutefois préoccupé par le fait que les services placés sous votre contrôle — le Service canadien du renseignement, par exemple — n'ont pas abordé ce sujet. Il s'agit d'une menace à l'échelle du Canada et, dans certains cas, je pense qu'elle atteint le seuil du terrorisme. Que fait le gouvernement pour mettre fin à ces actes terroristes contre les groupes confessionnels dans notre pays? Que faites-vous, monsieur le ministre?

L'hon. Dominic LeBlanc: Je collabore chaque jour avec la GRC et d'autres partenaires du secteur de la sécurité pour m'assurer que nous disposons des outils nécessaires pour bien protéger les Canadiens. La décision de considérer un acte comme un acte terroriste n'est pas une décision politique: ce travail est entre les mains des procureurs, des enquêteurs, de la police nationale et des polices locales partenaires. Cela dit, nous savons qu'en raison de l'augmentation du nombre de crimes haineux, la GRC doit collaborer avec les forces policières locales afin de comprendre la nature de la menace et de s'assurer que la police locale et la GRC — dans le cas du crime organisé transnational — disposent des outils dont elles ont besoin pour protéger les Canadiens.

Le président: Merci.

Nous passons maintenant à Mme O'Connell.

Mme Jennifer O'Connell (Pickering—Uxbridge, Lib.): Je vous remercie, monsieur le président.

Messieurs les ministres, merci de votre présence parmi nous.

Il a beaucoup été question de la protection des renseignements personnels et des inquiétudes à cet égard; c'est un sujet dont les témoins ont beaucoup parlé. Je pense que le député d'en face a mal rapporté les propos du commissaire à la protection de la vie privée. Cela dit, le gouvernement avait clairement l'intention, dans ce cas, d'établir des bases législatives dans le projet de loi C-26 puis de régler certains des détails au moyen de la réglementation. Le commissaire à la protection de la vie privée a dit vouloir participer à l'élaboration de la réglementation pour s'occuper spécifiquement des enjeux concernant la protection des renseignements personnels, de détails à propos des PME et de communautés autochtones qui pourraient avoir besoin d'aide et d'un travail de fond pour mettre en oeuvre les objectifs visés. Pourriez-vous nous dire comment on compte utiliser la réglementation et le travail du commissaire à la protection de la vie privée pour régler des préoccupations liées à la protection des renseignements personnels?

L'hon. Dominic LeBlanc: De toute évidence, aucun élément du projet de loi à l'étude ne modifierait l'applicabilité de la Loi sur la protection des renseignements personnels. Comme je l'ai dit dans ma déclaration préliminaire, si nous pouvons aider des secteurs qui font partie des infrastructures essentielles de l'économie canadienne — par exemple les banques et les entreprises de télécommunication —à rendre leurs systèmes plus sûrs, si nous nous entraidons en nous appuyant bien sûr sur le Centre de la sécurité des télécommunications, ce sera aussi une façon de nous protéger contre les atteintes à la vie privée et à la confidentialité des renseignements personnels.

Je repense aux conversations que j'ai eues avec le premier ministre Furey de Terre-Neuve-et-Labrador quand des personnes utilisant un rançongiciel ont exporté les données d'une autorité sanitaire desservant de 40 à 50 % de la population de la province. Vous pouvez imaginer à quel point les résidants de la province se sentaient vulnérables. Cette situation a été résolue avec l'aide du Centre de la sécurité des télécommunications. Si le projet de loi peut, d'une certaine manière, encourager — pour employer un terme poli — les entreprises du secteur privé à faire tout en leur pouvoir pour assurer la sécurité des données, ou les y « contraindre », pour utiliser un autre mot, ce sera aussi important, à notre avis.

Comme je l'ai déjà dit, madame O'Connell, ce serait un plaisir de répondre spécifiquement à la question des amendements, de collaborer avec le commissaire à la protection de la vie privée et d'entendre d'autres experts en la matière. Nous respectons l'application de la Charte des droits, de la Loi sur la protection des renseignements personnels et d'autres mesures législatives importantes. Nous croyons que, fait correctement, le projet de loi à l'étude contribuera à améliorer et à protéger la confidentialité des renseignements personnels des Canadiens. Nous envisageons avec plaisir les délibérations du Comité de même que la participation du commissaire à la protection de la vie privée, bien sûr. Son point de vue nous sera essentiel pour arriver à un juste équilibre.

● (0910)

Mme Jennifer O'Connell: Certains laissent entendre qu'il existerait des tribunaux secrets, mais quand il est question d'enjeux concernant la sécurité nationale, tous les gouvernements ont déjà recours aux lois en vigueur — comme la Loi sur le Service canadien du renseignement de sécurité —, à des contrôles judiciaires et au processus judiciaire. Le projet de loi va-t-il au-delà de ce qui existe déjà dans les lois canadiennes, pour ce qui est de protéger la sécurité nationale tout en permettant que se déploie le processus judiciaire, pour garantir qu'aucun gouvernement n'outrepasse les pouvoirs législatifs?

L'hon. Dominic LeBlanc: C'est une bonne question. Vous avez aussi siégé au Comité des parlementaires sur la sécurité nationale et le renseignement. Vous avez donc pu être informée de certains des dangers qui menacent la sécurité nationale. Vous connaissez aussi les processus prévus par la Loi sur le Service canadien du renseignement de sécurité, le SCRS, que vous avez mentionnée. À titre d'exemple, en tant que ministre, je signe les mandats du SCRS. Ils sont examinés, à juste titre, par la Cour fédérale du Canada, lors d'audiences à huis clos tenues en présence d'un amicus curiae.

Je comprends. Je suis député depuis un certain temps. L'expression « tribunaux secrets » sonne bien dans un clip. Elle ne correspond à rien de nouveau ou de différent, mais c'est une expression chargée qui vise à provoquer des réactions.

Il est question ici d'un juste équilibre semblable à celui d'autres mesures législatives que vous avez mentionnées; de toute évidence, les décisions peuvent faire l'objet d'un contrôle judiciaire au besoin.

M. Champagne souhaite ajouter quelques mots.

L'hon. François-Philippe Champagne: Je souhaite revenir à des idées fondamentales en lien avec ce qu'a dit un collègue. Le ministre de l'Industrie a le pouvoir « de prendre des mesures pour promouvoir la sécurité du système canadien de télécommunication ». Certains disent qu'il s'agit de vastes pouvoirs. Rappelons, toutefois, que ces pouvoirs visent un objectif très clair et sont plutôt ciblés: il s'agit de promouvoir la sécurité du système canadien de télécommunication. Par conséquent, dans le cadre d'un contrôle judiciaire sous la supervision de la cour, les gens examineraient quel était l'objectif et si les mesures prises concordaient avec l'objectif, c'est-à-dire la sécurité du réseau. Je crois que cela limite les pouvoirs accordés par la loi, dans une optique d'agir très rapidement. Il s'agit d'un objectif très spécifique.

Le président: Merci.

Nous passons maintenant à Mme Michaud, qui dispose de deux minutes et demie.

[*Français*]

Mme Kristina Michaud: Merci, monsieur le président.

Messieurs les ministres, je vais être honnête avec vous, mais je pense que c'est quelque chose que vous savez déjà. Au Bloc Québécois, ce que nous aimons faire à l'occasion de l'étude d'un projet de loi, c'est de nous assurer que les champs de compétence des provinces et du Québec sont bien respectés.

Il y a quand même une crainte relativement au projet de loi C-26. Des dirigeants d'Électricité Canada sont venus témoigner devant ce comité, et ils nous ont fait part de cette crainte. Il faut dire que le projet de loi C-26 inclut les réseaux de lignes électriques interprovinciales et internationales dans sa liste de systèmes critiques. On peut comprendre, entre les lignes, qu'une organisation comme Hydro-Québec, par exemple, pourrait être visée par ce projet de loi. Vous me direz si je me trompe.

Les dirigeants d'Électricité Canada se sont dits désireux de voir apporter certains amendements à ce projet de loi pour éviter les dédoublements, les chevauchements ou les doubles emplois avec les compétences des agences provinciales qui sont déjà parties prenantes.

Par exemple, Hydro-Québec, une organisation qui fait la fierté des Québécois, pourrait recevoir une pénalité financière pouvant aller jusqu'à 15 millions de dollars si elle ne se conformait pas, pour une raison ou une autre, à certains décrets ou arrêtés ministériels.

Est-ce bien ce qu'il faut comprendre?

Qu'est-ce que le projet de loi C-26 représente pour Hydro-Québec, par exemple?

● (0915)

L'hon. Dominic LeBlanc: Monsieur le président, je remercie Mme Michaud de sa question.

Hydro-Québec ne devrait pas faire la fierté des Québécois et des Québécoises seulement, mais bien de tous les Canadiens. Je partage l'enthousiasme de ma collègue à l'égard de cette institution très importante pour le pays.

J'ai discuté de la question avec le ministre du Québec qui est responsable de la cybersécurité. Nous avons eu une bonne discussion. Il a soulevé exactement les mêmes inquiétudes que celles soulevées par Mme Michaud. Évidemment, nous voulons respecter les champs de compétence du gouvernement du Québec, mais la loi donne aussi au gouvernement du Canada certaines compétences dans certains secteurs de l'économie. Nous voulons aussi que nos champs de compétence soient respectés. Vous avez parlé d'Hydro-Québec, et il y aura évidemment des zones d'intersection.

Personnellement, je pense qu'il faut collaborer avec le gouvernement du Québec. Les objectifs du gouvernement du Québec sont les mêmes que les nôtres. J'ai été impressionné par les efforts de mon homologue québécois quant à la sécurisation des systèmes critiques au Québec. Encore une fois, le Québec sert d'exemple pour le reste du Canada.

Nous n'allons pas chercher la chicane, c'est certain. Nous allons essayer de travailler en étroite collaboration avec le gouvernement du Québec, mais nous allons assumer notre responsabilité à l'échelle nationale, sans que cela enlève quoi que ce soit aux gouvernements provinciaux.

Le Centre canadien pour la cybersécurité, du ministère de la Défense nationale, est probablement un chef de file national. Nous allons devoir collaborer avec les provinces et communiquer nos connaissances et nos compétences avec nos homologues des provinces.

[*Traduction*]

Le président: Merci.

M. Julian a maintenant la parole pour deux minutes et demie.

M. Peter Julian: Je vous remercie, monsieur le président.

Une coalition de groupes nationaux, comprenant notamment l'Association canadienne des libertés civiles, la Ligue des droits et libertés, et le Conseil du Canada de l'accès et de la vie privée, a critiqué le projet de loi tout en proposant des solutions concrètes.

Comme il est clair, pour les membres de cette coalition, que le projet de loi C-26 limiterait l'accès des demandeurs aux éléments de preuve, l'une des solutions proposées serait de créer un rôle d'avocat spécial, afin que les éléments de preuve puissent être examinés dans un tribunal de droit sans être divulgués à des tiers. Cette recommandation s'inspire, bien sûr, des dispositions de la Loi sur l'immigration et la protection des réfugiés.

J'aurais deux questions pour vous, monsieur LeBlanc, au sujet de l'idée d'avoir recours à un avocat spécial. Premièrement, pourquoi le gouvernement n'a-t-il pas envisagé, dès le départ, de créer un rôle d'avocat spécial dans le projet de loi? Deuxièmement, le projet de loi comporte des failles importantes. Le gouvernement est-il maintenant favorable à l'idée de l'améliorer en créant un rôle d'avocat spécial?

L'hon. Dominic LeBlanc: Nous avons pris note de la suggestion que vous mentionnez à juste titre.

Je n'ai vraiment pas une connaissance approfondie de cet aspect de la législation sur la sécurité nationale. Vous avez toutefois parlé d'exemples tirés de la Loi sur l'immigration et la protection des réfugiés, selon lesquels ces avocats spéciaux seraient en mesure de participer aux audiences à huis clos et d'avoir accès aux renseignements appropriés.

Je sais que, dans le contexte du SCRS, des amicus curiae peuvent participer aux audiences de la Cour fédérale. Nous verrions donc d'un bon œil que le Comité propose des suggestions ou des amendements afin que nous arrivions à un juste équilibre. Nous n'aurions décidément pas d'objection de principe si le Comité décidait, dans sa grande sagesse, d'ajouter un amendement qui pourrait, je l'espère, répondre à certaines de ces préoccupations tout à fait légitimes. Nous serions favorables à ce genre de démarche.

Je ne sais pas pourquoi on n'a pas prévu une telle disposition dès le départ, mais je serai ravi de collaborer avec des collègues si ce point est considéré comme un oubli ou une erreur qu'il est possible de corriger. Je suis heureux d'accepter cette suggestion dans un esprit de collaboration.

M. Peter Julian: Je vous remercie.

Comme Mme Michaud l'a rappelé il y a un instant, il a été question, pendant le témoignage d'Électricité Canada, du fait que la coopérative nord-américaine de l'énergie, la NERC, est déjà assujettie à divers règlements et qu'on se demande comment le projet de loi C-26 viendra ajouter aux exigences. Électricité Canada recommande d'éviter les chevauchements de règlements ou d'exigences.

Dans quelle mesure le gouvernement a-t-il consulté des groupes de l'industrie, comme la NERC, pendant l'élaboration du projet de loi? Le gouvernement est-il ouvert à l'idée de favoriser une meilleure harmonisation entre les dispositions du projet de loi C-26 et les règlements déjà mis en œuvre par les groupes de l'industrie?

● (0920)

Le président: Monsieur Julian, votre temps de parole est écoulé. J'ai été plus que généreux.

Nous passons maintenant à M. Lloyd.

M. Dane Lloyd: Merci, monsieur le président.

Monsieur le ministre LeBlanc, le projet de loi C-26 porte sur la cybersécurité. Nous savons que le gouvernement du Canada dispose de capacités limitées dans le domaine des technologies de l'information et qu'il dépend souvent d'entrepreneurs et de consultants. Nous avons appris hier que votre gouvernement avait accordé à GC Strategies des contrats dont la valeur s'élève à 258 millions de dollars.

Cette entreprise de TI composée de deux personnes travaillant chez elles a-t-elle obtenu de votre ministère des contrats liés à la cybersécurité ou aux dispositions du projet de loi?

L'hon. Dominic LeBlanc: De toute évidence, comme nous l'avons déjà dit, cette entreprise suscite de vives préoccupations. Tous les contrats conclus avec elle sont suspendus depuis l'automne dernier. Des audits internes et des enquêtes sont en cours à l'Agence des services frontaliers du Canada. Je sais que le Conseil du Trésor et le ministère de l'Approvisionnement examinent aussi cette situation.

Je n'ai pas connaissance de contrats liés à la cybersécurité qui auraient été conclus entre cette entreprise et le ministère de la Sécurité publique. Il y a des éléments bien connus à l'Agence des services frontaliers. Je serai heureux de voir à ce que le Comité reçoive les renseignements demandés.

Tout cela fait partie des enquêtes internes en cours. Comme nous l'avons dit, s'il y a eu des comportements inappropriés, ils pourront mener à des sanctions sévères, de toute évidence.

M. Dane Lloyd: Merci.

On sait que l'ASFC a accordé 134 contrats à cette entreprise. Certains de ces contrats ont-ils un lien avec la cybersécurité au Canada?

L'hon. Dominic LeBlanc: Je crois que l'Agence des services frontaliers a apporté des précisions au sujet du nombre de contrats que vous mentionnez. Elle a précisé que le chiffre en question faisait référence aux modifications apportées à des contrats. Le nombre de contrats est beaucoup plus bas. Je le répète, je serai heureux de transmettre au Comité des renseignements sur la participation de cette entreprise à des mandats sur la cybersécurité.

C'est un point qui nous préoccupe, bien sûr, et il fait l'objet des enquêtes internes que j'ai mentionnées; je ne cherche pas à en diminuer l'importance. J'ai d'ailleurs parlé de cette série d'enjeux avec la présidente de l'ASFC ce matin. Je serai heureux de transmettre au Comité les renseignements demandés.

M. Dane Lloyd: Merci. Vous engagez-vous, monsieur le ministre, à fournir ces renseignements au Comité?

L'hon. Dominic LeBlanc: Je m'y engage. Il s'agit de comprendre la nature des contrats dans le cadre desquels cette entreprise a pu travailler sur des questions de cybersécurité.

M. Dane Lloyd: Merci.

Ma question complémentaire s'adresse au ministre Champagne.

Innovation, Sciences et Développement économique Canada a attribué 25 contrats à GC Strategies. Certains de ces contrats avaient-ils rapport à la cybersécurité ou à des dispositions du projet de loi C-26?

L'hon. François-Philippe Champagne: Comme le ministre LeBlanc l'a mentionné, des enquêtes internes sont en cours pour évaluer la nature exacte de ces contrats. Je me ferai un plaisir de revenir devant le Comité pour fournir plus de détails si certains d'entre eux ont, comme mon collègue l'a suggéré, un lien quelconque avec la cybersécurité.

Je soupçonne que ce n'est pas le cas, mais nous allons le confirmer et fournir la réponse au Comité.

M. Dane Lloyd: Monsieur le président, nous savons qu'à la Défense nationale, six contrats ont été attribués à GC Strategies, et nous savons qu'aux Affaires mondiales, douze contrats ont été attribués à ce fournisseur.

Je ne m'attends pas à ce que vous sachiez si ces contrats se rapportaient eux aussi à la cybersécurité. Le savez-vous?

L'hon. François-Philippe Champagne: Je ne le sais pas, mais je pense que le ministre LeBlanc et moi-même pouvons nous engager auprès du Comité à demander à nos collègues de suivre exactement le même genre de procédure que celle que nous entreprendrons pour confirmer au Comité…

Je soupçonne que ce n'est pas le cas, mais encore une fois, nous nous efforcerons de fournir une réponse au Comité.

M. Dane Lloyd: J'aimerais céder le reste de mon temps de parole à M. Motz.

Merci, monsieur le président.

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): Merci beaucoup, monsieur le président.

La Stratégie nationale sur les infrastructures essentielles énumère dix secteurs essentiels pour la sécurité des infrastructures, mais le projet de loi ne parle que de cinq ou six d'entre eux.

Y a-t-il une raison de ne pas inclure dans ce projet de loi la santé, l'alimentation, l'eau, le secteur manufacturier, etc., des secteurs qui ont une importance cruciale pour la sécurité des Canadiens?

L'hon. Dominic LeBlanc: Bien entendu, cette loi ne peut s'appliquer qu'aux secteurs sous réglementation fédérale. Le gouvernement veut collaborer avec les partenaires dans les provinces et les territoires qui, par exemple, gèrent les systèmes de santé. C'est une vulnérabilité que j'ai signalée: nous ne pouvons pas légiférer dans ce domaine particulier. Nous cherchons à conclure des accords avec d'autres partenaires, quand c'est possible.

● (0925)

M. Glen Motz: Quels efforts avez-vous déployés, vous ou M. Champagne, auprès des provinces, des territoires, des administrations municipales et des gouvernements des Premières Nations pour régler ces questions fondamentales afin qu'ils bénéficient eux aussi d'une protection adéquate, dans ce cas-ci, du point de vue de la cybersécurité?

L'hon. François-Philippe Champagne: C'est une très bonne question et, comme le ministre LeBlanc l'a dit, les consultations sont en cours.

Je dirais que les secteurs que nous avons désignés sont également l'épine dorsale; le système de télécommunications est un catalyseur pour bon nombre de ces autres secteurs de l'économie. Au départ, nous avons ciblé les secteurs qui sous-tendent un autre domaine de manière systémique. Au bout du compte, la cybersécurité pourrait avoir un champ d'application très large parce que, comme je l'ai dit, les Canadiens sont concernés, les PME sont concernées, mais les secteurs sous réglementation fédérale que nous avons ciblés sont en quelque sorte l'épine dorsale.

Comme le ministre LeBlanc l'a dit, nous sommes en discussion pour voir comment y parvenir, et nous nous efforçons bien sûr toujours de faire en sorte que chaque secteur exposé à des risques du point de vue de la cybersécurité bénéficie d'une protection adéquate.

Le président: Merci.

M. Gaheer a la parole.

M. Iqwinder Gaheer (Mississauga—Malton, Lib.): Je remercie les ministres de comparaître devant le Comité.

Ma première question s'adresse au ministre LeBlanc. Nous savons que le projet de loi instaure une obligation de signalement pour les exploitants des infrastructures essentielles dans les différents secteurs.

M. Julian a abordé ce point. Électricité Canada a fait valoir que si un secteur ou une entreprise fait face à une cyberattaque, le signalement obligatoire, en particulier le signalement immédiat, pourrait être contraignant. Pourriez-vous nous dire pourquoi le signalement obligatoire, par opposition à un signalement volontaire, est important?

L'hon. Dominic LeBlanc: Vous avez raison. Ce projet de loi mettrait en place un système, un régime de signalement obligatoire. Nous avons conscience qu'il s'agit d'un fardeau ou d'une tâche que nous imposons à des entreprises privées, mais pour les raisons que mon collègue a mentionnées, ces entreprises privées sont de plus en plus l'épine dorsale des services de base sur lesquels les Canadiens comptent pour faire tourner l'économie du pays et pour assurer la sécurité et la sûreté des gens chez eux, au volant de leur voiture.

Même si beaucoup seraient désireux de signaler volontairement un incident, le signalement obligatoire nous permettra, pour revenir à ce qu'a dit M. Julian, d'obtenir des données sur la nature et le nombre exacts de ces menaces, et cela nous permettra également de travailler avec d'autres entreprises pour mieux les protéger quand une défaillance particulière est détectée, qu'une menace donnée est mise à exécution ou qu'un acte est commis.

L'objectif sera de travailler sans délai avec les autres acteurs dans le secteur concerné ou dans les secteurs comparables pour optimiser leur résilience et la protection dont ils bénéficient.

M. Champagne voulait ajouter quelque chose.

L'hon. François-Philippe Champagne: J'aimerais inviter mes collègues du Comité à considérer les interconnexions. Quand certains réseaux de télécommunications étaient hors service, pendant des catastrophes naturelles, c'était lié à une panne d'électricité. On ne peut pas examiner cette question en la compartimentant.

Il faut adopter une approche systémique. Par exemple, si une attaque est menée contre un système du réseau électrique, elle risque de se répercuter sur le réseau des télécommunications parce que, sans électricité et sans alimentation de secours, le réseau des télécommunications risque de ne pas rester en service.

C'est pourquoi il y a ce signalement qui nous permet d'agir très rapidement pour prévenir des dommages plus systémiques touchant des réseaux interconnectés. Comme je l'ai dit, quand on considère les télécommunications, quand on considère la distribution d'électricité, les réseaux sont étroitement connectés. Quand je parle aux premiers ministres des catastrophes qui ont frappé le pays, en particulier dans l'Est du Canada, ils mentionnent toujours l'électricité, parce que sans électricité, les stations ne sont pas opérationnelles, même avec une alimentation de secours.

S'il y avait une attaque, une cyberattaque contre le réseau électrique, nous voudrions savoir sans délai quelle incidence elle pourrait avoir sur le réseau des télécommunications également. Pensez à la 5G et à l'Internet des objets. Une attaque contre le réseau électrique pourrait avoir des répercussions dans bien des domaines. Des collègues ont mentionné la santé, le fonctionnement des hôpitaux et l'équipement des hôpitaux. Il s'agit d'une vision systémique de la protection des Canadiens.

M. Iqwinder Gaheer: Merci.

Au cours des travaux du Comité, nous avons beaucoup entendu parler de la transparence des pouvoirs inclus dans ce projet de loi et de l'exercice de ces pouvoirs. Le gouvernement serait-il disposé à rendre compte, par souci de transparence, du nombre de décrets ou d'arrêtés pris en application de cette mesure législative, tout en protégeant les détails relatifs à la sécurité?

● (0930)

L'hon. Dominic LeBlanc: Il s'agit là encore d'une bonne suggestion. Il faudrait consulter la chef du Centre de la sécurité des télécommunications, le CST, ou le directeur du Service canadien du renseignement de sécurité, le SCRS, ou d'autres hauts responsables qui ont, souvent sous le régime de la loi, la responsabilité de protéger ces renseignements.

C'est une discussion qui est menée dans le contexte de l'enquête judiciaire sur l'ingérence étrangère: quel est le meilleur moyen de communiquer aux Canadiens la nature de la menace d'ingérence étrangère? Pour prendre un exemple comparable, les cyberattaques, dont beaucoup proviennent d'acteurs étatiques étrangers, d'acteurs étatiques hostiles, pourraient être une situation similaire.

Ces renseignements doivent être protégés précisément pour ne pas donner à d'autres acteurs hostiles une feuille de route toute prête sur la procédure à suivre pour infecter un système d'alimentation en électricité à Montréal ou un système de santé dans une province. Je ne doute pas que les fonctionnaires feront ce travail dans le respect de la Charte des droits et de la Loi sur la protection des renseignements personnels.

Je le répète, je serais heureux de faire venir des fonctionnaires au Comité pour qu'ils travaillent avec vous et pour qu'ils vous expliquent la nature de cette obligation de signalement, mais s'il y avait une sorte de sommaire mentionnant que *x* décrets ou arrêtés ont été pris au cours d'une année donnée… Je serais heureux de travailler avec le Comité, mais je ne suis pas un expert.

Il y a un « effet mosaïque ». Je le tiens du directeur du SCRS. Parfois, si on publie des éléments d'information, cela peut sembler anodin dans un contexte particulier, mais un acteur étatique hostile, qui cherche peut-être à exposer les Canadiens à un grand danger, est en mesure de rassembler divers éléments d'information publique pour parvenir à une conclusion, même si la conclusion est erronée. Un tel agent n'est pas forcément tenu par une obligation d'établir les faits hors de tout doute raisonnable.

Je veux juste m'assurer qu'il n'y a pas d'interconnexion et que nous ne prenons pas d'engagements qui seraient dangereux, mais je me ferai un plaisir de travailler avec le Comité.

Le président: Merci.

Nous passons maintenant à la troisième série de questions.

Nous vous écoutons, monsieur Motz.

M. Glen Motz: Merci beaucoup, monsieur le président.

Une fois de plus, messieurs les ministres, plusieurs témoins ont dit au Comité dans leurs mémoires respectifs que ce projet de loi, tel qu'il a été rédigé et déposé, est truffé de défauts: il va trop loin, il n'oblige pas le gouvernement à rendre des comptes et il manque de transparence.

Avez-vous tenu des consultations sur ce projet de loi? De toute évidence, vous n'avez pas écouté ce que disaient les personnes consultées.

L'hon. François-Philippe Champagne: Il y a eu une vaste consultation, et je dirais, monsieur Motz, qu'il faut aussi penser au danger de l'inaction. Je respecte le point de vue de tout le monde, mais les menaces dont nous avons parlé concernent le secteur des télécommunications, le secteur de l'énergie, les services financiers et les transports. Si vous considérez nos pairs dans le monde, conférer ces pouvoirs, c'est agir de manière responsable pour les Canadiens.

Comme je l'ai dit, dans le secteur des télécommunications, comme vous vous en souviendrez, nous avons pu obtenir un engagement volontaire, mais je pense que les Canadiens qui nous regardent chez eux aimeraient que le gouvernement ait le pouvoir d'exiger la prise des mesures nécessaires pour protéger les réseaux à fibres optiques d'une défaillance systémique…

M. Glen Motz: Merci, monsieur le ministre. Je m'excuse.

Je vais céder le temps qu'il me reste à M. Lloyd.

M. Dane Lloyd: Merci.

Dans son récent rapport sur ArriveCAN, la vérificatrice générale a fait des révélations accablantes au sujet de la cybersécurité concernant votre ministère. Je cite: « Les mises à l'essai de l'application ArriveCAN comportaient des lacunes » et « [d]es tests de cybersécurité [ont été] effectués par des ressources qui n'avaient pas d'autorisation de sécurité ou qui n'avaient pas été identifiées dans les autorisations de tâches. » De plus, la vérificatrice générale a constaté que « certaines ressources ayant participé aux évaluations de sécurité n'avaient pas [...] [l]'autorisation de sécurité » appropriée.

Monsieur le ministre, comment pouvons-nous avoir l'assurance que la sécurité des Canadiens est la priorité absolue du gouvernement quand les entreprises chargées d'assurer la cybersécurité dans les dossiers que vous jugez prioritaires n'ont même pas l'autorisation de sécurité? Pouvez-vous garantir aux Canadiens qu'aucun des renseignements personnels qu'ils ont communiqués via l'application ArriveCAN n'a été compromis par ces entreprises qui n'avaient pas d'autorisation de sécurité?

L'hon. Dominic LeBlanc: Bien évidemment, nous avons trouvé préoccupantes ces conclusions de la vérificatrice générale. Après les discussions que j'ai eues avec la présidente de l'Agence des services frontaliers, je suis convaincu qu'elle a mis en place — comme vous le savez, avant le rapport de la vérificatrice générale, l'ombud de l'approvisionnement s'est lui aussi penché sur ce dossier — une série de mesures de nature à empêcher que cette situation se reproduise.

● (0935)

M. Dane Lloyd: Je ne doute pas qu'il en soit ainsi pour l'avenir, monsieur le ministre, mais pouvez-vous garantir que les renseignements personnels des Canadiens n'ont pas été compromis par ces entreprises qui n'avaient pas la classification de sécurité pour effectuer des tests de cybersécurité sur l'application ArriveCAN? Pouvez-vous dire aux Canadiens que leurs renseignements n'ont pas été compromis?

L'hon. Dominic LeBlanc: Ce que je peux dire aux Canadiens, c'est que le gouvernement et des organismes comme le CST, qui a une responsabilité générale en matière de protection des systèmes informatiques fédéraux, sont très efficaces et font tout ce qui est possible pour protéger tous les systèmes qui contiennent des données personnelles appartenant à des Canadiens.

La perfection n'existe pas dans ce travail, et c'est précisément pour cela que nous travaillons avec des alliés dans le monde, avec le Groupe des cinq. C'est précisément pour cela que cette obligation de signalement sera une mesure importante...

M. Dane Lloyd: Monsieur le ministre, menez-vous une enquête pour déterminer si ces renseignements ont été compromis?

L'hon. Dominic LeBlanc: Toutes les circonstances entourant l'application ArriveCAN, ce qui a mené à cette situation ainsi que le rôle joué par des entreprises privées font l'objet d'une enquête. Par ailleurs, comme je l'ai dit, je ne doute pas que les problèmes relevés par la vérificatrice générale ont été corrigés.

Je rappelle au Comité que, dans le contexte des premiers mois de la COVID, tous les gouvernements du pays, les gouvernements provinciaux — j'étais ministre des Affaires intergouvernementales — se hâtaient de faire ce qu'il fallait…

M. Dane Lloyd: Rien ne justifie de mettre en péril les renseignements personnels des Canadiens.

Le président: Merci.

M. Bittle a maintenant la parole, pour quatre minutes.

M. Chris Bittle (St. Catharines, Lib.): Merci beaucoup, monsieur le président.

Monsieur LeBlanc, M. Motz a parlé des secteurs sous réglementation provinciale et de leur importance dans le contexte de la sécurité. Pouvez-vous nous parler du rôle du gouvernement fédéral à cet égard et nous dire s'il est possible de modifier la loi pour faire état du rôle des provinces en ce qui concerne la protection des Canadiens dans les secteurs sous réglementation provinciale?

L'hon. Dominic LeBlanc: C'est au coeur même de l'exercice que nous essayons tous d'accomplir avec le projet de loi C-26.

La fédération donne à nos partenaires provinciaux et territoriaux les compétences sur des domaines aussi importants que les systèmes de santé et les infrastructures routières. Nous avons tous en tête des exemples de cyberattaques visant ces secteurs parmi les infrastructures essentielles. J'ai parlé aux maires de certaines villes. Il a été mentionné que Saint John, au Nouveau-Brunswick, une petite ville canadienne, a été visée par une cyberattaque assez préoccupante.

Nous ne pouvons faire ce travail qu'en partenariat avec les provinces et les territoires, et, bien sûr, la responsabilité leur incombe dans le cas des municipalités également. Nous serions tout à fait disposés à conclure des accords avec les provinces et les territoires. Nous pensons que le projet de loi C-26, s'il est adopté et reçoit la sanction royale, peut servir de modèle à d'autres lois provinciales qui devraient accompagner cette loi fédérale.

Comme le veulent nos collègues, nous cherchons toujours à respecter les compétences provinciales.

[*Français*]

C'est certainement une priorité pour nous. Cependant, nous n'allons pas évacuer le besoin d'être un partenaire et un chef de file ni celui d'échanger des données, dans la mesure où c'est sécuritaire. Nous allons signer des ententes avec des provinces précisément pour nous permettre d'échanger des données.

Cela dit, nous reconnaissons qu'il y a des situations d'urgence dans les domaines de compétence provinciale, et c'est pourquoi j'ai donné l'exemple de Terre-Neuve-et-Labrador. À l'époque, le premier ministre de Terre-Neuve-et-Labrador nous a dit que la province était complètement dépassée sur le plan des ressources, et il a demandé au gouvernement du Canada d'intervenir. Évidemment, nous avons fait ce qu'il était possible de faire à ce moment-là pour les aider à résoudre cette situation.

[*Traduction*]

M. Chris Bittle: Merci beaucoup.

Cette question s'adresse à l'un ou l'autre d'entre vous.

Ce projet de loi fait partie des efforts déployés par le Canada pour renforcer la cybersécurité. Pouvez-vous nous parler de l'urgence qu'il y a à avoir des programmes et des lois en place pour assurer la sécurité des renseignements des Canadiens et des infrastructures essentielles, ainsi que des autres mesures que le gouvernement prend, le cas échéant, à cet égard?

L'hon. François-Philippe Champagne: Rétrospectivement, nous avons pris de nombreuses mesures. Le travail de ce gouvernement a commencé en 2013 par l'établissement du Programme d'examen de la sécurité. Puis, en 2018, nous avons publié la Stratégie nationale de cybersécurité. En 2019, un investissement important, de plus de 100 millions de dollars, a été réalisé pour élaborer un cadre visant à protéger les cybersystèmes essentiels. En 2021, nous avons mené l'examen interministériel de sécurité de la 5G.

Ce qui est incontestable, c'est qu'en mai 2022, nous avons fait savoir très clairement qu'il n'y aurait plus d'équipement de Huawei ou de ZTE dans l'un des réseaux les plus importants au pays, celui des télécommunications.

Vous l'aurez constaté, à chaque étape, nous avons essayé, avec le ministère de la Sécurité publique, de garder une longueur d'avance, parce qu'en matière de cybersécurité, les acteurs malveillants essaieront toujours de nous rattraper, d'une façon ou d'une autre. Nous travaillons avec nos partenaires du Groupe des cinq, avec nos partenaires du G7 et avec nos alliés dans le monde entier pour repérer les menaces, interrompre l'action des acteurs malveillants et protéger notre réseau essentiel.

Le texte que nous avons devant nous est essentiel pour les entreprises canadiennes, en particulier pour les secteurs qu'il protège. Je répète encore une fois que le réseau des télécommunications en fait partie, parce qu'avec l'Internet des objets et la 5G, il sera partout. C'est pourquoi le travail qui occupe le Comité aujourd'hui est si important.

● (0940)

Le président: Merci.

Nous allons passer à Mme Michaud.

La parole est à vous.

[*Français*]

Mme Kristina Michaud: Merci, monsieur le président.

Les éléments qui sont revenus très souvent pendant les consultations que nous avons tenues ici, au Comité, ce sont évidemment ceux liés à la transparence et à la protection de la vie privée.

Certains collègues ont d'ailleurs abordé ces éléments. Selon le Commissariat à la protection de la vie privée du Canada, ce serait peut-être une bonne idée que le gouvernement le consulte avant de prendre quelque décision que ce soit dans le cadre du projet de loi C-26. Ce serait peut-être une façon de rassurer les Québécois et les Canadiens.

Évidemment, le projet de loi C-26, dans sa forme actuelle, ne prévoit pas de délai entre le moment où le gouvernement accède à des données personnelles et aux renseignements personnels consignés dans les entreprises, par exemple, et le moment où il les supprime dans le cadre de ce projet de loi. Par ailleurs, on sait aussi qu'il y a énormément de fuites de données et que le gouvernement n'est pas nécessairement à l'abri de ces fuites non plus.

Comment pouvons-nous atteindre un équilibre, d'une part, entre le droit à la vie privée et à la protection des renseignements personnels, et, d'autre part, la prise de pouvoir, les décrets et les arrêtés qui se font de façon très confidentielle?

Comment trouver l'équilibre dans tout cela? Que pouvez-vous dire aux Québécois, aux Canadiens et aux PME pour les rassurer?

L'hon. François-Philippe Champagne: Je dirais d'abord que les pouvoirs accordés visent à assurer la sécurité de systèmes désignés. L'objectif est très clair, et c'est la sécurité. Dans le cas d'une cyberattaque, qui pourrait avoir un effet sur l'ensemble de différents secteurs, soit les télécommunications, le système bancaire ou le réseau de transport au pays, vous comprendrez qu'il est urgent d'agir.

Il est tout aussi urgent d'intervenir quand il y a des désastres naturels ou, pour reprendre encore l'exemple de Rogers, quand 12 millions de Canadiens et de Canadiennes n'ont accès à aucun système de paiement au pays.

Ce sont toutes ces raisons qui nous poussent à rechercher ce juste équilibre. Je comprends le désir de consultation. Prenons l'exemple d'une cyberattaque visant la technologie 5G, qui pourrait avoir des répercussions sur l'ensemble des systèmes. Si on publiait les détails de la défaillance survenue chez un acteur de l'industrie en particulier, cela pourrait inciter des gens malveillants à se précipiter dans la brèche. On augmenterait ainsi le risque systémique.

Je pense que c'est l'équilibre qu'on essaie de trouver. Les pouvoirs proposés sont quand même liés à un objectif clair de sécurité. Le droit administratif s'applique, tout comme le contrôle judiciaire et la Charte canadienne des droits et libertés, par exemple.

[*Traduction*]

Le président: Merci.

Monsieur Julian, vous avez la parole.

[*Français*]

M. Peter Julian: Merci, monsieur le président.

Le rapport de la vérificatrice générale sur l'application ArriveCAN parle justement de cette mauvaise pratique liée au traitement des données confidentielles.

[*Traduction*]

Il faut que nous en tirions une leçon.

Au sujet du projet de loi C-26, nous avons entendu le témoignage d'une représentante du Citizen Lab de l'Université de Toronto. L'une des recommandations était qu'il faudrait que des indemnisations soient prévues si le gouvernement ne gère pas correctement les renseignements confidentiels, personnels ou dépersonnalisés, et qu'il faudrait modifier la loi pour permettre aux particuliers et aux fournisseurs de services de télécommunication de demander une indemnisation si le gouvernement ne gère pas correctement ces renseignements.

Ma question s'adresse au ministre LeBlanc.

Croyez-vous qu'il est approprié d'incorporer dans cette loi les leçons tirées d'ArriveCAN?

● (0945)

L'hon. Dominic LeBlanc: Absolument, parce que, comme tous mes collègues et, je pense, tous les Canadiens, j'ai pris acte des conclusions de la vérificatrice générale. J'ai également été tenu au courant d'autres processus d'examen internes avant le rapport de la vérificatrice générale, et tout cela me donne à penser qu'il y a là une occasion d'éviter certaines de ces préoccupations mêmes. Nous avons expliqué le contexte dans lequel ces développements ont eu lieu. Il ne justifie en rien les circonstances financières entourant ce projet ni, ce qui est peut-être plus important encore, les risques liés à la protection des renseignements personnels des Canadiens.

Si le Comité veut suggérer un moyen approprié d'imposer au gouvernement du Canada l'obligation de faire en sorte que la situation mentionnée par la vérificatrice générale ne se reproduise jamais, nous sommes ouverts à ce type de travail.

M. Peter Julian: Nous avions aussi une recommandation visant à interdire la divulgation de renseignements personnels ou dépersonnalisés à des organismes étrangers. Cela vient de la coalition.

Appuyez-vous cette recommandation?

L'hon. Dominic LeBlanc: J'ai également pris note de cette recommandation. J'aimerais entendre certains des dirigeants de nos organismes de sécurité, tels que le Service canadien du renseignement de sécurité ou le Centre de la sécurité des télécommunications, au sujet — comme nous l'avons dit en réponse à certaines questions de nos collègues — de la capacité d'établir des partenariats efficaces avec des alliés, en particulier les États-Unis dans ce contexte. Ils ont des systèmes de cyberdéfense parmi les plus perfectionnés au monde. Nous devons apprendre d'eux. Cela ne veut pas dire que nous sommes insensibles ou que nous gérons mal les renseignements personnels des Canadiens. Il faudrait que ce soit assujetti aux lois applicables et à la Charte des droits.

Si le Comité veut examiner cet aspect, je me mets à sa disposition. Le Comité prendra ses propres décisions en ce qui concerne les amendements, bien entendu. Je ne suis pas un expert pour ce qui est de déterminer le juste équilibre dans l'échange d'information avec des partenaires étrangers. Je pense que nous devons l'autoriser en partie. Nous devons veiller à ce que le tout soit bien encadré et à ce que les bonnes mesures de protection soient en place pour les données privées des Canadiens. Selon moi, si nous réussissons à protéger les infrastructures essentielles, la boucle sera bouclée parce que, dans une certaine mesure, nous protégeons également les données privées des Canadiens qui sont actuellement détenues par des acteurs du secteur privé. Je pense aux renseignements financiers que ma banque aurait sur moi ou sur n'importe lequel d'entre nous. Les banques prennent cela très au sérieux, bien sûr, mais y a-t-il un moyen pour le gouvernement du Canada de travailler en partenariat avec elles?

La boucle sera ainsi bouclée. Je regarde M. Julian, que je connais depuis longtemps. Il sera préoccupé par l'équilibre dans ce travail, tout comme moi. Si le Comité veut trouver la bonne façon de s'assurer que le juste équilibre a été atteint, je serai heureux de travailler avec le Comité et de veiller à ce que des experts qui ont peut-être des points de vue beaucoup plus éclairés que le mien soient en mesure d'offrir cette perspective.

Le président: Je vous remercie.

Avant de suspendre la séance, je demanderais aux témoins de faire preuve d'indulgence à notre égard. Je vous remercie d'être venus ici aujourd'hui avec vos équipes.

Chers collègues, nous allons entendre les prochains témoins. Nous avons déjà rencontré et questionné certains d'entre eux lors d'une séance d'information technique. Je rappelle que nous devons vérifier certains travaux du Comité avec le greffier. Si vous estimez avoir posé suffisamment de questions pertinentes aux ministres aujourd'hui, je demanderai le consentement unanime pour permettre aux ministres et aux prochains témoins de partir afin que nous puissions nous occuper des travaux du Comité et passer à autre chose.

Est-ce que tout le monde est d'accord?

M. Dane Lloyd: Monsieur le président, j'aimerais que nous ayons une brève série de questions avec les témoins. Nous pourrons ensuite passer rapidement aux travaux du Comité.

Le président: Très bien. Nous allons suspendre la séance pendant cinq minutes.

Je vous remercie.

● (0945)

_____(Pause)_____

● (0955)

Le président: J'aimerais souhaiter la bienvenue aux autres fonctionnaires qui se sont joints à nous.

Du ministère de l'Industrie, nous accueillons Wen Kwan, directeur principal, Secteur du spectre et des télécommunications, et Andre Arbour, directeur général, Secteur des stratégies et politiques d'innovation.

Nous allons accorder environ trois minutes à chaque intervenant, dans la mesure du possible. Si nous devons écourter les interventions, nous le ferons.

Je vais commencer par M. Lloyd.

M. Dane Lloyd: Merci, monsieur le président. Je serai très bref.

Je remercie les fonctionnaires de leur présence.

Certains témoins ont dit craindre que le projet de loi entraîne une augmentation draconienne des coûts de conformité, tout en faisant monter les coûts pour prévenir les cyberattaques et préserver leur cyberinfrastructure.

Si vous savez à combien on estime l'augmentation des coûts de conformité pour toutes les industries touchées par le projet de loi, pouvez-vous le dire au Comité aujourd'hui? Sinon, j'aimerais que vous vous engagiez à faire parvenir cette information au Comité avant que nous commencions notre étude article par article.

M. Patrick Boucher: Il y a encore beaucoup de travail à faire dans le cadre du processus réglementaire, et c'est quelque chose qui, à mon avis, est fondamental pour que le projet de loi aille de l'avant.

M. Dane Lloyd: Mais vous n'avez pas la réponse pour le moment.

M. Patrick Boucher: Je dirais que le coût des atteintes aux cybersystèmes dépasse de loin...

M. Dane Lloyd: Je comprends.

Je veux simplement savoir quels sont ces coûts estimatifs...

Mme Jennifer O'Connell: J'invoque le Règlement, monsieur le président. En toute justice, au sein de notre comité, l'intervenant pose une question et donne au témoin l'occasion d'y répondre. Ce n'est pas correct de lui couper la parole.

Le président: Monsieur Lloyd, vous avez la parole.

M. Dane Lloyd: Une question à laquelle on peut répondre par oui ou par non n'exige pas beaucoup de temps, monsieur le président.

J'aimerais également que les témoins fournissent au Comité des renseignements sur toute estimation de l'augmentation nette des équivalents temps plein que le gouvernement devrait peut-être embaucher pour administrer les dispositions du projet de loi.

Avez-vous cette information sous la main? Sinon, pouvez-vous vous engager à l'envoyer au Comité?

Je vous remercie. C'est ma dernière question.

M. Patrick Boucher: Encore une fois, je pense qu'un processus réglementaire exhaustif sera mis en place, non seulement en partenariat avec l'industrie, mais aussi avec les provinces et les territoires, afin d'étoffer cette mesure législative et de déterminer les seuils pour l'application de la loi.

Il s'agit d'une véritable approche de partenariat que nous adoptons ici avec les parties prenantes et les partenaires, et ce sont là certains des détails que nous allons devoir cerner en collaboration avec les partenaires.

M. Dane Lloyd: Pouvez-vous au moins nous fournir ces estimations?

N'avez-vous pas de modélisation économique sur les répercussions des formalités administratives, les répercussions sur le PIB...? Avez-vous ce genre de modélisation et pouvez-vous en faire part au Comité?

M. Patrick Boucher: La mise en œuvre du projet de loi ne devrait pas entraîner de lourdeurs administratives. Il s'agit de travailler avec l'industrie...

M. Dane Lloyd: Le projet de loi ne fera pas augmenter les coûts de conformité?

M. Patrick Boucher: Il s'agit de travailler avec l'industrie pour nous assurer que nous protégeons les infrastructures essentielles sur lesquelles les Canadiens comptent toujours les jours.

Le président: Je vous remercie.

Nous allons passer à M. McKinnon.

M. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.): Merci, monsieur le président.

Je remercie les témoins de leur présence.

Nous avons entendu des témoins alléguer que le projet de loi amènera le gouvernement à accéder aux renseignements personnels, notamment dans les téléphones cellulaires, à les recueillir et, surtout, à les utiliser à mauvais escient.

Est-il probable qu'on en vienne là, et pourquoi?

Je pose la question à M. Schaan.

[*Français*]

M. Mark Schaan (sous-ministre adjoint principal, Secteur des stratégies et politiques d'innovation, ministère de l'Industrie): Monsieur le président, je remercie le député de la question.

[*Traduction*]

En ce qui concerne la collecte de renseignements personnels, comme il est indiqué dans le projet de loi C-26, le ministre a le pouvoir de prendre des décrets qui lui permettront de protéger la sécurité du système de télécommunications.

Il y a deux choses qui, à mon avis, sont vraiment importantes à souligner. Les mesures et les décrets liés au pouvoir du ministre doivent être arrimés à cet objectif de sécurité et réservés à cet égard. De même, il y a un critère de proportionnalité qui s'applique, en vertu du droit administratif, aux décrets que le ministre prend.

Il y a deux autres points que je trouve vraiment importants. Premièrement, la Loi sur la protection des renseignements personnels continue de s'appliquer au ministre de l'Industrie et à ses fonctionnaires par l'entremise du ministère. Deuxièmement, la Loi sur la protection des renseignements personnels et les documents électroniques continue de s'appliquer aux fournisseurs de services de télécommunications visés par le pouvoir de prendre des décrets.

Des mesures de protection de la vie privée sont en place pour les deux entités, tant du côté du gouvernement que du côté du secteur privé, et il y a des limites à la capacité du ministre de prendre des décrets.

● (1000)

M. Ron McKinnon: Je vous remercie.

Nous avons beaucoup entendu parler de la protection de nos infrastructures contre les acteurs malveillants, mais nous avons aussi entendu parler de la nécessité de nous protéger contre les catastrophes naturelles et tout le reste: feux de forêt, inondations, et j'en passe.

Pouvez-vous nous dire comment le projet de loi pourrait faciliter cet effort?

M. Mark Schaan: Je le ferai avec plaisir.

[*Français*]

Je vous remercie de la question.

[*Traduction*]

Je pense qu'il est important de souligner que l'objectif de sécurité des télécommunications, comme l'a souligné le ministre, permet en fait un vaste champ d'application, en ce sens que la sécurité est fondamentale dans un certain nombre de contextes. Même si nous l'associons souvent à la cybersécurité, je pense qu'en l'occurrence, nous devons réfléchir à la sécurité en fonction de la question de savoir, par exemple, si nous pouvons accéder en toute sécurité au système de télécommunications en cas de catastrophe naturelle, chose qui arrive de plus en plus souvent.

Le ministre de l'Industrie a le pouvoir de prendre des décrets aux termes du projet de loi C-26, par exemple, pour permettre à un fournisseur de services de télécommunications d'élaborer un plan de sécurité en ce qui concerne ses services, ses réseaux ou ses installations et...

Le président: Je vous remercie.

Madame Michaud, vous avez la parole.

[*Français*]

Mme Kristina Michaud: Merci, monsieur le président.

Je pense que les fonctionnaires ont très bien informé les ministres de leurs ministères respectifs, parce qu'on a répondu à toutes mes questions.

Je vais laisser tomber le reste de mon temps de parole, parce que j'aimerais que nous discutions du temps que nous aurons pour déposer nos amendements.

[*Traduction*]

Le président: Merci, madame Michaud.

Monsieur Julian, vous avez la parole.

M. Peter Julian: Je vous remercie de votre présence.

J'ai posé tout à l'heure une question sur la NERC, la North American Electric Reliability Corporation, et la réglementation correspondante. Dans quelle mesure les ministères communiquent-ils avec des associations d'infrastructures vitales comme celle-là pour s'assurer que nous ne nous retrouvons pas avec un problème de conformité aux lois et aux règlements, ce qui fait qu'une entreprise ou une entité pourrait être tiraillée dans deux directions opposées?

M. Patrick Boucher: Dans le cadre de l'élaboration du projet de loi, il y a eu de très vastes consultations auprès d'associations comme celle dont vous parlez. Cela se poursuivra tout au long du processus réglementaire visant à établir ces règlements.

Nous voulons également nous assurer de collaborer avec les provinces et les territoires pour veiller à ce qu'il y ait une harmonisation dans la mise en œuvre de ces diverses lois pour l'industrie — c'est-à-dire les entités susceptibles d'être assujetties à des lois fédérales comme celle-ci, par exemple, et à des lois provinciales. C'est un engagement qui, selon moi, est fondamental pour le projet de loi, et c'est quelque chose que nous allons continuer de faire grâce à une mobilisation accrue.

M. Peter Julian: Lorsque vous parlez d'harmonisation, voulez-vous dire, alors, que les lois ou les règlements prévus sont modifiés dans une certaine mesure pour éviter les chevauchements ou les contradictions entre deux directions différentes afin d'assurer la cybersécurité? Ou est-ce que l'harmonisation vise à amener les autres organisations à changer leurs règles? Ce sont deux approches très différentes.

M. Patrick Boucher: À mon avis, c'est le premier aspect que vous venez de mentionner: l'harmonisation fait en sorte que les dispositions législatives et réglementaires ne sont pas contradictoires et que ces organisations ne sont pas tiraillées dans deux directions opposées.

Je le répète, nous voulons collaborer davantage avec les provinces. C'est un des engagements que nous avons pris dans le cadre de notre dialogue avec les provinces, les territoires et l'industrie pour nous assurer que nous faisons ce qu'il faut pour l'industrie tout au long du processus réglementaire.

M. Peter Julian: Le projet de loi prévoit notamment qu'un avis doit être signifié sans délai à la suite d'une cyberattaque. Différents témoins ont laissé entendre, d'une manière qui m'a semblé assez explicite, qu'il faudrait que le délai accordé à cette fin soit plus clairement précisé.

Certains proposent un délai de 72 heures pour communiquer cet avis, et ce, dans le but de laisser suffisamment de temps pour contrer la cyberattaque, ou tout au moins s'efforcer de le faire. Selon ces témoins, les exigences en matière de signalement et d'avis seraient devenues lourdes à un point tel qu'il n'est plus possible de neutraliser l'attaque et de riposter adéquatement. Si vous devez passer plus de temps à vous assurer de respecter la loi à la lettre qu'à contrer la cyberattaque, il peut vraiment y avoir un problème.

Comment le ministère définit-il cette obligation d'avis immédiat? Êtes-vous d'accord avec ces nombreux témoins qui nous ont dit que la période allouée à cette fin doit être mieux précisée et suffisamment longue pour permettre à l'organisation, à l'entreprise ou à l'entité d'enrayer la cyberattaque avant de devoir en aviser les autorités?

M. Patrick Boucher: Je conviens effectivement que l'on devrait préciser la période allouée pour informer les autorités compétentes.

C'est un aspect que nous avons abordé et que nous continuerons d'examiner dans le cadre de nos échanges en vue d'intégrer le tout à nos mécanismes réglementaires. Il s'agit encore une fois de trouver le juste équilibre entre, d'une part, l'importance de veiller à ce que nous soyons au fait de la menace afin que l'expertise du Centre puisse être mise à contribution, et, d'autre part, la nécessité d'avertir les autres secteurs pour qu'ils puissent mettre en place les mesures qui s'imposent afin de protéger leurs propres infrastructures, le tout en tenant compte des réalités que vous venez d'évoquer.

Je pense que nous allons bel et bien devoir clarifier le tout, et nous sommes déterminés à collaborer avec nos partenaires à cette fin.

● (1005)

Le président: Merci.

Nous avons maintenant quelques questions de régie interne pour lesquelles notre greffier aimerait obtenir des réponses.

Revenons d'abord à un sujet dont nous avons traité lors de notre dernière réunion. Si le Comité souhaite commencer l'étude article par article du projet de loi C-26 le lundi 26 février, je recommande de fixer au mercredi 21 février, à midi, la date limite pour soumettre des amendements.

Je sais qu'il y a eu des discussions à ce propos, alors je vais vous demander si ce délai vous convient toujours.

Nous vous écoutons, monsieur Shipley.

M. Doug Shipley: Merci, monsieur le président.

À la lumière de l'étude que nous venons de mener à terme et de ce que nous avons pu entendre encore aujourd'hui, je m'attends à ce qu'un bon nombre d'amendements soient proposés. Je pense qu'il risque d'être un peu difficile de soumettre tous ces amendements d'ici mercredi prochain. Si nous pouvions repousser l'échéance au mercredi suivant, après la semaine de relâche, cela nous laisserait la fin de semaine prochaine pour y travailler.

Nous n'avons pas autant de ressources que nos collègues du parti ministériel. Je n'apprends rien à personne. Nous allons tout faire pour soumettre nous aussi nos amendements, mais une semaine de plus nous faciliterait la tâche.

Le président: À vous la parole, madame Michaud.

[*Français*]

Mme Kristina Michaud: Merci, monsieur le président.

Mon commentaire va dans le même sens que celui de mon collègue. De notre côté aussi, nos ressources sont assez limitées. Préparer des amendements et s'assurer de leur conformité auprès de la conseillère législative est un exercice fastidieux. Il y a beaucoup d'échanges de part et d'autre.

Le 21 février, c'est dans moins d'une semaine; cela nous laisse très peu de temps. Il ne faut pas oublier que nous allons commencer l'étude du projet de loi la semaine suivante et que, par la suite, nous allons être dans nos circonscriptions pendant deux semaines. Nous allons donc devoir nous dépêcher pour faire notre travail, à mon avis. Par la suite, l'étude du projet de loi serait mise sur pause, parce que nous allons passer plusieurs semaines dans nos circonscriptions au mois de mars.

Je propose que nous ayons un peu plus de temps pour soumettre nos amendements. Il me paraît raisonnable de nous accorder une semaine supplémentaire, comme le proposait M. Shipley. En attendant, le Comité pourrait commencer son étude sur les vols de voiture.

[*Traduction*]

Le président: Merci.

Monsieur Julian, je vous en prie.

[*Français*]

M. Peter Julian: Je suis d'accord avec mes collègues.

D'une part, nous pourrions commencer notre étude sur les vols de voiture dans une semaine et demie. D'ici à mardi prochain, nous pourrions soumettre la liste des témoins que nous voulons voir participer à l'étude proposée par Mme Michaud concernant les vols de voiture. Pour ce qui est des amendements, nous pourrions fixer la date limite de dépôt pour la semaine suivante.

D'autre part, j'aimerais proposer quelque chose pour la semaine suivante. Sur les sept prochaines semaines, il y a juste deux semaines de séance. Si nous faisons notre étude sur le vol de voitures la semaine prochaine, je propose que le Comité tienne des réunions plus longues pour discuter des amendements proposés au projet de loi C-26.

Pour être honnête, je trouve qu'il est difficile de discuter des amendements pendant deux heures et de continuer notre discussion trois jours plus tard, parce qu'il y a souvent des liens entre les amendements. Il me paraît plus utile de tenir une réunion de 15 h 30 à minuit, par exemple. Si nous faisions cela, nous pourrions terminer l'étude du projet de loi cette semaine-là. Je parle de la deuxième semaine de séance qui aura lieu en mars.

Je propose donc que nous tenions de plus longues réunions, que nous reportions la date limite pour ce qui est du dépôt des amendements et que nous commencions notre étude sur les vols de voiture la semaine après la semaine prochaine.

● (1010)

[*Traduction*]

Le président: Merci.

À vous maintenant, madame O'Connell.

Mme Jennifer O'Connell: Merci, monsieur le président.

Bien que je comprenne que certains puissent avoir besoin d'un peu plus de temps, je ne voudrais pas que nous perdions nos deux séances de la semaine prochaine. Nous devons nous réunir le 26 et le 29. Si nous voulons commencer l'étude sur le vol de voitures le 26 février, c'est très bien — parallèlement aux amendements qui pourront être alors soumis —, mais je ne suggérerais pas que nous y consacrions également notre réunion du 28. Nous devons garder à l'esprit qu'il n'y a qu'une semaine de séance en mars, et que l'une des réunions que nous avons déjà confirmées — celle du 21 mars — doit porter sur le mandat du ministre.

Cela nous laissera en fait seulement deux réunions, celles du 28 février et du 18 mars, alors même que la menace est tout ce qu'il y a de plus réel, comme on nous l'a rappelé encore aujourd'hui. Tout le monde s'entend pour dire qu'il est urgent d'adopter ce projet de loi.

Je conviens avec M. Julian que nous pourrions tenir des séances plus longues, mais il faudrait que les amendements soient présentés d'ici le 26 février. Nous pourrions ainsi débuter l'étude article par article le 28 février. Nous pourrions tout de même commencer l'étude sur le vol de voitures en lui consacrant, dans un premier temps, notre réunion du 26 février.

C'est un compromis qui permettrait de reporter le délai pour la présentation des amendements, sans toutefois que nous perdions nos deux réunions prévues en février. Je serais par ailleurs en faveur des séances prolongées.

Le président: Nous vous écoutons, monsieur Shipley.

M. Doug Shipley: Merci.

Il y a beaucoup d'intervention au sujet des différentes dates. Je pense que nous devons clarifier un peu les choses.

Nous allons reporter d'une semaine le dépôt des amendements. À notre retour, nous allons commencer le lundi notre étude sur les vols d'automobile. Est-ce bien ce que vous avez dit, madame O'Connell? Et que se passera-t-il le jeudi de cette semaine-là? Je suis désolé. Est-ce que ce sera l'étude article par article?

Après cela, est-ce que nous poursuivrions en alternance avec l'étude sur les vols de voiture?

Mme Jennifer O'Connell: La motion n'a pas été adoptée. Je pense que nous devrions d'abord terminer l'étude article par article étant donné que nous ne disposerons que de deux séances. Je suis d'accord avec M. Julian pour que nous prolongions nos réunions lors des deux journées en question. Ensuite, une fois l'étude article par article terminée, nous pourrons reprendre notre étude sur les vols d'automobile.

M. Doug Shipley: Merci pour ces précisions.

Le seul problème, c'est que certains de nos députés siègent à plus d'un comité et qu'ils pourraient avoir d'autres réunions ces soirs-là, alors je ne sais pas s'il serait possible...

M. Glen Motz: Il est assez intéressant de noter que ce projet de loi a été déposé en juin 2022. Il y a donc 20 mois qui se sont écoulés depuis, et voilà maintenant que nous voudrions précipiter les choses après avoir entendu tous ces témoins... Qui plus est, nous aurons d'importantes recommandations à vous soumettre dans le cadre de l'étude article par article pour apporter les correctifs nécessaires à ce projet de loi, car c'est la responsabilité du Comité de le faire.

Je ne vois pas pourquoi il faudrait tout à coup s'empresser de conclure le tout en tenant des séances plus longues en l'espace d'une semaine ou deux. Nous avons aussi d'autres responsabilités, et je ne suis pas favorable à la tenue de réunions prolongées.

Je pense que nous devrions entreprendre l'étude sur les vols de voiture. Lorsque nous aurons terminé nos recommandations d'amendement et que nous les aurons soumises, nous pourrons revenir au projet de loi C-26 pour en faire l'étude article par article. Il est certain qu'il nous faudra bien plus que quelques séances prolongées pour y arriver.

Mme Jennifer O'Connell: La sécurité n'est pas si importante.

M. Glen Motz: Vous avez ce dossier en main depuis juin 2022.

Le président: À vous la parole, monsieur McKinnon.

M. Ron McKinnon: Merci, monsieur le président.

Je suis tout à fait d'accord avec Mme O'Connell, et j'appuie la prolongation des séances le moment venu.

En ce qui concerne la remarque de M. Motz suivant laquelle ce projet de loi a été déposé en juin 2022, nous devrions nous rappeler qu'il a été renvoyé au Comité en mars 2023. Par conséquent, nous sommes saisis du projet de loi depuis un an à peine. Tout retard dans l'étude de ce projet de loi est donc attribuable au Comité lui-même, et non au gouvernement.

C'est un projet de loi primordial. Nous devons nous mettre à la tâche. C'est dans ce contexte que les séances prolongées revêtent une importance capitale. Il ne s'agit pas simplement de reporter le tout d'une semaine parce que nous allons en fait perdre la majeure partie du mois de mars.

Je pense qu'une fois que nous aurons commencé l'étude article par article de ce projet de loi, nous devrons la mener à terme le plus tôt possible, conformément à ce que suggère Mme O'Connell. Nous devons profiter de toutes les occasions qui s'offrent à nous pour progresser dans ce dossier.

● (1015)

Le président: Monsieur Julian, je vous en prie.

M. Peter Julian: Merci, monsieur le président.

Je dirais, en réponse aux commentaires de M. Motz sur le fait d'avoir d'autres responsabilités, que chaque député du NPD — et je pense que c'est la même chose pour le Bloc — doit porter quatre chapeaux à la fois. Si nous pouvons trouver du temps pour venir ici, je pense que les conservateurs devraient pouvoir le faire aussi.

Si je dois comprendre des propos de mes collègues conservateurs qu'ils entendent essayer de ralentir ou de bloquer le projet de loi, la situation est bien différente d'une étude que nous pourrions mener en sachant que tous les partis vont agir de bonne foi. À titre d'exemple, si nous nous réunissions de 15 h 30 à minuit le lundi, à notre retour lors de cette deuxième semaine, nous devrions être en mesure de faire de réels progrès, pour autant, bien évidemment, que tous les partis aient vraiment l'intention d'améliorer le projet de loi. Il y a en effet une différence entre une séance prolongée avec obstruction et une séance prolongée au cours de laquelle nous travaillons systématiquement à l'analyse des amendements proposés.

Nous convenons tous que ce projet de loi doit être amélioré. Je crois sincèrement que nous pouvons le faire lors de la semaine suivant notre deuxième retour. Ainsi, nous pourrions consacrer notre prochaine semaine de séance à notre étude sur les vols d'automobile. Si nous nous entendons pour tenir des audiences prolongées au cours de cette deuxième semaine de séance, je pense qu'aucun parti ne s'opposera à ce que nous tenions deux réunions sur les vols d'automobile dans deux semaines d'ici. Mais si nous ne nous entendons pas pour prolonger les audiences au cours de cette deuxième semaine, je pense que la question de la première semaine deviendra plus problématique.

Si nous travaillons tous ensemble pour améliorer ce projet de loi, le faire adopter par le Comité et le renvoyer à la Chambre, alors je pense que nous avons ici une stratégie: deux réunions sur les vols d'automobile dans deux semaines; une date limite pour le dépôt des amendements la semaine suivante; puis, à notre retour, des audiences prolongées, y compris peut-être une réunion supplémentaire le mardi soir pour nous permettre d'examiner les amendements.

Le président: Merci.

Madame Michaud, vous avez la parole.

[*Français*]

Mme Kristina Michaud: Merci.

J'aimerais que nous récapitulions nos discussions au sujet des dates.

Je ne pense pas que ce soit une mauvaise idée de prolonger les heures de réunion. Siéger jusqu'à minuit, cela ressemble un peu à une procédure de bâillon.

Je conviens que nous pourrions en faire plus dans une période de quatre ou cinq heures, comme le lundi soir de 16 h 30 à 20 h 30 ou 21 h 30. Je n'y vois pas d'inconvénient.

Vous me confirmerez, monsieur le président, que nous pourrions fixer la date de dépôt des amendements au 26 février et que la réunion du 26 février porterait sur les vols de voitures.

À la rencontre du jeudi 29 février, nous commencerions l'étude du projet de loi C-26. À cette date, le greffier nous aurait déjà transmis les amendements proposés par les autres partis, parce que nous devons nous accorder un moment pour étudier ces amendements.

Comme ce sera le jeudi matin, nous ne pourrons pas vraiment prolonger cette réunion. Cela nous amène alors deux semaines plus tard, au lundi 18 mars. J'imagine que c'est à cette réunion que nous prolongerions un peu les heures. Le jeudi, nous recevrions M. LeBlanc.

Nous poursuivrions donc l'étude du projet de loi C-26 le 8 avril.

Est-ce que je me trompe, monsieur le président?

[*Traduction*]

Le président: Merci.

Je tiens simplement à souligner que le greffier vient de m'indiquer que les amendements devront être transmis au plus tard le 26 février, à midi.

C'est à vous, monsieur Shipley.

M. Doug Shipley: Merci, monsieur le président.

Beaucoup de dates ont été mentionnées.

Monsieur Julian, je pense que vous avez trouvé une bonne solution. J'espère avoir bien saisi ce que vous proposiez. Sinon, n'hésitez pas à me corriger.

Pendant la semaine suivant notre premier retour, nous traiterions des vols d'automobile le lundi et le jeudi, puis, lorsque nous reviendrons pour la semaine de séance suivante, nous pourrions tenir des réunions prolongées. Je pense que nous pouvons nous entendre là-dessus.

M. Peter Julian: C'est en quelque sorte un échange de bons procédés. S'il y a consentement pour prolonger les audiences afin d'examiner les amendements le lundi et peut-être aussi le mardi à notre retour, alors je pense que tout le monde serait d'accord pour consacrer ces deux journées aux vols de voiture.

M. Doug Shipley: Monsieur le président, je suis désolé, mais j'aimerais tenter de résumer le tout. Nous serons la semaine prochaine dans nos circonscriptions respectives. La première semaine après notre retour, les deux réunions porteraient sur les vols d'automobile et, à notre retour suivant, nous tiendrions des séances prolongées pour l'étude du projet de loi C-26. Est-ce bien ce que vous proposez, monsieur Julian?

M. Peter Julian: C'est exactement ce que je propose.

M. Doug Shipley: Je pense que c'est un bon compromis. Nous sommes d'accord, monsieur Julian.

Un député: Il est entendu que le lundi de notre retour...

Le président: Nous vous écoutons, madame O'Connell.

Mme Jennifer O'Connell: Merci.

Monsieur le président, je sais bien qu'il faut aussi du temps pour examiner les amendements, mais s'il y a des heures disponibles, même au cours de cette semaine du 26 février, pourquoi ne pourrions-nous pas enquérir de la possibilité de tenir des réunions supplémentaires? Nous pourrions quand même nous pencher sur les vols de voiture dans le cadre de nos réunions régulières, mais demander qu'on nous réserve des créneaux additionnels si la chose est possible.

Nous pourrions mener les deux études de front, mais nous vous laissons le soin de trouver une solution.

● (1020)

Le président: D'accord. Nous verrons bien si la magie de la présidence opérera.

M. Dane Lloyd: Je suis un peu inquiet de devoir m'en remettre à votre magie.

Le président: C'était peut-être un mauvais choix de mots.

M. Dane Lloyd: Je pense qu'il est convenu, du moins pour la majorité des membres du Comité, que nous voulons consacrer deux journées aux vols d'automobile lors de la prochaine semaine de séance avant de tenir des réunions prolongées à compter du mois de mars pour l'étude du projet de loi C-26. C'est du moins ce que j'ai cru comprendre.

Je veux tout simplement éviter toute mauvaise surprise. Je ne voudrais surtout pas recevoir un avis nous conviant à une séance de très longue durée d'ici la fin février alors même qu'il n'est pas très clair que le Comité a donné son accord.

Le président: Je pense que la présidence a pu entendre tous les points de vue exprimés de part et d'autre. J'en tiendrai compte dans mes échanges avec notre greffier.

M. Dane Lloyd: Vous savez que lorsque nous n'avons pas l'impression d'être vraiment consultés ou écoutés, nous avons tendance à adopter certains comportements.

Le président: C'est votre prérogative, monsieur Lloyd.

M. Ron McKinnon: Monsieur le président, il ne faut pas oublier de tenir compte du temps dont le greffier législatif aura besoin pour passer en revue les amendements. Je pense qu'il lui faudra sans doute quelques jours pour s'acquitter de cette tâche.

Le président: Monsieur Shipley, vous avez la parole.

M. Doug Shipley: Merci, monsieur le président.

Je serai très bref. Nous avons évoqué notre étude sur les vols de voiture, mais nous n'avons pas discuté des ministres qui pourraient être convoqués lors des audiences à ce sujet. Nous suggérons que le ministre de la Justice, le ministre de la Sécurité publique et le ministre des Transports soient tous invités si tous les membres du Comité conviennent qu'il serait important d'entendre ces trois ministres à propos de cet enjeu d'importance.

Je pense que ces propositions pourraient sans doute faire l'unanimité, monsieur le président.

M. Ron McKinnon: Nous pouvons toujours inviter des ministres, mais nous ne savons pas s'ils seront bel et bien disponibles, n'est-ce pas?

Le président: Madame O'Connell, vous pouvez réagir.

Mme Jennifer O'Connell: Merci.

Je pense qu'il est préférable de ne pas prendre de décision à la hâte. Le Comité a adopté une motion, et nous devrions nous en tenir à ce que prévoit cette motion. Par la suite, si nous devons inviter d'autres témoins, le Comité pourra toujours le faire. On ne peut pas se contenter de proposer ainsi des témoins à l'improviste; il faut respecter la motion qui a été adoptée à l'unanimité par le Comité.

Je crois que c'est la bonne façon de faire les choses, plutôt que de simplement ajouter des témoins au gré des propositions de l'un et de l'autre, alors que nous avons déjà dépassé le temps alloué au Comité. Il y a un processus à suivre.

Le président: Allez-y, monsieur Motz.

M. Glen Motz: Merci, monsieur le président.

Pour que les choses soient bien claires, les amendements doivent être transmis au plus tard le 26 février. Pour les 26 et 29 février, il est suggéré que nous amorcions notre étude sur les vols d'automobile. C'est ce que la majorité constituée par les députés de l'opposition a proposé. Ensuite, le lundi 18 mars, nous commencerions l'étude article par article du projet de loi C-26 en gardant à l'esprit que ce jour-là, le lundi 18, nous prolongerions nos heures de réunion pendant une période raisonnable si les ressources disponibles le permettent. Je pense qu'il serait tout à fait sensé de commencer l'étude du projet de loi C-26 à ce moment-là.

Le président: Merci, monsieur Motz.

Monsieur Julian, à vous la parole.

M. Peter Julian: Je suppose que la date limite pour proposer des témoins aux fins de l'étude sur les vols de voiture est fixée à lundi?

Le président: Je crois que vous avez déjà soumis vos propositions.

M. Peter Julian: Merci. Je suggérerais que, si quelqu'un souhaite proposer d'autres témoins, il le fasse d'ici lundi.

Le président: Merci.

D'accord. Vous pouvez donc vous en remettre à la présidence.

Pour le projet de loi C-26, le greffier a distribué lundi une ébauche de budget au montant de 14 500 $.

Y a-t-il des questions ou des commentaires?

M. Chris Bittle: J'en fais la proposition.

Le président: La motion est proposée. Parfait.

Nous allons maintenant passer à un nouveau budget de déplacement concernant notre étude du problème grandissant des vols de voiture.

À la demande des membres du Comité qui souhaitaient réduire le plus possible les coûts engagés pour cette visite, notre greffier vous a soumis deux nouvelles options de budget pour un déplacement vers le port de Montréal aux fins de cette étude.

Dans le premier cas, un autobus serait affrété pour un coût total de 8 199 $. Dans le deuxième cas, nous opterions pour le train avec navette en autobus pour un montant cumulé de 9 399 $.

Notre greffier pourra vous fournir de plus amples détails au besoin.

Oui, monsieur McKinnon.

● (1025)

M. Ron McKinnon: Monsieur le président, question procédure, la motion a été proposée pour le premier budget, mais nous ne nous sommes pas prononcés.

Tout cela est approuvé. D'accord.

Le président: Après discussion avec notre greffier, je recommanderais que nous adoptions les deux options budgétaires afin d'offrir une plus grande souplesse lors de la prochaine étape d'approbation devant le Sous-comité des budgets de comité du Comité de liaison.

Est-ce que cela vous convient?

Des députés: D'accord.

Le président: Plaît-il au Comité que la séance soit levée?

Des députés: D'accord.