CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

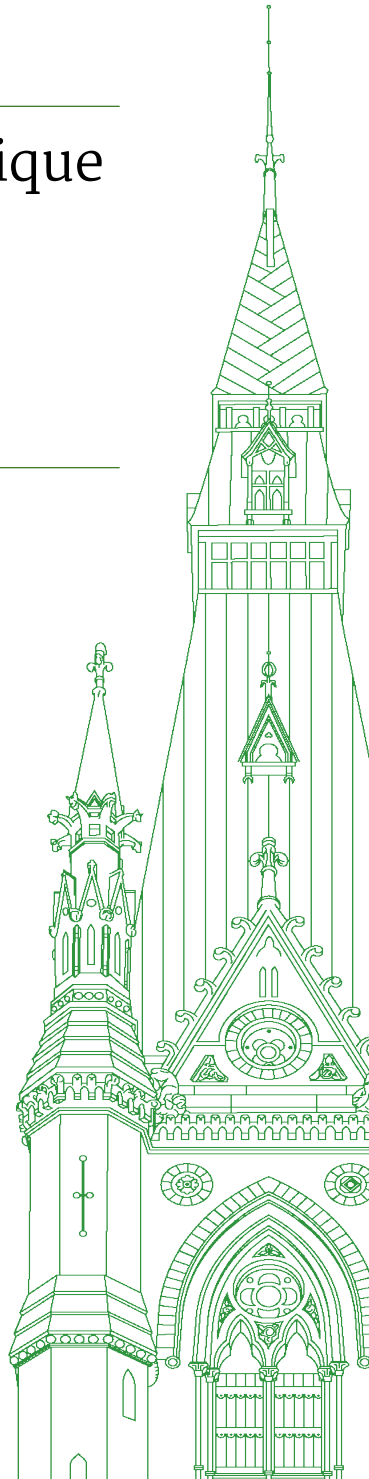
45e LÉGISLATURE, 1re SESSION

Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 018

Le jeudi 4 décembre 2025



Président : Jean-Yves Duclos

Comité permanent de la sécurité publique et nationale

Le jeudi 4 décembre 2025

● (1105)

[*Français*]

La vice-présidente (Claude DeBellefeuille (Beauharnois—Salaberry—Soulanges—Huntingdon, BQ)): Bonjour, tout le monde. J'ouvre la séance.

Bienvenue à la 18e réunion du Comité permanent de la sécurité publique et nationale de la Chambre des communes.

Conformément à l'article 108(2) du Règlement et à l'ordre de renvoi de la Chambre du 3 octobre 2025, le Comité se réunit dans le cadre de son étude du projet de loi C-8, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois.

Avant de souhaiter la bienvenue aux témoins, étant donné que je préside la réunion d'aujourd'hui, j'aimerais demander le consentement de tous les membres du Comité pour garder mon privilège d'avoir un tour de parole de six minutes et un autre de deux minutes pour poser des questions aux témoins.

Ai-je le consentement unanime du Comité à cet effet?

Des députés: D'accord.

La vice-présidente (Claude DeBellefeuille): Merci beaucoup.

J'aimerais maintenant souhaiter la bienvenue aux témoins que nous recevons pour la première heure de la rencontre.

Nous recevons d'abord à titre personnel Mme Kate Robertson, qui est associée de recherche principale au Citizen Lab de l'Université de Toronto. Elle participe à la rencontre par vidéoconférence.

De plus, nous avons parmi nous M. John de Boer, qui est vice-président aux relations gouvernementales de BlackBerry.

Enfin, nous recevons également par vidéoconférence M. Matthew Hatfield, qui est directeur général d'OpenMedia.

Vous êtes tous les bienvenus.

Nous débutons par vous, madame Robertson. Vous avez cinq minutes pour votre allocution d'ouverture.

[*Traduction*]

Kate Robertson (associée de recherche principale, Citizen Lab, University of Toronto, à titre personnel): Bonjour. Je vous remercie.

Je m'appelle Kate Robertson. Je suis avocate et actuellement chercheuse au Citizen Lab de l'Université de Toronto.

Mes commentaires s'appuient sur les recherches du Citizen Lab en matière de cybersécurité et de télécommunications, ainsi que sur l'analyse du droit constitutionnel que j'ai soumise dans un mémoire au Comité.

La deuxième et la troisième partie de mon mémoire présentent des modifications visant à combler les lacunes constitutionnelles et à réduire les risques liés à la cybersécurité dans le projet de loi. Dans l'introduction du mémoire, deux priorités sont cernées en ce qui concerne les modifications recommandées.

La première consiste à protéger explicitement la technologie de chiffrement dans les réseaux de télécommunications canadiens. À l'heure actuelle, les vastes pouvoirs prévus dans le projet de loi pourraient avoir pour effet de compromettre les normes de chiffrement à des fins d'accès légal.

Par exemple, en vertu de l'article 15.2 de la Partie 1 du projet de loi, le ministre pourrait exiger que les fournisseurs de services de télécommunications mettent en œuvre « des normes qu'il précise ». Le ministre pourrait aussi interdire aux fournisseurs de services de télécommunications d'utiliser « les produits ou les services qu'il précise ». Le ministre pourrait également « imposer des conditions quant à leur utilisation de produits ou de services ». Ce ne sont là que quelques exemples.

Même si les responsables ont précisé que cette loi n'est pas un projet de loi sur la surveillance et que ces dispositions n'autorisent pas la compromission du chiffrement, aucune disposition explicite ne le garantit. Un futur gouvernement pourrait interpréter l'article 15.2 proposé de manière très différente en faisant valoir que le renforcement des capacités de surveillance favoriserait les intérêts du Canada en matière de sécurité. Une disposition interprétative est donc essentielle pour protéger le chiffrement, qui est une forme essentielle de cybersécurité.

Dans mon mémoire, je souligne que le projet de loi C-2 récemment déposé, qui propose également de vastes pouvoirs pour ordonner des modifications aux réseaux de télécommunications, contient une disposition distincte qui représente, selon le gouvernement, un moyen proposé pour garantir qu'aucun arrêté ne puisse compromettre le chiffrement. En revanche, il n'y a toujours rien de comparable dans le projet de loi C-8.

La huitième recommandation énoncée dans mon mémoire suggère d'ajouter une disposition selon laquelle les arrêtés ne peuvent pas être utilisés pour compromettre la confidentialité, la disponibilité ou l'intégrité d'un service de télécommunications. Cette formulation est largement utilisée pour décrire les trois éléments essentiels d'une cybersécurité élevée. Elle est d'ailleurs utilisée par les organismes fédéraux au Canada.

Je peux également répondre à des questions sur d'autres formulations qui seraient également envisageables. Je peux envoyer ces suggestions par écrit après la réunion, si cela peut vous être utile.

Au bout du compte, puisque l'intention du projet de loi, comme on nous l'a dit, n'est pas la surveillance ou le contournement du chiffrement, cela ne devrait pas constituer une amélioration controversée au projet de loi.

La deuxième priorité concerne le fait que le pouvoir de collecte étendu et sans mandat prévu à l'article 15.4 proposé constitue une lacune constitutionnelle importante. Comme nous le savons, les fournisseurs de services de télécommunications sont les vecteurs des renseignements les plus confidentiels connus de notre système juridique. Je me permets de ne pas partager l'avis selon lequel cette loi ne s'appliquerait qu'aux renseignements techniques. Le libellé de la loi — qui est l'élément important, au bout du compte — crée un vaste pouvoir qui permet de collecter, sans mandat, des renseignements personnels et dépersonnalisés auprès des entreprises de télécommunications.

Je partage l'avis du commissaire au renseignement du Canada — qui a déjà témoigné — selon lequel les pouvoirs de perquisition et de saisie sans mandat constituent une lacune constitutionnelle dans le projet de loi et qu'aucune justification apparente n'a été fournie. Je suis d'accord avec la recommandation de M. Noël selon laquelle on devrait apporter un changement important pour exiger que l'utilisation des renseignements par le Centre de la sécurité des télécommunications soit soumise à une autorisation ministérielle annuelle et, au bout du compte, à l'approbation du commissaire au renseignement. Il s'agirait d'une amélioration importante, mais comme il l'a fait remarquer, il subsisterait une lacune générale dans le projet de loi C-8 en ce qui concerne la collecte sans mandat, un problème qu'il a déclaré vouloir laisser à d'autres le soin de régler.

La troisième recommandation indiquée dans mon mémoire comblerait cette lacune plus importante en proposant que la collecte de renseignements personnels et dépersonnalisés soit soumise à l'autorisation de la Cour fédérale. Cette mesure est essentielle pour donner au projet de loi C-8 une assise constitutionnelle beaucoup plus solide.

Étant donné le temps dont je dispose, j'invite les membres du Comité à me poser une question sur les raisons pour lesquelles les garanties actuelles prévues dans le projet de loi, qui sont pour la plupart inapplicables au pouvoir de collecte prévu à l'article 15.4, sont insuffisantes pour remédier à cette lacune constitutionnelle.

Je vous remercie. Veuillez consulter mon mémoire pour connaître mes autres recommandations.

● (1110)

[*Français*]

La vice-présidente (Claude DeBellefeuille): Merci beaucoup, madame Robertson.

Nous passons maintenant à vous, monsieur de Boer. Vous avez cinq minutes pour votre allocution d'ouverture.

John de Boer (vice-président, Relations gouvernementales, BlackBerry): Merci, madame la présidente.

[*Traduction*]

Lorsque les Canadiens montent dans leur voiture, ils sont convaincus que les systèmes essentiels à la sécurité fonctionneront parfaitement. Lorsque les systèmes d'automatisation industrielle assurent le bon fonctionnement de nos réseaux énergétiques, nous sommes convaincus qu'ils fonctionneront comme prévu. C'est cette confiance que BlackBerry offre chaque jour.

Notre système d'exploitation QNX est intégré dans plus de 255 millions de véhicules actuellement en circulation. Il alimente des systèmes de contrôle industriels, des centrales nucléaires et des systèmes autonomes dans des environnements essentiels à la mission où la sécurité, la fiabilité et la performance sont des éléments indispensables. On compte sur le système QNX pour garantir la sécurité et la fiabilité de ces systèmes, car l'échec n'est pas envisageable. Notre responsabilité ne s'arrête pas là.

Nous protégeons les systèmes qui permettent aux dirigeants de rester en communication pendant les crises et les systèmes qui coordonnent les interventions d'urgence lorsque chaque seconde compte. Lorsqu'une cyberattaque menace un réseau électrique et perturbe les réseaux de transport ou lorsqu'un incident de sécurité nationale exige une action immédiate, BlackBerry veille à ce que les renseignements de nature délicate restent sûrs et que les décideurs puissent communiquer sans craindre d'être interceptés ou compromis.

Notre mission est simple. Nous préservons l'intégrité des opérations essentielles, afin que les gouvernements et les services essentiels puissent réagir rapidement et en toute confiance. Dans ces moments-là, la confiance n'est pas facultative. Elle est nécessaire. C'est la raison pour laquelle les banques, les fournisseurs d'énergie, les fournisseurs de services de télécommunications et les agences de transport font confiance à BlackBerry. Dès le départ, notre entreprise a été fondée dans un souci de sécurité.

BlackBerry appuie fermement le projet de loi C-8, et surtout la Partie 2 du projet de loi. En effet, les infrastructures essentielles sont de plus en plus numériques, ce qui en fait une cible de choix pour les cybercriminels et les acteurs parrainés par un État.

Les enjeux sont considérables. Ces systèmes fournissent des services essentiels et hébergent des données de nature délicate. Une seule violation peut avoir une série de répercussions au-delà des frontières et des secteurs. Le Canada est le seul pays du G7 à ne pas avoir de système de signalement obligatoire des incidents de cybersécurité liés aux infrastructures essentielles. Il est temps d'harmoniser et de renforcer nos systèmes de cyberdéfense.

Le projet de loi C-8 constitue une avancée majeure. Il améliorera la connaissance de la situation et la réponse collective, il renforcera l'apprentissage organisationnel en vue de cerner les risques systémiques et d'éclairer les pratiques cybernétiques, et il améliorera la gouvernance d'entreprise en élevant la cybersécurité au niveau du conseil d'administration.

L'expérience mondiale montre que ces lois sont efficaces. Par exemple, la loi américaine de 2022 sur la déclaration des incidents cybernétiques pour les infrastructures essentielles a permis d'accélérer le déploiement des ressources, l'analyse des tendances et le partage de renseignements. Selon les responsables, cela permet de repérer plus tôt les campagnes adverses et de prendre des mesures coordonnées. La directive SRI 2 de l'Union européenne et la loi australienne sur la sécurité des infrastructures essentielles présentent des avantages comparables.

La réussite dépend de trois facteurs. Le premier est la rapidité. Un signalement rapide permet une réponse rapide. Le deuxième est une définition claire de ce qui constitue un incident à signaler. Le troisième est l'accès à des outils sécurisés et certifiés de signalement des incidents et de gestion des événements critiques qui permettent aux parties prenantes de communiquer en cas de crise.

Le Canada a besoin de cette rapidité et de cette clarté. Le rapport de la vérificatrice générale d'octobre 2025 a révélé que la réponse du Canada à une cyberattaque majeure avait été retardée de sept jours en raison de protocoles incomplets et de l'absence d'un outil permettant un partage sécurisé des renseignements. Ce retard a donné aux attaquants plus de temps pour accéder à des renseignements de nature délicate. Le signalement obligatoire doit donc être accompagné d'outils et de procédures permettant une communication fluide.

Nous recommandons cinq mesures pour rendre la loi plus efficace. Tout d'abord, il faut définir clairement et de manière cohérente ce que représente un « incident devant être signalé ». Deuxièmement, il faut rendre obligatoire la déclaration rapide des incidents grâce à une approche à plusieurs étapes et à un avis initial dans les 72 heures, suivi d'un rapport détaillé. Troisièmement, il faut donner accès à des outils sécurisés pour la communication et la coordination en temps réel. Quatrièmement, il faut garantir la protection en matière de responsabilité pour les signalements faits de bonne foi. Cinquièmement, il faut que la continuité des activités fasse partie des exigences fondamentales pour veiller à ce que les entités puissent communiquer, se mobiliser et rétablir rapidement les services.

En conclusion, grâce au projet de loi C-8, le Canada passerait d'un ensemble disparate de lignes directrices volontaires à un cadre obligatoire qui tient compte des pratiques exemplaires à l'échelle mondiale.

● (1115)

Je vous remercie.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Merci.

Je passe maintenant la parole à Matthew Hatfield, d'OpenMedia, pour cinq minutes.

[*Traduction*]

Matthew Hatfield (directeur exécutif, OpenMedia): Bonjour.

Je m'appelle Matt Hatfield, et je suis directeur général d'OpenMedia, une communauté populaire de 230 000 personnes au Canada qui travaillent ensemble pour favoriser un Internet ouvert, accessible et sans surveillance. Je vous parle depuis le territoire non cédé de la Première nation de Tsawout, sur l'Île Salt Spring, en Colombie-Britannique.

Toute lacune doit être prise en considération. En effet, si vous adoptez ce projet de loi et qu'il contient une lacune importante, cette lacune ne fera pas qu'affaiblir le projet de loi; elle aura aussi une incidence bien plus importante que l'objectif visé par la loi. À l'heure actuelle, le projet de loi C-8 contient plusieurs lacunes graves que vous devez corriger.

Le projet de loi C-8 s'appuie sur le projet de loi C-26, Loi concernant la cybersécurité, qui a été adopté l'année dernière par le comité précédent, et il lui ressemble beaucoup. Ces deux projets de loi donnent aux futurs ministres de l'Industrie le pouvoir de déconnecter de manière permanente et secrète les citoyens canadiens d'Internet sans les en informer ou leur expliquer leur décision, de prendre des arrêtés qui ordonnent aux entreprises de télécommunications de faire ou de ne pas faire toute chose que le ministre juge nécessaire pour protéger notre infrastructure de télécommunications, et de vous tenir, vous, nos représentants élus, dans l'ignorance totale du contenu de ces arrêtés. C'est tout simplement un pouvoir trop important qui ne fait l'objet d'aucune surveillance. Le Canada a besoin de lois en matière de cybersécurité, mais vous ne devriez pas adopter le projet de loi dans sa forme actuelle.

Le paragraphe 15.2(2) proposé confère au ministre le pouvoir d'ordonner aux fournisseurs de services de télécommunications de faire ou de ne pas faire tout ce qu'il juge nécessaire pour sécuriser le système de télécommunications canadien. De manière plus constructive, le projet de loi C-8 précise désormais que le ministre doit utiliser ces pouvoirs de manière raisonnable et conforme à l'objectif de la loi.

Qui décidera si cette norme est respectée? Ce n'est pas le public. Nous ne sommes informés de l'existence de ces arrêtés que dans un rapport annuel. Ce ne sont pas vos collègues du Comité des parlementaires sur la sécurité nationale et le renseignement. Le ministre doit seulement vous expliquer pourquoi il estime que ces mesures sont raisonnables, sans avoir à vous prouver qu'elles le sont. Ce n'est pas de la transparence et de la reddition de comptes, c'est du théâtre. Le ministre est tenu de réfléchir sérieusement à la question de savoir si ses décisions sont raisonnables et proportionnées et de vous promettre par écrit qu'elles le sont, mais aucune surveillance n'est exercée pour vérifier si c'est bien le cas. Cela ressemble beaucoup à une loi qui m'obligerait à vous donner de très bonnes raisons pour justifier le fait que j'ai la main dans le sac, mais qui ne vous permet pas de vérifier ce que je fais réellement dans le sac.

Nos alliés démocratiques ne rédigent pas de loi comme celle-ci. Au Royaume-Uni, le gouvernement ne peut pas émettre ce type d'arrêté sans consulter l'Ofcom, un organisme de réglementation indépendant. Les différentes utilisations des pouvoirs en matière d'arrêtés nécessitent l'approbation d'un comité technique indépendant, d'un juge chargé de l'examen ou des deux. Toutefois, dans le projet de loi C-8, le ministre décide seul.

En Australie, si une entreprise de télécommunications estime qu'un arrêté pourrait compromettre la confidentialité ou la sécurité de son réseau, elle peut exiger un examen technique par un juge indépendant et un expert technique. Au Canada, le ministre prend ses décisions seul. De plus, ce n'est pas une coïncidence si ces examens d'experts qui sont intégrés dans la loi protègent également le gouvernement contre la création accidentelle de catastrophes techniques par la prise d'arrêtés dont il ne comprend pas les conséquences et qui nuisent à l'infrastructure des télécommunications plutôt que de la protéger.

L'approche du Canada, madame la présidente, ne s'appuie pas sur un système de freins et de contrepoids démocratiques. On donne plutôt aux futurs ministres carte blanche pour mettre en place un système d'arrêtés secrets et permanents dont le caractère raisonnable et proportionné est laissé entièrement à leur discrétion, et les corrections nécessaires ressemblent à celles des dernières étapes du projet de loi C-26.

Tout d'abord, les nouveaux pouvoirs du gouvernement doivent être limités par un examen indépendant. L'avis du ministre selon lequel ses arrêtés sont nécessaires et proportionnés n'est pas suffisant. Un juge et un expert technique devraient avoir pleinement accès à ces arrêtés avant leur publication ou, en cas d'urgence, dans les 30 jours, et ils devraient avoir la possibilité d'annuler les arrêtés qui vont trop loin.

Deuxièmement, l'objectif légitime du projet de loi C-8 est la protection systémique des infrastructures, et non pas la surveillance abusive des Canadiens. Cela signifie que le projet de loi doit interdire explicitement les arrêtés qui ont pour effet de créer une faiblesse systémique ou un chiffrement détourné, un libellé que nos alliés australiens ont déjà utilisé. Si la porte est ouverte au ministre, elle l'est aussi aux pirates informatiques.

En outre, les renseignements personnels doivent être clairement définis comme étant confidentiels et, s'ils sont collectés de manière fortuite dans le cadre de l'application du projet de loi C-8, ils doivent être rapidement détruits. En toutes circonstances, le projet de loi C-8 doit interdire le partage des renseignements personnels collectés en vertu de celui-ci avec des agences de renseignement étrangères qui ne sont pas assujetties à nos lois.

Troisièmement, le gouvernement ne doit pas être autorisé à garder secrète de manière permanente la manière dont il utilise ces nouveaux pouvoirs, ni à votre égard ni à l'égard du public. En dehors des situations d'urgence immédiate, la norme de divulgation des activités menées en vertu du projet de loi C-8 devrait être un niveau plus élevé que ce qui est actuellement requis. Cela signifie que le public devrait être informé non seulement du nombre d'arrêtés pris, mais aussi de la description par le ministre de ce qu'ils accomplissent et des raisons pour lesquelles ils sont nécessaires. Le Comité des parlementaires sur la sécurité nationale et le renseignement devrait recevoir une description complète des arrêtés, afin que les députés puissent déterminer si le rapport public du ministre dit la vérité aux Canadiens.

Plus de 10 000 Canadiens ont écrit à notre gouvernement pour demander que cette loi en matière de cybersécurité ne soit adoptée que si elle prévoit des mesures de protection des droits robustes. C'est votre travail. Nous vous prions instamment d'écouter ces électeurs et d'adopter les amendements que la société civile vous a soumis, afin que cette loi soit ce qu'elle devrait être.

Je vous remercie. J'ai hâte de répondre à vos questions.

● (1120)

[*Français*]

La vice-présidente (Claude DeBellefeuille): Merci beaucoup, monsieur Hatfield.

Je remercie les témoins de leurs présentations.

Nous allons maintenant passer aux questions des députés. Nous commençons par un tour de six minutes pour M. Lloyd.

[*Traduction*]

Dane Lloyd (Parkland, PCC): Je vous remercie.

Je remercie les témoins d'être ici aujourd'hui.

J'aimerais poser ma première question à M. Hatfield.

Vous avez dit qu'aucune surveillance n'était exercée lorsque le ministre prend une décision, et le projet de loi indique que cette décision doit être raisonnable. Étant donné que ces pouvoirs auraient principalement une incidence sur les fournisseurs de services de télécommunications, mais aussi, dans certains cas, sur des particuliers, comme on l'a précisé, ces personnes ne peuvent-elles pas demander un examen judiciaire de ces décisions et, si un juge estime qu'ils ne sont pas raisonnables, faire annuler les arrêtés en question? Ne serait-ce pas une protection?

Matthew Hatfield: Je laisserai à ma collègue, Mme Robertson, le soin de vous donner l'avis d'une avocate à ce sujet.

Pour ma part, je m'exprime à titre de défenseur de l'intérêt public.

Si quelqu'un finit par obtenir l'annulation d'une décision, cela pourrait prendre des mois, voire des années, avant qu'elle ne soit modifiée. Bien entendu, de nombreuses personnes au Canada n'auraient pas les ressources ou les connaissances nécessaires pour contester ces arrêtés. Je ne pense pas que cela soit aussi efficace qu'un processus intégré que le gouvernement serait obligé de suivre pour engager une procédure ultérieure.

Kate Robertson: En vertu de la Constitution, les tribunaux rechercheront un système de reddition de comptes digne de ce nom. En l'absence de transparence, d'un avis aux personnes concernées, y compris le besoin éventuel de bâillons stricts qui empêcheraient certaines personnes de savoir que leur vie privée ou d'autres intérêts ont été touchés, cela entrave leur capacité à accéder aux mécanismes d'examen. À cet égard, l'examen judiciaire est donc insuffisant d'un point de vue constitutionnel.

Je tiens également à souligner qu'il existe une norme raisonnable optimale et qu'une présomption de déférence s'applique, et c'est la raison pour laquelle j'ai recommandé de prévoir une disposition qui précise qu'il ne s'agit pas de surveillance, mais de cybersécurité, car en l'absence d'une telle disposition interprétative, cela serait également évalué selon une norme différente dans le cadre du processus d'examen judiciaire.

● (1125)

Dane Lloyd: Madame Robertson, des représentants de la Canadian Constitution Foundation m'ont dit que même si un bâillon est prononcé à l'encontre d'une personne, cette personne conserve son droit de demander un examen judiciaire. N'est-ce pas le cas?

Kate Robertson: C'est juste, mais s'ils ne sont pas eux-mêmes visés par la consigne du silence, ils ne seraient pas au courant de l'existence des décrets du gouvernement ou des mesures prises ultérieurement par les fournisseurs de services de télécommunications.

Dane Lloyd: Le ministère nous a dit que toute personne touchée par ces décrets est informée de la situation. N'est-ce pas le cas?

Kate Robertson: C'est faux, et tout dépend vraiment de la nature précise du décret. Ce projet de loi laisse entendre à bien des égards que c'est une question qui regarde les fournisseurs de services de télécommunications et le gouvernement, du point de vue du ministre qui l'a présenté. À bien des égards, je dois dire que le grand public est traité comme s'il ne faisait pas partie de l'équation. S'il y a un décret qui vise une personne en particulier, ce serait différent. Bien souvent, compte tenu de l'objectif du projet de loi et de la façon dont on en a discuté, il s'agit des décrets visant les fournisseurs de services de télécommunications, de sorte que les personnes ne seraient pas avisées.

Dane Lloyd: J'aimerais changer de sujet et parler des règles de cryptage. Quelles parties prenantes seraient les plus préoccupées par la possibilité que le chiffrement soit compromis par ce projet de loi? S'agirait-il de joueurs comme BlackBerry ici aujourd'hui?

Kate Robertson: C'est tout à fait possible.

Je salue l'enquête que la CBC a menée en 2017 ayant révélé une chose. Lorsqu'un journaliste d'enquête a donné à un chercheur en sécurité le numéro de téléphone d'un député, il a pu intercepter les lieux, les messages textes et les communications de ce député — c'était consensuel, mais c'est pour illustrer le problème. Cela montre vraiment les points faibles systémiques inhérents aux réseaux de communication mobile dans le monde. C'est ce que nous espérons que la technologie 5G et 6G nous aideront à résoudre, notamment par l'introduction de caractéristiques de sécurité robustes, y compris le chiffrement.

Dane Lloyd: Je vous remercie. Je suis désolé, mais mon temps est limité.

Monsieur de Boer, vous êtes ici pour représenter le secteur des télécommunications. Je me demande pourquoi vous n'avez pas soulevé de préoccupations à l'égard du chiffrement dans votre témoignage d'aujourd'hui. Est-ce une de vos inquiétudes, et pouvez-vous nous en dire plus à ce sujet?

John de Boer: Du point de vue de BlackBerry, je pense que la notion de caractère raisonnable est très importante ainsi que celle de contrôle judiciaire, mais nous ne sommes plus dans le domaine des télécommunications.

Dane Lloyd: D'accord.

John de Boer: Nous nous concentrons davantage sur la cybersécurité.

Dane Lloyd: Chez BlackBerry, composez-vous avec le chiffrement?

John de Boer: Nous traitons avec le chiffrement.

Dane Lloyd: Craignez-vous que les dispositions du projet de loi C-8 permettent au gouvernement de déjouer votre chiffrement ou de vous forcer légalement à enfreindre vos normes à ce chapitre?

John de Boer: Nous serons préoccupés si cela se concrétise, mais nous aimerions qu'il y ait un contrôle judiciaire et un droit au caractère raisonnable.

Dane Lloyd: Pensez-vous que les dispositions de ce projet de loi donnent au gouvernement le pouvoir de le faire?

John de Boer: Je ne suis pas vraiment en mesure de me prononcer là-dessus. Ce n'est pas mon domaine.

Dane Lloyd: C'est une grande préoccupation qui a été soulevée par de nombreux intervenants. Théoriquement, si le gouvernement venait vous voir et adoptait un décret qui semble enfreindre les normes de chiffrement de votre entreprise, quelle serait la réponse de BlackBerry?

John de Boer: Ce serait un problème.

Dane Lloyd: Votre entreprise demanderait-elle un contrôle judiciaire de la décision avant de s'y conformer ou...?

John de Boer: Ce serait au cas par cas. Je ne peux pas me prononcer sur un scénario fictif, mais nous l'examinerions certainement.

Dane Lloyd: Oui, de nombreux témoins ont décrit ce scénario comme étant très réel, et c'est préoccupant. Je vous remercie.

Je ne sais pas si vous pourriez fournir des renseignements au Comité par la suite. Si vous pouviez obtenir cette information...

John de Boer: Je le ferai avec plaisir.

Dane Lloyd: ... ce serait vraiment utile au Comité.

Merci.

Je pense que mon temps est écoulé.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Merci beaucoup, monsieur Lloyd. Vous me rendez la vie facile en vous arrêtant un peu avant la fin de votre temps de parole.

Je cède maintenant la parole à Mme Acan pour six minutes.

Sima Acan (Oakville-Ouest, Lib.): Merci, madame la présidente.

[*Traduction*]

Monsieur de Boer, j'ai un diplôme en génie électronique, et je me suis spécialisée en télécommunications. Au fil des ans, j'ai travaillé dans le domaine de l'automatisation industrielle, que vous avez mentionnée, et de la robotique, où la communication et la cybersécurité étaient au cœur des activités. C'est pourquoi mes questions s'adresseront à vous.

Vous avez déjà témoigné en faveur des objectifs du projet de loi C-26, qui était la version précédente de celui dont nous sommes saisis. Compte tenu de l'ampleur des cybermenaces qui pèsent sur les services essentiels, pouvez-vous nous expliquer pourquoi un cadre législatif comme le projet de loi C-8 est nécessaire à la situation du Canada en matière de cybersécurité, en particulier dans le secteur des télécommunications sous réglementation fédérale?

● (1130)

John de Boer: Vous savez, comme je l'ai dit dans mon témoignage, le Canada est le seul pays du G7 à ne pas avoir de projet de loi sur le signalement obligatoire des cyberincidents ou de programme de cybersécurité pour les infrastructures essentielles. Il a fallu beaucoup de temps pour en arriver là. Le contexte des menaces a considérablement évolué, de sorte qu'il est absolument essentiel de protéger les services essentiels.

C'est un début. Nous nous concentrons sur quatre secteurs réglementés par le gouvernement fédéral, mais nous savons que des approches similaires doivent également être adoptées dans d'autres secteurs critiques.

En réalité, le Canada travaille en étroite collaboration avec ses alliés. Nous avons des alliés du Groupe des cinq et d'autres. S'ils constatent que nous sommes déphasés et que nos infrastructures essentielles ne sont pas suffisamment protégées, cela pourrait aussi miner la confiance dans nos systèmes. Je pense donc que c'est très important.

Sima Acan: Merci beaucoup.

Vous m'amenez en fait à ma deuxième question.

Vous recommandez d'harmoniser le cadre de cybersécurité du Canada avec ceux des partenaires du Groupe des cinq. Au-delà de la simple observation et du signalement des incidents, quels mécanismes précis adoptés par d'autres pays — comme le Royaume-Uni, l'Australie ou les États-Unis — pour préserver l'équilibre entre les besoins en matière de sécurité opérationnelle et la transparence le Canada devrait-il adopter afin de renforcer le projet de loi C-8?

John de Boer: Un domaine qui pourrait être intéressant serait, tout d'abord, d'assurer une protection de responsabilité pour la déclaration faite de bonne foi. Ce volet du projet de loi doit être renforcé pour cadrer avec les États-Unis, par exemple, ainsi que l'Union européenne et l'Australie.

En ce qui concerne les autres incidents, nous pourrions préciser le type d'incident de cybersécurité qui nécessiterait un signalement. À l'heure actuelle, selon la définition du projet de loi, il s'agit de tout incident qui peut nuire à la continuité ou à la sécurité d'un système critique. Aux États-Unis, en Europe et en Australie, on y a ajouté le mot « important ». Je pense qu'il doit y avoir plus... Je sais que ce sera précisé dans le règlement, mais il est important que nous fassions certaines distinctions.

Sima Acan: Je vous remercie.

Du point de vue d'une entreprise de technologie au service du gouvernement et du secteur privé, comment percevez-vous la nécessité d'élargir la réglementation gouvernementale et les infrastructures essentielles à la sécurité? Comment trouver un juste milieu entre cette obligation et les responsabilités qui sont assumées par les exploitants privés désignés en vertu de la Loi sur la protection des cybersystèmes essentiels proposée?

John de Boer: Pour répondre sans détour, il faut un partenariat public-privé, et je pense que le gouvernement canadien a fait des progrès à cet égard. Il incombe également au secteur privé de veiller à ce que ses produits soient sécuritaires et respectent une norme acceptable expressément pour les infrastructures essentielles. Des notions, comme intégrer la sécurité dès la conception, sont vraiment importantes pour comprendre les risques à la sécurité associés à la chaîne d'approvisionnement des tiers. Pour BlackBerry, c'est la raison pour laquelle nous prenons très au sérieux la certification de nos produits. Nous obtenons des certifications des autorités nationales pour nous assurer que nos produits sont approuvés.

Il est vraiment essentiel que le gouvernement du Canada laisse entendre aux infrastructures essentielles et au reste du pays qu'il est important d'utiliser des produits sûrs. L'industrie privée doit également s'efforcer de fabriquer des produits sûrs au lieu de simplement lancer immédiatement des produits qui pourraient comporter des lacunes. S'occuper de la sécurité après coup ne fonctionne pas.

Sima Acan: Merci beaucoup.

Me reste-t-il du temps, madame la présidente? D'accord.

Dans votre témoignage précédent sur le projet de loi C-26, vous avez expressément recommandé que le projet de loi C-8 harmonise les exigences en matière de signalement des cyberincidents avec celles des pays du Groupe des cinq, comme vous l'avez mentionné. L'un des objectifs du projet de loi C-8 est de moderniser notre cadre de cybersécurité auprès de ces partenaires. Pourriez-vous nous dire comment les dispositions du projet de loi sur le signalement des incidents et l'observation concordent maintenant avec celles de nos partenaires du Groupe des cinq?

John de Boer: Absolument. En ce qui concerne le signalement des incidents et l'observation, comme je l'ai mentionné dans mon témoignage, le signalement des cyberincidents est obligatoire dans 16 secteurs ayant une infrastructure essentielle aux États-Unis. Ils doivent être signalés dans les 24...

● (1135)

[*Français*]

La vice-présidente (Claude DeBellefeuille): Je m'excuse de vous interrompre, monsieur de Boer, mais le temps de parole de Mme Acan est écoulé. Vous pourrez profiter d'un prochain tour pour terminer votre réponse.

C'est maintenant à mon tour de disposer de six minutes pour poser quelques questions aux témoins, comme convenu.

Ma première question s'adresse à Mme Robertson.

Le commissaire à la protection de la vie privée nous a parlé des principes de nécessité et de proportionnalité pour encadrer la collecte et l'échange de renseignements personnels. Ce sont des principes qu'on retrouve dans de nombreuses lois, mais ils ne se trouvent pas de façon systématique dans le projet de loi C-8.

Que pensez-vous de l'introduction systématique de ces principes dans le projet de loi C-8?

[*Traduction*]

Kate Robertson: Je suis tout à fait d'accord avec le commissaire à la protection de la vie privée du Canada. Je suis tellement d'accord que la recommandation 5 de mon mémoire fait les mêmes suggestions.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Excusez-moi, madame Robertson, mais je m'aperçois que l'interprétation en français ne fonctionne pas. Comme c'est moi qui préside la séance, je me permets de vous interrompre pour le signaler.

[*Traduction*]

Le greffier du Comité (Andrew Wilson): Je veux juste vérifier si l'interprétation fonctionne en français.

Elle fonctionne. Je vous remercie.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Merci.

Pourriez-vous reprendre votre réponse, madame Robertson?

[*Traduction*]

Kate Robertson: Je m'excuse de ne pas pouvoir répondre en français.

Comme je l'ai indiqué, je suis tout à fait d'accord avec les observations du commissaire à la protection de la vie privée du Canada sur l'importance d'apporter cet amendement à la législation. C'est inclus pour un aspect, mais pas partout, comme vous l'avez souligné. C'est l'une des lacunes constitutionnelles vraiment importantes que j'ai relevées à l'article 15.4 proposé, qui porte sur le pouvoir de collecte de renseignements.

La cinquième recommandation de mon mémoire porte précisément sur l'enjeu que le commissaire à la protection de la vie privée du Canada a soulevé dans son témoignage. J'établirais un lien non seulement avec le cadre de protection de la vie privée dont le commissaire est responsable, mais aussi avec les principes constitutionnels que j'ai analysés et qui s'appliquent dans ce contexte.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Dans votre présentation, vous nous avez fait part de vos préoccupations à l'égard de l'article 15.2 proposé dans le projet de loi. Cet article pourrait être utilisé pour créer des portes dérobées et, au bout du compte, affaiblir les normes de chiffrement. Je ne suis pas une informaticienne, mais j'ai compris qu'il est difficile actuellement de pénétrer les systèmes, puisque la norme de chiffrement est très élevée. Abaisser cette norme pourrait mettre en péril la sécurité.

Est-ce que j'ai bien compris votre argument?

[*Traduction*]

Kate Robertson: Oui, vous l'avez très bien compris. La seule précision que je voudrais apporter, c'est que la technologie traditionnelle des télécommunications était non sécurisée dès la conception. Avec les réseaux pérennes de communication mobile, nous voyons encore des faiblesses qui exposent les gens à la cyberfraude et à d'autres types de surveillance malveillante, comme l'espionnage industriel et des fonctionnaires.

Il y a des dispositifs de sécurité, y compris le chiffrement, dans la technologie 5G et 6G, mais nous savons qu'en Europe, par exemple, les forces de l'ordre ont exercé des pressions pour désactiver ces technologies qui améliorent la protection de la vie privée afin de faciliter la surveillance policière. Or, c'est exactement l'inverse de ce que nous voulons et de ce dont nous avons désespérément besoin pour nous assurer que nos systèmes sont sécurisés dès la conception plutôt que le contraire.

Nous devons combler le plus de lacunes possible plutôt que de créer de nouvelles brèches. Je suppose que c'est pourquoi les représentants du gouvernement ont convenu que ce projet de loi ne porterait ni sur la surveillance ni sur le décodage des chiffrements. Or, nous ne pouvons le savoir que si nous l'avons inscrit dans la loi elle-même, ce qui est une lacune que nous recommandons de combler de toute urgence.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Madame Robertson, aviez-vous eu l'occasion de témoigner dans le cadre du projet de loi C-26? Ces préoccupations avaient-elles été discutées et débattues?

Avez-vous eu l'occasion de sensibiliser le gouvernement sur cette faiblesse dans le projet de loi C-8, qui était aussi dans le projet de loi C-26, et de lui signaler qu'elle pourrait causer des préjudices, voire favoriser des cyberattaques?

● (1140)

[*Traduction*]

Kate Robertson: Le problème, c'est qu'il y a de multiples façons d'interpréter la manière de prendre ces arrêtés. Nous aimerions que le processus soit le plus transparent et responsable possible, car certains pourraient juger que le décryptage est un moyen d'assurer la sécurité du Canada, mais nous savons que c'est faux.

La combinaison actuelle de l'ambiguïté en matière d'interprétation et de la possibilité que ces arrêtés soient pris en secret rend particulièrement inquiétante la possibilité que ces nouveaux dispositifs de sécurité soient compromis par...

[*Français*]

La vice-présidente (Claude DeBellefeuille): Je m'excuse de vous interrompre, madame Roberston, mais il semble qu'il n'y a plus d'interprétation.

La situation est infiniment désolante pour vous autant que pour moi.

[*Traduction*]

Le greffier: Je veux simplement vérifier encore une fois que l'interprète francophone est de retour sur le canal français.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Ça fonctionne, maintenant.

Veuillez excuser cette petite contrainte qui s'impose à nous, madame Robertson. C'est parce que les interprètes font leur travail à distance. C'est donc un obstacle de plus pour l'interprétation de vos propos.

Vous pouvez maintenant poursuivre.

[*Traduction*]

Kate Robertson: Oui, je disais qu'avec le secret qui s'ajoute au manque de clarté, ces arrêtés pourraient être utilisés pour décoder le chiffrement, et c'est un problème.

J'ajouterais qu'il n'est pas difficile d'imaginer que ces arrêtés puissent être adoptés à des fins de surveillance. Le ministère de la Sécurité publique a présenté un projet de loi dans le but précis d'installer de nouvelles capacités dans les systèmes de télécommunications. Bien sûr, ce devrait être une législation distincte si c'est fait, et être associé à des mesures de protection très différentes. Ce projet de loi porte sur la cybersécurité, et non sur la surveillance, d'après ce qu'on nous dit, et c'est pourquoi nous devons veiller à ce que le projet de loi C-8 ne permette pas ce genre de compromis.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Merci beaucoup, madame Robertson.

Chers collègues, comme nous avons commencé la rencontre en retard, nous avons une décision à prendre. La première option serait de commencer le prochain tour comme prévu en accordant la parole à M. Au, à M. Ehsassi et à moi-même, mais MM. Caputo et Powlowski n'auraient pas leur tour de parole. L'autre option serait d'accepter que la rencontre se termine plus tard, pour permettre aux membres du Comité de prendre la parole selon l'ordre normal.

Voulez-vous ajouter entre 15 et 20 minutes à la rencontre ou voulez-vous réduire le temps dont vous disposerez pour poser vos questions?

Une voix: Nous pouvons terminer plus tard.

La vice-présidente (Claude DeBellefeuille): Vous êtes donc d'accord pour que la réunion se termine vers 13 h 20. Elle se terminerait à 13 h 17, plus précisément.

Nous passons donc au deuxième tour.

Monsieur Au, vous avez la parole pour cinq minutes.

[*Traduction*]

Chak Au (Richmond-Centre—Marpole, PCC): Merci beaucoup.

Mes questions s'adressent à M. de Boer.

Je suis tout à fait d'accord avec vous lorsque vous dites que la confiance est importante pour assurer la sécurité et la fiabilité. Vous avez également mentionné que nous sommes le seul pays du G7 à être en retard, alors ma première question est la suivante: par rapport aux autres pays du G7, à quel point sommes-nous en retard, et quelle est l'importance de ce retard?

John de Boer: Les États-Unis ont adopté une loi semblable en 2022, c'est-à-dire il y a près de quatre ans. En Europe, la directive SRI 2 a été promulguée en octobre dernier, tandis que le Japon a promulgué une directive en avril et l'Australie, l'an dernier. Ainsi, nous avons au moins un à quatre ans de retard par rapport à nos pairs, essentiellement, et cela nous rend vulnérables.

Chak Au: Dans ce cas, pensez-vous que le retard est intentionnel, ou est-ce de la négligence?

John de Boer: Je ne dirais pas qu'il est intentionnel. Je sais que le gouvernement essaie de travailler sur ce projet de loi et de l'adopter depuis un certain temps. Il faut du temps pour bien le rédiger.

De plus, notre système fédéral complique les choses, mais je souligne à grands traits que la situation est déjà urgente. Il faut adopter le projet de loi. La cybersécurité est probablement l'une des menaces les plus répandues nous guettant aujourd'hui.

● (1145)

Chak Au: Très bien.

Pour poursuivre dans la même veine, je déteste parfois entendre les formulations « C'est un pas dans la bonne direction » ou « C'est un bon premier pas. »

Combien de pas devons-nous faire pour arriver à la destination voulue? Que recommandez-vous? Comment pouvons-nous nous approcher plus rapidement de la destination?

John de Boer: Je considère que le projet de loi est un premier pas parce que, tout d'abord, il porte sur quatre secteurs d'infrastructures essentielles. Or, nous en avons beaucoup plus. Même la notion de ce qu'est une infrastructure essentielle est en train de changer. Il a fallu des années à Sécurité publique Canada pour élaborer une nouvelle stratégie sur les infrastructures essentielles.

Cette évaluation changera constamment. Il est vraiment important que nous continuions d'élargir l'applicabilité de ces exigences au-delà de ces quatre secteurs. Il faut aussi une approche harmonisée avec les provinces et les territoires.

Malheureusement, les auteurs de menaces trouvent de nouvelles façons d'attaquer nos infrastructures essentielles. Nous devons nous adapter et être prêts à nous adapter.

Chak Au: Autrement dit, comment peut-on être plus proactif au lieu de toujours essayer de rattraper le retard? Que recommandez-vous?

John de Boer: L'une des principales recommandations que je peux faire est de renforcer les partenariats public-privé. Travaillez plus étroitement avec des entreprises comme BlackBerry et d'autres qui en savent beaucoup plus, dans certains cas, sur les auteurs de menaces qui s'en prennent aux infrastructures essentielles. Nous les voyons jour après jour, alors qu'il y a des limites à ce que le gouvernement canadien peut faire.

L'une des initiatives que le gouvernement canadien promeut est le Collectif canadien pour la cyberdéfense, une initiative judicieuse qui réunira des entités des secteurs public et privé pour faire face à des crises immédiates et à moyen terme.

C'est un bon premier pas.

Chak Au: C'est un autre bon premier pas.

Dans votre rapport, vous faites état d'un grand nombre de cyberattaques — cinq millions en trois mois —, alors le problème est grave.

Pensez-vous que le projet de loi C-8, dans sa forme actuelle, vous aiderait, vous et votre entreprise, à faire face à ces cyberattaques?

John de Boer: L'échange de renseignements est vraiment important. Le fait de comprendre comment la menace évolue, quelles sont les tendances et quels types de tactiques et de procédures les auteurs de la menace utilisent vous aide à établir des moyens de défense à l'avenir.

Le projet de loi C-8 rend notamment obligatoire la communication de renseignements à titre confidentiel. Quand on sait ce que trament l'ennemi ou les acteurs voyous, on peut mieux se préparer, alors oui, la réponse courte à votre question est que le projet de loi aidera BlackBerry et nos clients. Il nous aidera à faire évoluer notre technologie vers des normes de chiffrement plus élevées, notamment.

C'est très important.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Merci beaucoup, monsieur de Boer.

Je passe maintenant la parole à M. Ehsassi pour cinq minutes.

[*Traduction*]

L'hon. Ali Ehsassi (Willowdale, Lib.): Merci, madame la présidente.

Je remercie nos témoins. Les témoignages m'éclairent beaucoup.

Je vais commencer par M. de Boer.

Vous avez souligné à plusieurs reprises aujourd'hui la nécessité d'établir des partenariats public-privé, et vous avez également mentionné que nous sommes en retard par rapport à nos partenaires du Groupe des cinq.

Est-ce que certains partenaires du Groupe des cinq se servent de partenariats public-privé?

John de Boer: Oui. Il y a environ trois ans, les États-Unis ont mis en place le collectif conjoint de cyberdéfense, qui réunit les secteurs privé et public. Au Royaume-Uni, ainsi qu'en Australie, ce modèle existe depuis plus de cinq ans. La bonne nouvelle, c'est que le Canada s'est également joint à ce qu'on appelle l'Initiative internationale de lutte contre les rançongiciels, que BlackBerry copréside dans le cadre d'un partenariat public-privé.

Les gouvernements ont donc sérieusement commencé à travailler en étroite collaboration avec le secteur privé. Ce modèle existe dans d'autres pays.

L'hon. Ali Ehsassi: S'agit-il d'un processus consultatif?

John de Boer: Il ne s'agit pas seulement de consultations. Dans certains cas, les intervenants agissent ensemble pour vaincre des acteurs malveillants, ainsi que pour faire face aux cybermenaces actives et y réagir.

L'hon. Ali Ehsassi: D'accord. Je vous remercie de ces renseignements.

Votre troisième recommandation est de donner accès à des outils de sécurité. Pouvez-vous nous en dire plus à ce sujet?

● (1150)

John de Boer: Comme il en a été question dans le rapport de la vérificatrice générale d'octobre, même si vous avez le mandat clair de communiquer l'information, vous serez restreints si vous n'avez pas de moyen de la communiquer efficacement à ceux qui en ont besoin. En ce moment, selon ce rapport, le gouvernement du Canada ne dispose pas d'un outil sanctionné pour échanger des renseignements efficacement. Chez BlackBerry, c'est notre domaine d'expertise. Ce qui nous importe est de veiller à ce que quiconque partage des renseignements le fasse de façon sécurisée, et non au moyen d'applications commerciales ou d'applications qui n'ont pas été conçues pour échanger des renseignements sécurisés.

Notre recommandation serait de trouver un moyen — un outil — et d'en tirer parti de manière coordonnée pour l'ensemble des infrastructures essentielles et du gouvernement. Il faut des outils certifiés à cette fin et qui sont approuvés précisément pour l'échange de renseignements.

L'hon. Ali Ehsassi: Merci beaucoup.

Je vais maintenant m'adresser à Mme Robertson.

Merci beaucoup, madame Robertson. Je crois comprendre que, dans l'ensemble, sans entrer dans les détails, vous êtes très favorable au projet de loi C-8. Est-ce exact?

Kate Robertson: Nous sommes favorables à une approche plus proactive de la part du gouvernement. Comme nous le soulignons dans notre recherche, les pratiques passées, le manque de reddition de comptes et le secret excessif ont mené à...

L'hon. Ali Ehsassi: De façon générale — pas dans les détails, mais de façon générale —, vous comprenez que nous accusons du retard par rapport à nos partenaires du Groupe des cinq et qu'il est important que nous le rattrapions. Est-ce exact?

Kate Robertson: Ce que je dis, c'est que le gouvernement doit jouer un rôle plus proactif. Cependant, il a malheureusement été complice de certaines technologies de surveillance qui sont responsables d'avoir rendu ces technologies peu sûres au départ. Il faut vraiment que...

L'hon. Ali Ehsassi: Cela ne répond pas vraiment à ma question. Merci.

Kate Robertson: Eh bien, cela répond à la question de mon point de vue. C'est mon avis.

L'hon. Ali Ehsassi: Non. Je comprends que vous n'approuvez pas certaines dispositions. C'est entendu. Mais que vous ne répondiez pas à la question de savoir si le projet de loi C-8, en règle générale, va dans la bonne direction... C'est essentiellement ce que je demandais.

Kate Robertson: On m'a déjà posé cette question. Je pense qu'il faut une stratégie à long terme; l'intervention ne sera pas rapide. Il existe d'autres outils à cette fin. Je préférerais — et c'est mon point de vue — que des amendements soient proposés plutôt que de simplement adopter le projet de loi tel quel parce que nous évoluons dans un climat de peur.

L'hon. Ali Ehsassi: Merci. L'intervention ne sera pas rapide, comme nous l'ont dit de nombreux témoins. Nous sommes loin derrière nos partenaires du Groupe des cinq. Personne ne prétend que l'intervention sera rapide. Mais vous convenez, madame Robertson, qu'il y aura un contrôle judiciaire pour toute décision prise par le ministre, n'est-ce pas?

Kate Robertson: Non. Je ne souscris pas à cette affirmation. Il y aura contrôle judiciaire seulement si une partie en demande un. Bien sûr, s'il y a un secret...

L'hon. Ali Ehsassi: Mais le droit est inscrit dans le projet de loi. Il est indéniable. Vous en convenez, si je comprends bien.

Kate Robertson: Il est impossible d'exercer ce droit si nous ne savons pas que le décret du gouvernement a été pris ou sans savoir quels en seraient les effets. Donc, si...

L'hon. Ali Ehsassi: Merci. Vous dites que les personnes visées pourraient ne pas être au courant de leur...

[*Français*]

La vice-présidente (Claude DeBellefeuille): Merci beaucoup, monsieur Ehsassi. C'est très intéressant et passionnant. Cette discussion pourra se poursuivre plus tard.

C'est maintenant mon tour de parole de deux minutes et demie.

Monsieur Hatfield, selon vous, le projet de loi prévoit-il un mécanisme de contrôle des ordres donnés par le Cabinet en matière de cybersécurité? Pensez-vous que c'est suffisant? Aurait-on besoin d'amender le projet de loi pour mieux encadrer le pouvoir du ministre?

[*Traduction*]

Matthew Hatfield: Oui, tout à fait.

Je vais répondre à la question qui vient d'être posée: le projet de loi C-8devrait-il être adopté dans sa forme actuelle? Non. Devrait-il être adopté sous une forme ou une autre? Oui, potentiellement, si les amendements pertinents sont apportés.

Nos mesures de protection et nos lois en matière de cybersécurité sont effectivement inférieures à celles de nos alliés. Dans ces circonstances, pourquoi envisageons-nous d'adopter un projet de loi prévoyant une surveillance bien moindre que celle de nos alliés? Je pense que c'est l'étape cruciale à franchir. Le ministre ne peut pas prendre ces décisions seul. Notre droit à un contrôle judiciaire, qui ne s'applique que lorsque nous apprenons l'incidence d'un décret secret que nous n'avons jamais vu, n'est pas du tout un véritable droit.

Divers organismes pourraient être habilités, comme il se doit, à assurer une surveillance. Le Comité des parlementaires sur la sécurité nationale et le renseignement, ou CPSNR, pourrait obtenir beaucoup plus de renseignements sur le contenu de ces décrets afin qu'il puisse en juger. Par ailleurs, la population doit aussi avoir une idée plus claire de ce qui se passe invariablement dans le système. Sinon, les décrets secrets pourraient se multiplier, ce qui créerait un système en expansion qui pourrait porter sur la surveillance beaucoup plus que sur la cybersécurité.

● (1155)

[*Français*]

La vice-présidente (Claude DeBellefeuille): Avez-vous l'intention de nous suggérer des amendements afin de mieux encadrer le pouvoir du ministre? Vous ne les avez peut-être pas à la portée de la main, mais est-ce quelque chose que vous pourriez faire parvenir au Comité, monsieur Hatfield et madame Robertson, pour mieux nous éclairer?

[*Traduction*]

Matthew Hatfield: Oui, certainement.

Je peux en mentionner quelques-uns brièvement dès maintenant: interdire le secret permanent; soumettre les décrets et les renseignements secrets à des contrôles automatiques, par une partie externe, à un stade du processus; davantage communiquer à la population ce qui se passe; et implanter des protections supplémentaires concernant le chiffrement et la prévention des faiblesses inhérentes au système.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Merci beaucoup.

Nous allons maintenant passer à M. Caputo pour cinq minutes.

Frank Caputo (Kamloops—Thompson—Nicola, PCC): Merci, madame la présidente.

Bienvenue dans ce fauteuil.

[*Traduction*]

Je remercie tous les témoins — les deux qui comparaissent virtuellement et celui qui est présent dans la salle — de leur présence.

J'aimerais commencer par Mme Robertson.

Tout d'abord, votre mémoire est incroyablement complet. Je vous remercie d'avoir fourni un document aussi volumineux et précis.

Je ne suis pas sans savoir qu'on m'a souvent reproché au Comité d'interrompre des témoins, comme le ministre, et pourtant, vous avez été interrompus à maintes reprises quand vos réponses ne correspondaient peut-être pas à ce que certains membres du Comité auraient souhaité.

Je vais vous laisser le temps de terminer vos réponses aux questions qui ont été posées. Si vous avez quelque chose à ajouter, n'hésitez pas à le faire maintenant.

Kate Robertson: Merci beaucoup.

Permettez-moi de citer les observations du commissaire au renseignement du Canada: « Le grand absent [de ce projet de loi], c'est le public canadien, » dont les renseignements, qui font l'objet d'une attente raisonnable en matière de protection de la vie privée, pourraient être compromis à plus d'un égard dans le projet de loi.

Nous aimerions vraiment que le gouvernement adopte une approche plus proactive pour veiller à ce que des normes de sécurité à l'échelle du réseau nous protègent — vous, moi et tous ceux qui regardent cette réunion —, ainsi que nos communications.

Nous avons soulevé les lacunes constitutionnelles liées aux risques d'atteinte à la vie privée et aux risques en matière de cybersécurité. Pour sa part, le gouvernement est d'avis qu'il s'agit d'un contexte réglementaire où le droit à la protection de la vie privée est réduit. Cependant, nous savons que ce droit des utilisateurs de télécommunications n'est aucunement limité. La communication humaine n'est pas une question de réglementation. C'est pourquoi nous soulignons que l'équilibre qui est essentiel pour protéger la vie privée et la sécurité, dans ce cas-ci, ne répond pas aux attentes.

Vous avez reçu de ma part neuf recommandations au total. Nous croyons qu'elles sont tout à fait conformes à l'objectif du gouvernement dans le projet de loi, qui crée en fait un risque corrélatif: si des améliorations qui pourraient être apportées ne le sont pas, les tribunaux seront d'autant plus incapables de comprendre pourquoi une violation constitutionnelle est raisonnablement justifiée. Lorsque les lois inconstitutionnelles ne sont pas modifiées comme il se doit pour régler ces problèmes, les complications sont repoussées à plus tard et créent des enchevêtrements devant les tribunaux.

Frank Caputo: Merci. J'avais prévu de vous poser une question au sujet de la Charte, mais vous avez déjà clairement expliqué la situation.

Pour l'instant, j'aimerais proposer... N'importe lequel des témoins peut intervenir à ce sujet. Je ne crois pas que le projet de loi renferme une disposition de temporisation. Je pense que ce projet de loi est assez controversé. J'en entends parler en tant que porte-parole et nous en entendons parler au Comité. Le consensus — et ce n'est pas tout le monde qui le dit — est qu'il est nécessaire de légiférer sur ce sujet. Je vous paraphrase, madame Robertson: nous ne devrions pas adopter ce projet de loi à l'aveuglette et sans examen.

Comme je le disais dans ma carrière juridique, il n'importe pas seulement d'accomplir le travail: il faut faire les choses comme il faut, surtout dans un dossier comme celui-ci.

L'un des mécanismes à envisager est une disposition de temporisation. J'aimerais beaucoup que chacun d'entre vous, ou quiconque le souhaite, me donne son avis. Je suppose qu'une disposition de temporisation peut prendre plusieurs formes. L'une d'entre elles est un examen en comité après cinq ans, ce qui, d'après mon expérience, ne se produit généralement pas. On ne fait que remettre l'exercice à plus tard. Une autre forme serait un examen législatif. Je ne sais pas si cet exercice pourrait avoir lieu ni comment il aurait lieu, mais j'imagine que nous pourrions envisager cette voie. Une autre option est que le projet de loi devienne caduc au terme de trois ans. Autrement dit, il faudrait un nouveau texte de loi pour le relancer.

L'un d'entre vous a-t-il une opinion à ce sujet?

Monsieur Hatfield, vous avez la parole.

● (1200)

[*Français*]

La vice-présidente (Claude DeBellefeuille): Attendez, monsieur Hatfield, je crois qu'il y a un problème technique. Je pense que le son de la salle ne fonctionne pas bien. Nous allons vérifier ça.

[*Traduction*]

Le greffier: Monsieur Hatfield, pouvez-vous parler quelques secondes? Je veux voir s'il y a un problème de son dans la salle.

Frank Caputo: Monsieur Hatfield, pourriez-vous répéter votre réponse? Ensuite, madame Robertson et monsieur de Boer, vous pourrez nous faire part de vos réflexions.

Matthew Hatfield: [*Difficultés techniques*] avec la disposition de temporisation en ce moment, c'est que les députés n'ont pas les renseignements dont ils auront besoin pour juger de l'exercice dans trois ou cinq ans. Le gouvernement détient trop de renseignements secrets ou se contente de demander au ministre de dire ce qu'il estime raisonnable. Il faut être beaucoup plus informé pour pouvoir prendre une décision éclairée.

Frank Caputo: Professeure Robertson, avez-vous quelque chose à dire à ce sujet?

Kate Robertson: Je suis avocate et chercheuse à l'Université de Toronto, mais je ne porte pas le titre de professeure. Je voulais simplement le préciser.

Je dirais que nous avons eu l'occasion unique d'entendre une ancienne juge de la Cour fédérale qui a été très explicite, si je peux m'exprimer ainsi: elle a dit qu'il y a là une faiblesse constitutionnelle qui n'est aucunement justifiée, selon elle.

Bien sûr, j'appuie cette analyse, mais lorsque les enjeux sont exprimés aussi clairement...

[*Français*]

La vice-présidente (Claude DeBellefeuille): Je m'excuse grandement, mais je dois vous interrompre ici.

Ce tour de questions aux témoins est terminé.

Non, c'est vrai, il reste votre tour, monsieur Powlowski. J'étais en train de vous oublier. Je m'excuse mille fois. Est-ce que vous pardonnez cet oubli à votre jeune présidente de bientôt 62 ans?

[*Traduction*]

Marcus Powlowski (Thunder Bay—Rainy River, Lib.): Ne vous en faites pas.

[*Français*]

La vice-présidente (Claude DeBellefeuille): La parole est donc à vous pour cinq minutes, monsieur Powlowski.

[*Traduction*]

Marcus Powlowski: La qualité de mes questions va peut-être vous décevoir. Je ne suis pas un expert dans ce domaine. Le projet de loi C-8 est nouveau pour moi, et je suis nouvellement membre du Comité. J'ai une question d'ordre général; je cèderai peut-être ensuite la parole à M. Ehsassi.

J'ai l'impression que le projet de loi a pour but de nous permettre de détecter rapidement les incidents de cybersécurité et d'y répondre lorsque des acteurs malveillants comme les Russes ou les Chinois tentent d'interférer avec certains secteurs vitaux de notre société, ce qui semble être le cas. C'est la réalité des guerres modernes internationales.

Madame Robertson, monsieur Hatfield, je suppose que vos préoccupations ont trait au caractère adéquat de la protection des divers membres de la société, mais n'y a-t-il pas un compromis possible en ce qui a trait à... Comme l'a fait valoir M. de Boer, il faut réagir rapidement en cas de cyberincident. Si nous embourbons le processus avec... Ce n'est peut-être pas le bon mot. Si les exigences et les protections pour la société civile sont trop lourdes, cela ne compromet-il pas notre capacité à réagir rapidement aux cybermenaces? N'est-ce pas exactement ce que souhaite M. Poutine... Que nous ayons tellement de couches de protection qu'il nous faille des jours pour avoir la capacité légale d'agir?

Je vois une main levée. Madame Robertson, je crois que vous avez hâte de répondre à cette question aussi. Nous pourrions vous entendre en premier, puis nous entendrons M. Hatfield.

● (1205)

Kate Robertson: Nous ne nous entendons pas sur l'interprétation. Je comprends que les représentants du gouvernement sont d'avis qu'il ne faut pas contourner le chiffrement, mais nous recommandons une modification afin de le confirmer de manière explicite. À certains égards, c'est une question d'interprétation et non de procédure ou d'application régulière de la loi.

Si l'on prend mon exemple au sujet de l'autorisation par la Cour fédérale de la collecte de renseignements personnels et de la dépersonnalisation, ces procédures sont toujours associées à une clause relative aux circonstances exceptionnelles, lorsqu'il y a une situation urgente qu'il faut aborder. C'est pourquoi je dis que mes recommandations...

Marcus Powlowski: Excusez-moi. Pourriez-vous nous expliquer ce qu'est la clause relative aux circonstances exceptionnelles? De quoi s'agit-il exactement?

Kate Robertson: Cela signifie que si le gouvernement doit habituellement avoir l'autorisation d'un juge pour obtenir l'information, il s'agit d'une expectative raisonnable de vie privée, puisque la presque totalité des renseignements que possèdent les fournisseurs de services de télécommunications sont des renseignements personnels. L'autorisation n'est pas nécessaire en cas d'urgence. « Circonstances exceptionnelles » est un terme juridique qui signifie qu'il y a urgence et que nous avons besoin de l'information immédiatement. Il ne faut pas que ce soit la règle par défaut, toutefois. C'est pourquoi nous faisons valoir qu'une autorisation doit être requise. Cela ne minerait en rien la capacité du gouvernement d'intervenir rapidement au besoin.

Marcus Powlowski: Allez-y, monsieur Hatfield.

Matthew Hatfield: Nous voulons qu'il y ait un examen après coup, lorsque les décrets d'urgence sont nécessaires. Il est possible qu'une situation se présente et que le ministre doive réagir et obtenir de l'information immédiatement. C'est normal. Dans un tel cas, il faut qu'un examen se fasse dans les 30 ou 60 jours suivants, afin qu'un juge et un expert technique puissent confirmer que le décret était raisonnable et qu'il devrait peut-être être prolongé au-delà de la situation d'urgence. Dans le domaine de la protection de la vie privée et de la sécurité, on utilise souvent l'expression suivante: « faites confiance, mais vérifiez ». Nous voulons que la confiance envers le ministre puisse être prolongée, mais il faut ensuite s'assurer qu'un suivi est fait en ce qui a trait à l'objet du projet de loi.

Marcus Powlowski: Allez-y, monsieur Ehsassi.

L'hon. Ali Ehsassi: Merci.

J'aimerais poser une question à Mme Robertson. Vous avez parlé d'une ambiguïté en matière d'interprétation. Il me semble qu'une telle ambiguïté est toujours présente jusqu'à ce que les règlements soient adoptés de manière plus précise. Êtes-vous d'accord?

Kate Robertson: Je ne suis pas d'accord. Le défaut d'une mesure législative de baliser adéquatement les capacités de surveillance ou de collecte de renseignements d'une large portée représente en soi une cause pour que les tribunaux l'annulent, et c'est exactement le problème que nous avons à l'heure actuelle. Le gouvernement a fait valoir qu'il n'avait pas l'intention d'utiliser la loi d'une certaine façon. Toutefois, ce genre de garantie ne représente pas un fondement approprié pour délimiter une loi. Je cite le rapport spécial de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, ou OSSNR, qui souligne à titre d'exemple de remaniement d'une loi sur la sécurité nationale que l'un des organismes responsables de la sécurité nationale avait fait valoir devant un comité d'étude que...

[*Français*]

La vice-présidente (Claude DeBellefeuille): Merci beaucoup, madame Robertson. Je suis désolée de vous interrompre, mais le temps de parole de M. Ehsassi est maintenant écoulé.

Si je ne me trompe pas, cette fois-ci, c'est le bon moment de vous remercier de vos témoignages. Ils vont aider l'ensemble des membres du Comité à étudier le projet de loi plus en profondeur.

Monsieur de Boer, je vous remercie de vous être déplacé pour être des nôtres en personne.

Nous allons suspendre la rencontre pour accueillir le prochain groupe de témoins.

● (1205)

(Pause)

● (1210)

La vice-présidente (Claude DeBellefeuille): Nous reprenons la rencontre.

Nous souhaitons la bienvenue aux témoins. Je les remercie beaucoup de s'être déplacés pour participer à la rencontre en personne.

Nous accueillons tout d'abord M. Todd Warnell, qui est responsable de la sécurité de l'information à Bruce Power.

Nous recevons également M. Francis Bradley, qui est président-directeur général d'Électricité Canada.

Vous êtes les bienvenus.

Vous aurez chacun cinq minutes pour votre allocution d'ouverture.

Nous allons débuter par M. Todd Warnell.

[*Traduction*]

Todd Warnell (responsable de la sécurité de l'information, Bruce Power): Madame la présidente, mesdames et messieurs les membres du Comité, merci. Je m'appelle Todd Warnell. Je suis responsable de la sécurité de l'information pour Bruce Power, la seule centrale nucléaire du secteur privé au Canada. Depuis 2001, Bruce Power a fourni environ le tiers de l'électricité de l'Ontario et produit des isotopes médicaux qui sauvent des vies et qui sont utilisés partout dans le monde pour lutter contre le cancer.

Je vous remercie de me donner l'occasion de participer à votre examen du projet de loi C-8. Aujourd'hui, je vais me concentrer sur les raisons pour lesquelles il est impératif d'aller de l'avant avec ce projet de loi, en particulier la partie 2, la Loi sur la protection des cybersystèmes essentiels.

Les infrastructures essentielles du Canada font face à des cybermenaces sans précédent qui mettent en danger leur fiabilité de même que la sécurité et la vie quotidienne des Canadiens. Le projet de loi C-8 est une première étape cruciale pour renforcer notre résilience collective et assurer la sécurité des services essentiels. Ce projet de loi est plus qu'une politique; c'est un engagement à protéger l'épine dorsale de notre économie et de notre sécurité nationale dans un contexte de menace mondiale qui évolue rapidement.

Le secteur du nucléaire canadien a su démontrer qu'en collaborant avec le gouvernement, les organismes de réglementation, l'industrie, le milieu universitaire et les Canadiens, nous pouvons mettre sur pied et réglementer avec succès les cybersystèmes nécessaires à la prestation sûre et fiable des services essentiels.

Le projet de loi C-8 vise à sécuriser les systèmes essentiels, à encourager la gestion proactive des risques et à permettre une intervention gouvernementale responsable en cas de cybermenace importante.

La Loi sur la protection des cybersystèmes essentiels introduira un cadre général à partir duquel tous les secteurs essentiels, en collaboration avec le gouvernement et les organismes de réglementation, pourront élaborer et mettre en œuvre des règlements fondés sur les risques et le rendement afin d'améliorer la fiabilité et la résilience des services essentiels.

Des renseignements récemment publiés sur les services de renseignement canadiens et alliés indiquent très clairement que les États-nations et les organisations cybercriminelles se positionnent activement dans les infrastructures essentielles du Canada et d'ailleurs. Ces auteurs de menaces se préparent à des actions perturbatrices et potentiellement destructrices visant les services essentiels sur lesquels les Canadiens comptent au quotidien. Le Centre canadien pour la cybersécurité de même que des organismes alliés comme le centre national de cybersécurité du Royaume-Uni ont émis des avertissements publics clairs au sujet de la sophistication et de la persistance croissantes de ces menaces. L'urgence d'agir est mise en évidence par des incidents dans le monde réel et des campagnes en cours qui démontrent à la fois la capacité et l'intention des adversaires de perturber ou d'endommager les infrastructures essentielles.

Je vais passer en revue quelques points clés sur les avantages d'aller de l'avant avec le projet de loi C-8.

Premièrement, il faut renforcer la sécurité et la sûreté nationales. Le projet de loi C-8 est crucial pour protéger la sécurité nationale, puisqu'il exige des organisations privées et publiques au sein des infrastructures essentielles qu'elles adoptent des pratiques robustes en matière de cybersécurité. À mesure que les cybermenaces évoluent et deviennent de plus en plus sophistiquées, la sécurité des infrastructures et des services essentiels est primordiale pour la sécurité nationale et la sécurité publique.

Deuxièmement, il faut améliorer la gestion des risques. En appliquant des pratiques obligatoires de gestion des risques, le projet de loi aiderait les organisations à passer d'une posture réactive à une approche proactive qui atténue les risques avant qu'ils ne se transforment en incidents réels.

Troisièmement, il faut assurer l'autorité gouvernementale dans les scénarios à risque élevé. Le projet de loi C-8 donnerait au gouvernement le pouvoir d'agir rapidement lorsque des menaces graves planent sur les infrastructures essentielles, tout en protégeant les services essentiels et la confiance du public. Pour renforcer davantage l'efficacité de cette approche, il serait avantageux que le projet de loi C-8 établisse plus clairement la distinction entre le rôle du Centre canadien pour la cybersécurité en tant qu'autorité technique et les responsabilités des organismes de réglementation du secteur. La séparation claire de ces rôles contribuera à assurer des réponses coordonnées, efficaces et dirigées par des experts aux cybermenaces dans l'ensemble des secteurs des infrastructures essentielles du Canada.

Quatrièmement, il faut harmoniser nos pratiques à celles de nos alliés mondiaux. Ceux-ci appliquent ou ont déjà mis en œuvre des lois semblables en matière de cybersécurité. Le projet de loi C-8 permettrait au Canada de s'aligner sur ses partenaires internationaux et de faire en sorte qu'il soit plus facile pour les entreprises canadiennes de mener des activités à l'échelle mondiale dans des cadres sécurisés.

Enfin, il faut assurer la sécurité économique. Les cyberattaques contre des secteurs essentiels entraînent des répercussions économiques de grande portée. En veillant à ce que les industries et les services clés soient protégés, le Canada protégerait également sa stabilité économique, ce qui aiderait à prévenir les conséquences en cascade qui pourraient découler de la perturbation des services et des infrastructures.

En conclusion, le projet de loi C-8 repose sur de bonnes intentions et est une mesure plus que nécessaire en vue de répondre à la question urgente de la cybersécurité au Canada et dans les secteurs des infrastructures essentielles canadiens. Le contexte de la menace a grandement évolué, et les menaces ne sont plus dans la théorie. Il faut agir maintenant pour protéger les Canadiens et nos alliés.

● (1215)

Je vous remercie de me donner l'occasion de témoigner devant le Comité. Je serai heureux de répondre à vos questions.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Merci beaucoup, monsieur Warnell.

Je cède maintenant la parole à M. Bradley pour cinq minutes.

Francis Bradley (président-directeur général, Électricité Canada): Merci beaucoup.

Je suis Francis Bradley et je suis le PDG d'Électricité Canada.

Électricité Canada est la voix nationale de l'électricité au pays.

La vice-présidente (Claude DeBellefeuille): Excusez-moi, monsieur Bradley. J'ai l'impression qu'il y a un problème du côté de l'interprétation.

[*Traduction*]

Sima Acan: On entend trois autres voix en anglais sur le même canal.

[*Français*]

Le greffier: Nous allons faire un test. Est-ce que vous m'entendez seulement en anglais sur le canal anglais?

La vice-présidente (Claude DeBellefeuille): Je crois que ça fonctionne pour tout le monde, maintenant.

Vous pouvez recommencer votre introduction, monsieur Bradley.

Francis Bradley: Merci.

Électricité Canada est la voix nationale de l'électricité au pays. Nos membres produisent, transportent et distribuent de l'électricité dans chaque province et territoire.

Merci beaucoup de m'avoir invité à témoigner au sujet du projet de loi C-8. En décembre dernier, j'ai témoigné devant un comité de l'autre Chambre au sujet du projet de loi C-26.

Les nouvelles obligations en matière de cybersécurité prévues dans le projet de loi C-8 s'appliquent à certaines infrastructures essentielles de compétence fédérale. Dans notre secteur, cela vise principalement les lignes internationales et interprovinciales de transport d'électricité, ainsi que les centrales nucléaires. Comme plusieurs autres témoins, nous reconnaissons qu'il existe un écart législatif dans l'approche du Canada en matière de cybersécurité. Nous appuyons donc les objectifs généraux du projet de loi. Cependant, nous avons certaines préoccupations, et nous proposons quelques modifications pour mieux protéger les partenariats existants avec les organismes fédéraux et renforcer la sécurité de notre secteur.

● (1220)

[*Traduction*]

Premièrement, nous recommandons que le projet de loi C-8soit modifié pour introduire des protections claires et des dispositions d'exonération pour les organisations qui divulguent volontairement des cyberincidents ou des vulnérabilités au gouvernement. Ces protections devraient faire en sorte que les renseignements communiqués de bonne foi par les organisations ne soient pas utilisés pour intenter des poursuites ou imposer des sanctions réglementaires. À notre avis, l'absence de telles protections constitue une lacune majeure. Sans elles, les exploitants recevront probablement comme conseil juridique de ne communiquer que les renseignements minimums requis pour se conformer à la loi, et rien de plus.

Comme je l'ai dit au sujet du projet de loi C-26 sur la même question, cela aurait un effet paralysant sur la communication de renseignements. Ce serait une occasion ratée de favoriser une collaboration ouverte et l'échange de renseignements avec le gouvernement, deux éléments essentiels au renforcement de notre résilience collective.

Une deuxième préoccupation concerne les risques que pose le projet de loi C-8 pour les partenariats que les exploitants d'infrastructures essentielles entretiennent actuellement avec le Centre pour la cybersécurité du CST. Aujourd'hui, notre secteur bénéficie d'une relation de collaboration avec le Centre, qui se fonde sur la certitude que les renseignements qui lui sont communiqués ne sont pas divulgués aux organismes de réglementation, aux organismes d'application de la loi ou à d'autres ministères.

Le projet de loi C-8 pourrait changer cela. Il exigerait que le CST communique les rapports d'incidents aux organismes de réglementation, qu'il fournisse des conseils ou des services à ces organismes sur la conformité des exploitants aux mesures d'atténuation des risques liés à la chaîne d'approvisionnement et qu'il autorise son personnel à échanger des renseignements avec d'autres entités gouvernementales afin d'émettre des directives en matière de cybersécurité. Comme je l'ai dit plus tôt, ces nouvelles règles et responsabilités risquent d'entraîner un effet paralysant, puisque les exploitants pourraient hésiter à communiquer des renseignements au Centre pour la cybersécurité s'ils craignent qu'ils puissent plus tard être utilisés pour l'application de la réglementation.

Pour protéger ces partenariats vitaux, nous recommandons que le projet de loi C-8 définisse mieux l'échange de renseignements prévu entre le CST et le reste du gouvernement et assure une protection contre la divulgation des renseignements communiqués volontairement au Centre pour la cybersécurité. Une séparation claire entre les fonctions collaboratives du Centre pour la cybersécurité et les nouvelles obligations du CST pourrait être adoptée.

Nous pouvons nous inspirer d'un modèle semblable qui existe déjà dans notre secteur entre la North American Electric Reliability Corporation, ou NERC, et l'Electricity Information Sharing and Analysis Center, ou E-ISAC. Bien que l'E-ISAC soit géré par la NERC, il est tenu à l'écart des activités d'application de la loi sur le plan organisationnel, ce qui préserve la confidentialité et favorise l'échange ouvert de renseignements avec les exploitants du secteur de l'électricité.

Enfin, nous craignons que le projet de loi C-8 crée un cadre réglementaire redondant pour la cybersécurité dans le secteur de l'électricité, qui est déjà réglementé par les normes de la NERC et les organismes de réglementation provinciaux. Le secteur de l'électricité est unique en ce sens qu'il respecte les normes de protection des infrastructures critiques de la NERC, qui sont adoptées, appliquées et vérifiées par des organismes provinciaux. Ces normes garantissent déjà des mesures solides et exhaustives pour sécuriser le réseau. L'introduction de nouvelles exigences fédérales potentiellement conflictuelles risque de créer de l'ambiguïté, des fardeaux de conformité supplémentaires et un manque d'harmonisation de la réglementation, ce qui pourrait nuire à l'objectif du projet de loi d'améliorer la sécurité.

Pour atténuer ce risque, nous proposons d'inclure des dispositions qui permettent à l'organisme de réglementation fédéral de reconnaître et d'accepter la conformité à des cadres équivalents, comme les normes de protection des infrastructures critiques de la NERC. Nous serons aussi prêts à travailler avec le gouvernement dans le cadre du processus d'élaboration de la réglementation afin d'assurer l'harmonisation aux cadres existants.

[*Français*]

Bien que de nombreux autres aspects du projet de loi mériteraient également une attention, c'est tout le temps dont je dispose aujourd'hui...

La vice-présidente (Claude DeBellefeuille): Vous m'enlevez les mots de la bouche, monsieur Bradley. Le temps de parole qui vous était alloué est écoulé.

Nous allons commencer le premier tour de questions.

Monsieur Lloyd, vous avez la parole pour six minutes.

● (1225)

[*Traduction*]

Dane Lloyd: Nous remercions les témoins d'être avec nous.

Merci, madame la présidente.

Monsieur Bradley, est-ce que ces dispositions d'exonération que vous proposez existent dans d'autres administrations? Si oui, lesquelles?

Francis Bradley: C'est une excellente question. Je n'ai pas beaucoup de détails sur les dispositions d'exonération de façon spécifique...

Dane Lloyd: Pourriez-vous nous transmettre l'information plus tard?

Francis Bradley: Oui.

Je vous renverrais également à la représentante d'Échange canadien de menaces cybernétiques que vous avez reçue précédemment, et qui a parlé de façon détaillée des dispositions qui offrent une protection contre des poursuites.

Dane Lloyd: D'accord, merci.

Nous voulons protéger les fournisseurs afin qu'ils puissent transmettre l'information, mais qu'arriverait-il si un fournisseur avait fait preuve de négligence grave ayant entraîné un incident de cybersécurité? Est-ce que ces dispositions le protégeraient contre des poursuites criminelles s'il transmettait l'information au gouvernement?

Francis Bradley: Si vous parlez d'un cas évident... Excusez-moi, quel est le terme que vous avez utilisé?

Dane Lloyd: C'était la négligence grave.

Francis Bradley: Je ne crois pas que les dispositions d'exonération s'appliqueraient ici.

Dane Lloyd: Merci.

Nous ne voulons pas que les sociétés utilisent ces dispositions pour faire valoir qu'on ne peut faire enquête sur elles ou qu'on ne peut les accuser de quoi que ce soit lorsqu'elles vous transmettent l'information.

Francis Bradley: C'est exact.

Dane Lloyd: D'accord.

Êtes-vous d'accord avec les autres intervenants de l'industrie — nous avons reçu un mémoire de l'Electronic Transactions Association — qui font valoir que les exigences en matière de déclaration des changements à la cybersécurité sont trop larges et qu'elles pourraient entraîner un lourd fardeau pour les fournisseurs sans améliorer les résultats en matière de sécurité?

Francis Bradley: Nous ne savons pas exactement ce que sera ce fardeau en matière de déclaration, parce que nous n'avons pas encore vu la réglementation. Ce qui nous préoccupe, ce sont les doublons et les superpositions. Nous avons déjà un régime obligatoire, qui est propre au secteur de l'électricité, en raison des normes de la NERC. La déclaration est déjà obligatoire dans le secteur. On ne se préoccupe pas tant de la teneur de ce régime, parce que nous en avons déjà un.

Dane Lloyd: Selon vous, est-ce qu'il y a des changements législatifs qui pourraient réduire le fardeau associé aux doublons?

Francis Bradley: Oui. Selon la formulation actuelle de la loi, le décret « peut » désigner des normes équivalentes. Il faudrait énoncer que le décret « doit » désigner de telles normes. Il faudrait qu'il soit obligatoire et non facultatif de considérer les normes obligatoires existantes à titre d'équivalent.

Dane Lloyd: Merci.

Pouvez-vous nous parler des préoccupations relatives aux sanctions administratives pécuniaires proposées dans la loi? Croyez-vous que de telles sanctions représentent un outil constructif pour encourager la conformité?

Francis Bradley: De telles sanctions existent déjà dans notre secteur. Les normes de protection des infrastructures critiques de la NERC prévoient des pénalités. Nous n'en avons pas encore vu pour les entités canadiennes, mais en Amérique du Nord, des sanctions pécuniaires dans les six chiffres ont été désignées en ce qui a trait aux normes de protection des infrastructures critiques.

Dane Lloyd: Est-ce qu'elles encouragent la conformité ou est-ce qu'elles lui nuisent?

Francis Bradley: Je ne crois pas qu'elles aient une incidence sur la conformité.

Dane Lloyd: Craignez-vous que les dispositions sur l'échange obligatoire de renseignements de la LPCE, la loi sur la protection des cybersystèmes essentiels, puissent, par inadvertance, mener à la divulgation de données commerciales ou opérationnelles, ou même de données personnelles sensibles sur les employés? Si oui, pensez-vous que le projet de loi devrait être amendé pour mieux protéger ces renseignements?

Francis Bradley: Nous échangeons déjà des renseignements très sensibles de façon continue. À mon avis, les protections qui sont actuellement en place sont probablement suffisantes. Ce qui nous préoccupe, ce n'est pas tant la protection des renseignements, que la possibilité que ces renseignements soient utilisés à d'autres fins que l'amélioration de la sécurité. S'ils sont utilisés à des fins de sanction, s'ils sont utilisés par l'organisme de réglementation plutôt que par les responsables de la sécurité, c'est ce qui nous préoccupe.

Dane Lloyd: Merci.

Le projet de loi propose également d'imposer des sanctions importantes et une responsabilité potentielle aux dirigeants et aux administrateurs des entités désignées. D'autres intervenants nous ont dit qu'il n'y avait pas vraiment de précédent à cet égard dans d'autres pays.

Que pensez-vous de ces dispositions?

Francis Bradley: Je ne connais pas la situation dans les autres pays.

Dane Lloyd: Quelle est la situation au Canada?

Francis Bradley: D'une part, les dirigeants des sociétés sont ultimement responsables des actions de ces entités.

D'autre part, il y a aussi l'assurance responsabilité des administrateurs et des dirigeants qu'un organisme comme le nôtre et bien d'autres s'assurent d'avoir.

Dane Lloyd: Êtes-vous d'avis, comme d'autres intervenants de l'industrie, que les critères qui définissent un exploitant désigné ne sont pas clairs?

Francis Bradley: Je n'ai pas vu suffisamment de détails à ce sujet. C'est le genre de choses qui, je pense, seront clarifiées à l'étape de la réglementation. Je ne pense pas pouvoir me prononcer à ce sujet, parce que le règlement n'existe pas encore.

● (1230)

Dane Lloyd: Certaines personnes ont dit qu'à leur avis, le projet de loi ne précise pas très clairement qui sera un exploitant désigné et que cela pourrait s'appliquer à un grand nombre de petites et moyennes entreprises.

Je vous remercie du temps que vous nous avez accordé.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Il vous reste encore 50 secondes, monsieur Lloyd.

[*Traduction*]

Dane Lloyd: Oh, je pensais que vous me disiez que mon temps était écoulé.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Non, je vous ai fait signe pour vous dire qu'il vous restait une minute.

[*Traduction*]

Dane Lloyd: Monsieur Warnell, avez-vous des commentaires à faire sur l'une ou l'autre des questions que j'ai posées?

Todd Warnell: Au sujet des sanctions pécuniaires prévues dans ce projet de loi, je dirais que la responsabilité est équivalente à celle qu'ont les dirigeants pour la sécurité de leurs travailleurs.

La cybersécurité n'est pas un domaine distinct. Il s'agit de la sécurité des activités de l'exploitant, quel qu'il soit. Cette approche se trouve déjà dans d'autres lois. Son équivalence est en fait très utile pour veiller à ce que la cybersécurité soit au cœur des pratiques des exploitants.

Dane Lloyd: Pensez-vous que ce projet de loi contribuera à protéger notre réseau électrique contre la menace des éruptions solaires et des phénomènes coronaux?

Todd Warnell: Non, cela ne fait absolument rien pour renforcer les protections contre les phénomènes naturels. Il y a d'autres travaux dans d'autres domaines qui pourraient aider à ce sujet.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Je m'excuse de vous arrêter ici, monsieur Warnell. Vous aurez peut-être l'occasion de terminer votre réponse lors d'un prochain tour.

Je cède maintenant la parole à M. Ramsay pour six minutes.

Jacques Ramsay (La Prairie—Atateken, Lib.): Merci, madame la présidente.

Je remercie les témoins de leurs présentations.

Le groupe de témoins précédent nous a souligné les risques qui se poseraient pour la protection de la vie privée. Le bien-fondé de ces déclarations reste à déterminer, puisqu'un autre groupe de témoins reçu auparavant nous avait indiqué que les protections prévues dans le projet de loi étaient suffisantes. Je pense néanmoins que, comme on doit le faire pour chaque projet de loi, il est important d'examiner les avantages et les désavantages de celui-ci.

En lien avec ça, j'aimerais que vous nous disiez quels sont les dangers et quelles sont les conséquences des cybermenaces pour vos industries respectives. Quelle pourrait être la gravité de ces attaques potentielles? Qu'est-ce que ça veut dire pour le commun des mortels?

[*Traduction*]

Francis Bradley: Je peux peut-être commencer. Pour ce qui est des répercussions potentielles des cyberattaques, je crois que le secteur a été très efficace en matière de cyberprotection, mais si vous voulez comprendre quelles pourraient être les répercussions, il faudrait remonter à 2015, lorsque nous avons vu, pour la première fois, les répercussions sur les services d'électricité et les clients des cyberattaques de la Russie en Ukraine. Les lumières se sont en fait éteintes pour les clients.

Nous n'avons pas vu cela au Canada. Si vous voulez avoir une idée du pire des scénarios possible, c'est la perte de service. Bien sûr, l'électricité est, à notre avis, l'infrastructure clé dont dépendent toutes les autres infrastructures essentielles du pays. C'est l'une des raisons pour lesquelles nous avons travaillé à l'élaboration de normes de cybersécurité obligatoires et que nous y sommes assujettis depuis près de 20 ans dans le cadre de notre travail avec la NERC.

Nous avons des mesures de protection en place, car les répercussions potentielles seraient très graves si une cyberattaque privait les clients d'électricité.

Todd Warnell: Je rejoins les propos de M. Bradley: l'ampleur des actions qui pourraient être menées, qui seraient à la fois perturbatrices et destructrices, est extrêmement effrayante. La capacité des acteurs malveillants, qu'il s'agisse d'États-nations ou de cybercriminels, à infiltrer les réseaux et à provoquer des pannes imprévues ayant des répercussions sur la vie quotidienne des Canadiens, que ce soit pour la prestation de services de santé, l'approvisionnement en eau ou les services financiers, en raison d'une interruption de l'électricité, est bien réelle. Il ne s'agit plus de scénarios hypothétiques, alors que lors des discussions menées à un stade plus précoce de l'élaboration de ce projet de loi, je pense que beaucoup considéraient qu'il s'agissait d'alarmisme.

Si vous consultez les communiqués publiés par nos partenaires des services de renseignement ici au Canada et dans nos pays alliés, vous verrez que ces renseignements ont été déclassifiés. Le fait est que les auteurs de menaces sont déjà en place. Ils sont prêts à intervenir en cas de conflits cinétiques à grande échelle ou d'autres enjeux géopolitiques, et pourraient décider que ces événements justifient ce type d'action.

Nous avons dépassé le stade où des gens coiffés de chapeaux en aluminium s'inquiétaient de ce qui pourrait arriver. Nous savons maintenant que cette situation est bien réelle. Nous devons réagir à cette menace, et ce projet de loi constitue un bon premier pas dans cette direction.

● (1235)

[*Français*]

Jacques Ramsay: En ce qui concerne la double réglementation à laquelle vous avez fait allusion, monsieur Bradley, dans une autre séance, il a été bien expliqué que ça relevait surtout des directives et des règlements à prévoir, et qu'une entente était effectivement prévue pour ne pas avoir un chevauchement des services.

Maintenant, pour ce qui est des incidents qui devraient être rapportés, je comprends que ça peut représenter un grand nombre d'incidents. Je comprends qu'on va clarifier un peu ce qui doit être rapporté et ce qui ne mérite pas de l'être.

Les incidents évités de justesse, où on l'a échappé belle, ne sont pas prévus dans le projet de loi. Même si ces incidents ne sont finalement pas survenus, peuvent-ils être d'une gravité qui justifierait qu'ils soient rapportés? Si oui, est-ce qu'on devrait prévoir ça dans le projet de loi?

[*Traduction*]

Francis Bradley: Je commencerais par dire que, en ce qui concerne le risque de chevauchement, cette question serait réglée dans le cadre du processus réglementaire. C'est également ce qu'on nous a dit dans le cadre du projet de loi C-26. Je ne doute pas des responsables concernés, mais tant que nous n'aurons pas vu le règlement... Pour être honnête, notre expérience liée à l'élaboration de règlements à la suite de l'adoption de lois n'a pas toujours été positive. Cette méthode n'a pas toujours abouti au type de règlement que nous attendions. C'est pourquoi nous demeurons préoccupés à cet égard.

Pour ce qui est de ce qui devra faire l'objet d'un rapport, je vais peut-être laisser mon collègue, M. Warnell, qui est responsable de la sécurité des systèmes d'information et qui travaille donc en première ligne dans le domaine de la cybersécurité, prendre la parole.

L'idée de devoir faire rapport sur les accidents évités de justesse... Je ne vois pas très bien comment nous pourrions le faire. C'est assez clair dans le domaine de la santé et de la sécurité, par exemple. Cependant, je ne sais pas exactement ce qui constitue un « accident évité de justesse » dans le domaine de la cybersécurité. Je ne sais pas comment vous interprétez ou définissez cette notion.

Todd Warnell: Je veux bien...

[*Français*]

La vice-présidente (Claude DeBellefeuille): Je m'excuse de vous interrompre, monsieur Warnell, mais le temps de parole de M. Ramsay est écoulé. Je ne peux pas vous permettre de poursuivre votre réponse, mais vous aurez peut-être l'occasion de la terminer lors d'un prochain tour.

Merci beaucoup, monsieur Ramsay.

C'est maintenant mon tour de six minutes pour poser des questions aux témoins.

Monsieur Bradley, toute la question du chevauchement de la réglementation et des normes NERC nous préoccupe.

Pouvez-vous nous éclairer sur le rôle de la NERC dans le secteur de l'électricité au Canada et sur les risques qu'un tel chevauchement pourrait entraîner? Il est important de bien comprendre ça.

Francis Bradley: Merci beaucoup.

[*Traduction*]

Je veux bien vous parler un peu de cette relation avec la NERC, car elle est extrêmement importante.

[*Français*]

Nous estimons que le gouvernement n'a pas vraiment saisi ou n'a pas bien compris la réalité réglementaire dans notre secteur.

La NERC crée des normes de fiabilité. Les provinces adoptent ces normes et les appliquent.

[*Traduction*]

Je travaille avec la NERC depuis plusieurs décennies. Il s'agit d'une organisation nord-américaine. Il ne s'agit donc pas d'une organisation dont l'administration centrale est située aux États-Unis et qui nous dicte ce que nous devons faire. Deux Canadiens siègent au conseil d'administration de la NERC. Cinq Canadiens font partie du comité des représentants des membres de la NERC. Nous participons à l'élaboration de ces normes. Cette organisation existe depuis plusieurs décennies. Elle comprend et reconnaît les réalités auxquelles nous sommes confrontés, et elle bénéficie du soutien réglementaire des autorités canadiennes. Les normes de la NERC sont appuyées par tous les organismes de réglementation de toutes les provinces qui font partie du réseau de production-transport d'électricité.

[*Français*]

Que se passe-t-il dans des circonstances où il y a un tel chevauchement? Ça engendre des coûts plus élevés et de la confusion. Moins de ressources sont allouées à la sécurité et plus de ressources doivent s'assurer qu'on répond à différents niveaux et à différents types de réglementation.

La vice-présidente (Claude DeBellefeuille): J'ai une deuxième question.

Comme l'a souligné mon collègue Jacques Ramsay, nous avons entendu des représentants du gouvernement affirmer que leur objectif n'était pas de créer un chevauchement réglementaire, mais qu'ils travailleraient avec votre secteur pour s'assurer que ça ne se produirait pas.

Est-ce que ça vous rassure? De mon côté, je suis encore un peu inquiète. Est-ce vraiment suffisant ou faudrait-il envisager des amendements au projet de loi C-8 pour atténuer ce risque?

● (1240)

Francis Bradley: Merci beaucoup de la question. On m'avait posé la même il y a un an, quand on travaillait sur le projet de loi C-26.

Nous ne doutons pas des bonnes intentions de nos collègues du gouvernement fédéral, mais le projet de loi ne prévoit aucune obligation légale d'éviter le chevauchement. Nous voulons des garanties dans la loi, au lieu d'attendre les règlements.

Quelles pourraient être les solutions? On pourrait renforcer la disposition sur la compatibilité avec les régimes existants. Au lieu d'être une suggestion, il faudrait que ce soit une obligation. Je pense que, ça, c'est assez clair. De plus, il faudrait reconnaître l'équivalence. Par exemple, la conformité aux normes NERC en matière de protection des infrastructures essentielles devrait être considérée comme égale.

[*Traduction*]

Comme je l'ai dit plus tôt, notre expérience, lorsqu'on nous a dit « Ne vous inquiétez pas, nous allons régler ce problème dans le règlement », n'a pas toujours été positive. Lorsqu'il est clair que certaines modifications doivent être apportées au projet de loi, alors apportons-les.

Si nous voulons clairement dire « Reconnaissons l'équivalence », plutôt que « Nous pourrons envisager cette option à l'avenir », et que nous savons que c'est la voie à suivre, nous devrions opter pour une option législative plutôt que pour un règlement. Je pense que nos législateurs devraient guider ce processus, plutôt que de le laisser entre les mains des fonctionnaires qui rédigeront les règlements et les mettront en œuvre.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Il me reste une minute et demie et j'ai une dernière question à vous poser.

Est-ce que vous pourriez nous faire parvenir des propositions d'amendement qui traduiraient, par exemple, votre désir que toute cette question soit mieux encadrée? Est-ce qu'il est possible de nous les faire parvenir? Nous pourrions ainsi en prendre connaissance et comprendre plus profondément l'intention que vous voulez retrouver dans le projet de loi.

Francis Bradley: Absolument, nous travaillons activement là-dessus.

[*Traduction*]

Nous fournirons des recommandations précises à ce sujet et proposerons des modifications à apporter à certaines clauses afin de remédier à ce problème.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Il me reste encore un peu de temps.

Vous disiez que le projet de loi C-8 comportait certains risques pour votre partenariat avec le Centre canadien pour la cybersécurité. Est-ce que vous pourriez nous dire un peu, en 30 secondes, quel est le problème sur ce plan?

Francis Bradley: C'est vraiment une conséquence imprévue du projet de loi. Dans le secteur de l'électricité et dans celui d'autres infrastructures essentielles, nous profitons d'une relation très collaborative avec le Centre canadien pour la cybersécurité. Effectivement, ce que nous voulons, c'est préserver cette relation.

[*Traduction*]

En bref, nous entretenons aujourd'hui une relation très, très solide en matière d'échange de renseignements. Si les renseignements que nous échangeons risquent de se retrouver entre les mains des organismes de réglementation, il y aura forcément un refroidissement.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Merci beaucoup, monsieur Bradley.

Je passe maintenant la parole à Mme Kirkland pour cinq minutes.

Non, attendez, je me suis trompée. C'est au tour de M. Au.

[*Traduction*]

Chak Au: D'accord. Merci.

J'ai des questions à poser à M. Warnell.

Vous avez mentionné les partenariats public-privé. Je pense que c'est une très bonne idée. Pour ce qui est de la cybersécurité, il y a des aspects techniques et des composants liés à la technologie. Je pense que le gouvernement ne dispose pas toujours des renseignements les plus à jour ni des connaissances technologiques les plus récentes. Ce projet de loi donne au ministre le pouvoir de dicter à l'industrie ce qu'elle doit faire et ne pas faire. Je ne pense pas que ce soit la meilleure approche. Vous êtes mieux placés pour savoir ce que nous devons faire. Vous êtes sur le terrain.

Que pensez-vous du fait de devoir recevoir des directives du ministre sur ce qu'il faut faire et ne pas faire? Comment réagissez-vous à cette idée?

● (1245)

Todd Warnell: Nous estimons que la structure du projet de loi est adéquate, car elle favorise une « réponse rapide ». Le ministre lui-même n'agira pas de manière unilatérale et ne donnera pas d'instructions arbitraires à une industrie ou à un acteur de l'industrie. Il travaillera en collaboration étroite avec des entités privées et publiques. Il travaillera en collaboration avec le Centre canadien pour la cybersécurité et bénéficiera de ses conseils techniques. Nous ne considérons pas que le caractère arbitraire des décisions d'un ministre constitue un risque.

Lorsqu'une action perturbatrice ou destructrice est sur le point de se produire, il est primordial de pouvoir réagir rapidement. Le projet de loi tel qu'il est formulé permet de réagir rapidement. Il ne dit pas d'ignorer les experts techniques. Il ne dit pas d'agir de manière unilatérale. Il est conçu pour garantir une réponse rapide, ce qui, comme nous le savons, est primordial dans le domaine de la cybersécurité pour prévenir ou réagir à un incident en cours.

Chak Au: Parfait.

Dans vos observations, vous avez également mentionné que le projet de loi C-8 part d'une bonne intention et qu'il est nécessaire. Pourquoi pensez-vous, ou pensez-vous que le projet de loi permettrait de résoudre la plupart des problèmes?

Todd Warnell: Je vais m'appuyer sur la question que vous avez posée lors de la séance précédente.

Honnêtement, ce problème ne disparaîtra jamais. Le paysage des cybermenaces est en constante évolution, et il n'y a pas de fin en vue. Pour revenir au commentaire que vous avez formulé lors de la dernière séance, il s'agit d'une première étape. D'autres étapes suivront. Il y aura toujours des mesures à prendre. La technologie, les capacités et le paysage des cybermenaces continueront d'évoluer. Nous parlons et traitons de technologies qui sont actuellement déployées à grande échelle. Nous savons que l'intelligence artificielle continue de progresser rapidement. Le niveau d'attention accordé à cette question était déjà bien supérieur avant même que cette loi n'existe sous sa forme précédente, à savoir le projet de loi C-26.

Si ce projet de loi, tel qu'il est structuré, est important, c'est parce qu'il ne précise pas les technologies, l'approche ou les capacités nécessaires pour réagir. Il est volontairement large et vaste, car nous savons qu'il ne cessera d'évoluer très rapidement. Cette capacité du projet de loi suscite la consternation et soulève des problèmes. Je sais que de nombreux partenaires industriels et secteurs souhaiteraient des lignes de démarcation très claires et précises, mais celles-ci compromettraient la capacité à s'adapter à l'évolution des menaces, des capacités et des tactiques utilisées à travers le monde.

Chak Au: Encore une fois, il est évident que nous ne devrions pas essayer de rattraper un retard.

Quelle recommandation pourriez-vous formuler pour nous aider à être plus proactifs et à garder une longueur d'avance sur les criminels?

Todd Warnell: Encore une fois, je recommanderais de continuer d'encourager les partenariats public-privé qui existent aujourd'hui. Je recommanderais également de continuer de promouvoir ces éléments comme étant des éléments obligatoires pour la coordination et la collaboration entre le gouvernement et les autorités techniques, ainsi que les autorités compétentes du secteur privé. Ce serait ma principale recommandation.

Chak Au: Parfait.

Ma prochaine question s'adresse à M. Bradley.

Je comprends que dans les règlements et toutes sortes de procédures de production de rapport... Vous disposez d'un organisme professionnel. Vous disposez d'une norme professionnelle déjà établie. Le gouvernement tente de créer un autre niveau.

Êtes-vous d'accord pour dire que, si la norme industrielle est déjà plus stricte que la norme gouvernementale requise, il serait préférable que le gouvernement adopte la norme professionnelle ou permette à celle-ci de prévaloir, plutôt que d'imposer une norme supplémentaire? Êtes-vous d'accord?

Francis Bradley: Je suis tout à fait d'accord. C'est précisément ce que nous souhaitons dans ce cas. Nous fonctionnons actuellement sous...

[*Français*]

La vice-présidente (Claude DeBellefeuille): Je suis désolée de vous interrompre, monsieur Bradley. Je n'ai pas un rôle facile quand je dois interrompre les gens qui fournissent des réponses.

Merci beaucoup, monsieur Au.

Je passe maintenant la parole à Mme Acan pour cinq minutes.

Sima Acan: Merci, madame la présidente.

[*Traduction*]

Monsieur Warnell, j'ai eu le privilège de visiter Bruce Power cet été. Je tiens tout d'abord à vous remercier pour le travail acharné que vous accomplissez dans le secteur de l'électricité et pour votre position de leader mondial dans l'utilisation des technologies nucléaires en médecine, tant pour la stérilisation des dispositifs à usage unique que pour votre système de production d'isotopes unique en son genre. On l'utilise pour traiter le cancer. Vous aidez des centaines de milliers de patients.

L'Ontario produit environ 30 % de son électricité grâce à Bruce Power, et contribue à hauteur d'environ 40 % au PIB du Canada. La garantie d'un approvisionnement fiable en énergie est un facteur clé pour maintenir la sécurité économique et nationale de notre pays. Compte tenu du rôle essentiel que joue Bruce Power dans l'approvisionnement de l'Ontario en électricité, pourquoi est-il essentiel de protéger les infrastructures critiques du Canada contre les cybermenaces et autres acteurs malveillants?

Ma deuxième question est la suivante: comment le projet de loi C-8 répond-il à ces risques?

● (1250)

Todd Warnell: Je commencerai par dire que la capacité de Bruce Power à poursuivre ses activités, à fournir de l'électricité et à rester connecté, compte tenu de notre position et de nos pratiques en matière de défense et de profondeur liées à la sécurité, n'a aucune importance si notre produit ne peut être livré aux Canadiens. Elle n'aura aucune valeur si elle ne permet pas d'alimenter les appareils utilisés dans les télécommunications ou les transports pour permettre aux Canadiens de se déplacer et de communiquer dans tout le pays. Bruce Power n'est pas une île. Nous sommes un atout essentiel, mais notre produit doit être consommé par le biais de l'utilisation de l'électricité dans l'ensemble de l'industrie.

L'importance de ce projet de loi ne réside pas tant dans l'amélioration concrète des pratiques, comme le disait M. Bradley. Le secteur de l'électricité dans son ensemble dispose d'approches bien établies en matière de cybersécurité depuis deux décennies ou plus. Fondamentalement, le système collectif de systèmes est vulnérable. La fragilité se situe en aval. Il est dans l'intérêt de tous les Canadiens d'harmoniser les exigences relatives aux programmes et pratiques de cybersécurité et à la gestion des risques liés aux fournisseurs. Je ne suis pas ici aujourd'hui pour défendre les intérêts de Bruce Power. Je suis ici pour m'assurer que l'électricité et les isotopes puissent être acheminés là où on en a besoin, en particulier en période de crise ou de perturbation.

Sima Acan: Merci beaucoup.

Monsieur Bradley, souhaitez-vous ajouter quelque chose à ce sujet?

Francis Bradley: Oui.

Les interdépendances sont probablement l'enjeu crucial dans ce dossier. Elles l'ont toujours été, du moins de notre point de vue, depuis que l'on a commencé à discuter du projet de loi et au cours de son évolution, ces 10 dernières années. Nous avons participé à certaines de ces discussions initiales et nous étions favorables à une forme de législation, étant donné que le secteur de l'électricité, à grande échelle, est soumis à des normes obligatoires en matière de protection des infrastructures critiques et de cybersécurité.

Notre préoccupation a toujours été les autres éléments interdépendants de l'économie et de la chaîne d'approvisionnement qui fournissent des services aux clients finaux. Qu'en est-il du transport? Qu'en est-il des télécommunications? Qu'en est-il de la finance? Ils dépendent de nous. Nous dépendons d'eux. Nous savons que la situation est satisfaisante chez nous, mais nous avons des questions au sujet des autres secteurs.

Un texte législatif aussi large nous donne une plus grande assurance que l'ensemble des infrastructures critiques est protégé. Nous avons toujours été favorables à cette évolution, en raison des préoccupations liées à l'interdépendance.

Sima Acan: Merci beaucoup.

Monsieur Warnell, compte tenu des résultats du récent exercice de préparation aux situations d'urgence simulant une cyberattaque à Bruce Power, les exploitants d'infrastructures essentielles du Canada sont-ils bien préparés à répondre aux cybermenaces, y compris à Bruce Power? En outre, comment le projet de loi C-8 renforce-t-il leurs capacités et leur fournit-il des outils supplémentaires pour améliorer leur résilience?

Todd Warnell: Nous avons été très satisfaits du résultat inédit d'un exercice de cette ampleur, baptisé Huron Unity, que nous venons de mener à bien ici à la mi-novembre. Conformément à notre réglementation, celui-ci était auparavant axé sur la sûreté nucléaire. Nous y avons également intégré, pour la toute première fois, un véritable événement de perturbation numérique, afin de pouvoir continuer d'apprendre et de progresser vers l'excellence dans la gestion des événements à plusieurs échelles ou à multiples facettes.

Le projet de loi C-8 joue un rôle important dans la poursuite des travaux que nous avons réalisés, car grâce à lui, la pratique consistant à considérer la cybersécurité comme un élément à part entière et non comme un simple accessoire, deviendra acceptable et courante dans tous les secteurs d'infrastructures critiques. Il ne s'agit plus d'un domaine distinct. La cybersécurité est essentielle à la continuité des activités et à la garantie de l'obtention des résultats escomptés.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Merci infiniment, monsieur Warnell. Je m'excuse encore une fois de devoir vous arrêter alors que vos propos sont très intéressants.

C'est maintenant à mon tour d'avoir la parole pour deux minutes et demie.

Monsieur Bradley, tantôt, je vous ai senti un peu bousculé. Pourriez-vous me parler de l'importance du partenariat que vous avez avec le Centre canadien pour la cybersécurité? Il est important de bien comprendre les conséquences du projet de loi C-8 sur ce partenariat.

● (1255)

[*Traduction*]

Francis Bradley: Comme je l'ai mentionné plus tôt, nous entretenons des relations très solides avec le Centre pour la cybersécurité et ses responsables. Nous sommes l'un des premiers secteurs avec lesquels ce centre a commencé à établir une collaboration étroite. Bon nombre de mes membres, tant au niveau des PDG que des dirigeants de l'information, possèdent des cotes de sécurité et participent à des réunions et discussions classifiées. D'ailleurs, cette semaine encore, nous avons reçu un groupe.

De même, de nombreux renseignements ont été échangés dans cet espace confidentiel au sujet des difficultés et de certains événements qui se produisent dans le secteur. Cette relation a permis de partager des renseignements de manière très efficace. Je sais qu'ils envisagent d'appliquer ce modèle à d'autres secteurs afin de partager efficacement les renseignements.

Fondamentalement, ma préoccupation au sujet de ce projet de loi porte, comme je l'ai dit précédemment, sur la possibilité d'un « refroidissement » de ce partage de renseignements très efficace qui s'est développé au fil des ans, tant pour ce qui est des renseignements classifiés que non classifiés, et qui pourrait être compromis. Ces discussions ont permis de mettre en évidence la grande valeur de ce secteur, mais aussi celle du Centre pour la cybersécurité et, plus généralement, de l'ensemble des infrastructures critiques. Plus les employés du Centre pour la cybersécurité en apprendront sur les enjeux du secteur, plus ils seront en mesure d'aider les autres secteurs.

Ces canaux de partage de renseignements sont absolument essentiels, et je serais très préoccupé par toute mesure qui pourrait nuire à quelque chose que nous avons passé beaucoup de temps à examiner, à développer et à bâtir.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Il y aurait donc un risque que les partenaires retiennent certaines informations par crainte qu'elles soient utilisées à mauvais escient. Est-ce bien ça?

[*Traduction*]

Francis Bradley: Tout à fait, et cette préoccupation existait déjà il y a 20 ans, lorsque la NERC a été créée et que des normes obligatoires ont commencé à être mises en place, alors qu'auparavant il n'y en avait tout simplement pas.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Merci beaucoup, monsieur Bradley. Même quand c'est à mon tour, je dois vous interrompre lorsque le temps de parole est écoulé.

Je passe maintenant la parole à M. Caputo pour cinq minutes.

Frank Caputo: Merci, madame la présidente.

[*Traduction*]

Je voudrais commencer par présenter une motion pour laquelle un avis a été donné. Elle a été distribuée dans les deux langues officielles, et j'espère que tous les députés ont eu l'occasion de la lire. Elle est simple et claire, et j'espère qu'elle sera adoptée rapidement avec l'appui unanime de tous mes collègues. Nous pourrons ensuite reprendre les travaux du Comité.

Je ne crois pas avoir besoin de lire la motion afin qu'elle figure dans le procès-verbal, car elle a été distribuée. C'est tout ce que j'ai à dire pour le moment.

Je vous remercie de votre attention.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Vous proposez donc officiellement la motion dont vous aviez donné avis, monsieur Caputo, et vous voulez maintenant en discuter, est-ce exact?

[*Traduction*]

Frank Caputo: La motion vise essentiellement à reporter le début de l'examen article par article du projet de loi C-8jusqu'à ce que la ministre ait comparu devant le Comité.

[*Français*]

La vice-présidente (Claude DeBellefeuille): C'est parfait. La motion est recevable, puisqu'elle est en lien avec le projet de loi C-8.

Y a-t-il des commentaires sur la motion qui a été distribuée par M. Caputo? Tous les membres du Comité l'ont-ils reçue dans les deux langues officielles? Y a-t-il des personnes qui voudraient intervenir?

Monsieur Ramsay, vous avez la parole.

Jacques Ramsay: M. Caputo pourrait-il nous préciser les raisons de cette motion? Le ministre a déjà témoigné au sujet du projet de loi C-8.

[*Traduction*]

Frank Caputo: La ministre n'a pas comparu devant nous, même si elle a été invitée à le faire. Nous voulons rencontrer la ministre de l'Industrie.

Je vous remercie de votre attention.

[*Français*]

La vice-présidente (Claude DeBellefeuille): J'aimerais effectivement clarifier que, en ce qui concerne les télécommunications, la ministre de l'Industrie n'a pas témoigné dans le cadre du projet de loi C-8.

Je crois que ça répond à votre question, monsieur Ramsay.

Y a-t-il d'autres interventions?

Madame Acan, vous avez la parole.

[*Traduction*]

Sima Acan: Je voudrais proposer un amendement à la motion qui vise à supprimer tout ce qui suit les mots « projet de loi C-8 ».

[*Français*]

La vice-présidente (Claude DeBellefeuille): D'accord, vous voulez présenter un amendement à la motion de M. Caputo. L'avez-vous distribué? Cela a-t-il fait l'objet de discussions? Avez-vous le texte?

Voulez-vous lire votre amendement, madame Acan?

[*Traduction*]

Sima Acan: Je peux lire la motion qui en résultera. Après la modification, elle indiquera ce qui suit: « Que le président soit chargé d'inviter la ministre de l'Industrie à comparaître dans le cadre de l'étude du projet de loi C-8 ».

[*Français*]

La vice-présidente (Claude DeBellefeuille): Un amendement à la motion a donc été proposé.

Y a-t-il des réactions ou des questions sur l'amendement que vient de proposer Mme Acan à la motion de M. Caputo?

Comme personne ne semble vouloir intervenir, nous allons soumettre l'amendement à un vote par appel nominal.

Après le vote, je constate qu'il y a égalité des voix. La présidence doit donc trancher. Je suis contre l'amendement proposé par Mme Acan.

(L'amendement est rejeté par 5 voix contre 4.)

● (1300)

La vice-présidente (Claude DeBellefeuille): Nous revenons donc à la motion initiale de M. Caputo.

Y a-t-il d'autres commentaires? Sinon, nous allons passer au vote.

Souhaitez-vous intervenir, madame Acan?

[*Traduction*]

Sima Acan: Oui. Je voudrais apporter un autre amendement à la motion, si cela est possible, madame la présidente.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Ai-je bien compris que vous voulez proposer un autre amendement?

[*Traduction*]

Sima Acan: C'est un autre amendement.

[*Français*]

La vice-présidente (Claude DeBellefeuille): D'accord. Allez-y, madame Acan.

[*Traduction*]

Sima Acan: Je voudrais proposer un amendement visant à supprimer tout ce qui suit les mots « projet de loi C-8 », mais aussi à ajouter ce qui suit: « au plus tard le vendredi 30 janvier 2026 ». Je souhaite que le passage suivant soit supprimé de la motion: « et qu'une réunion pour l'examen article par article soit prévue », et j'aimerais ajouter ce qui suit: « à la séance suivant la comparution de la ministre et que le Comité ne passe pas à d'autres travaux avant la fin de l'examen article par article ».

[*Français*]

La vice-présidente (Claude DeBellefeuille): L'amendement vient d'être proposé, mais il n'a pas été déposé dans les deux langues officielles.

Monsieur Lloyd, voulez-vous intervenir au sujet de cet amendement?

[*Traduction*]

Dane Lloyd: Oui, j'aimerais parler de l'amendement.

Nous entendons parler de cet amendement pour la première fois, et il semble quelque peu complexe. J'aimerais donc le recevoir par écrit.

Si j'ai bien compris, l'amendement stipule que l'examen article par article ne commencera pas avant le 30 janvier? Cela permet à la ministre de comparaître devant le Comité d'ici le 30 janvier, après quoi l'examen article par article commencera.

[*Français*]

La vice-présidente (Claude DeBellefeuille): J'aimerais vous informer que nous avons les services d'interprétation jusqu'à 13 h 10. Ensuite, il faudra donner une pause de 30 minutes aux interprètes avant de recommencer nos travaux. Je voulais que vous sachiez qu'il nous reste actuellement sept minutes avant de devoir faire une pause, après quoi nous pourrons poursuivre nos travaux.

Voulez-vous intervenir, madame Acan?

[*Traduction*]

Sima Acan: Merci, madame la présidente.

Je voudrais lire dans son intégralité la motion qui en résultera, afin que tout soit clair:

> Que le président soit chargé d'inviter la ministre de l'Industrie à comparaître dans le cadre de l'étude du projet de loi C-8 au plus tard le vendredi 30 janvier 2026, et qu'une réunion pour l'examen article par article soit prévue à la séance suivant la comparution de la ministre, et que le Comité ne passe pas à d'autres travaux avant la fin de l'examen article par article.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Est-ce bien compris par tout le monde? Est-ce que ça va?

Y a-t-il des discussions sur l'amendement?

Monsieur Caputo, vous avez la parole.

[*Traduction*]

Frank Caputo: Pour être clair, cela signifie-t-il que nous nous retrouverons dans la même situation qu'en ce qui concerne le projet de loi C-12, c'est-à-dire que nous resterons ici littéralement jusqu'à minuit ou plus tard? Est-ce bien ce dont nous parlons?

[*Français*]

Sima Acan: Non.

Une voix: [*Inaudible*]

La vice-présidente (Claude DeBellefeuille): Attendez un instant. Je vous rappelle que M. Caputo s'adresse à la présidence lorsqu'il pose sa question.

Madame Acan, voulez-vous répondre à la question de M. Caputo?

Sima Acan: La réponse est non, madame la présidente.

La vice-présidente (Claude DeBellefeuille): Monsieur Lloyd, voulez-vous intervenir?

[*Traduction*]

Dane Lloyd: Merci, madame la présidente.

Je vous remercie de la précision qui a été apportée par la députée d'en face.

C'est la fin d'une semaine de session. Cela signifie-t-il qu'aucun autre travail ne pourra être entrepris avant la réunion avec la ministre de l'Industrie? Mardi, par exemple, aucun autre travail ne pourra être entrepris. Est-ce exact?

Sima Acan: Je pense que oui. C'est juste que nous examinerons chaque article au cours de chaque réunion jusqu'à ce que ce travail soit terminé. C'est mon intention.

● (1305)

Dane Lloyd: D'accord. Donc...

[*Français*]

La vice-présidente (Claude DeBellefeuille): Attendez un instant, monsieur Lloyd et madame Acan. Je vais donner la parole au greffier, qui pourra apporter une clarification.

[*Traduction*]

Le greffier: Madame Acan, essayez-vous de faire en sorte qu'une fois que le Comité aura commencé l'examen article par article, il ne passera pas à d'autres travaux, ou voulez-vous dire une fois que la ministre aura été invitée?

Sima Acan: Ce que je dis, c'est que l'examen...

Tout d'abord, j'aimerais travailler sur le projet de loi C-8 au plus tard le vendredi 30 janvier, et l'examen article par article sera prévu après la comparution de la ministre. Nous ne passerons pas à d'autres travaux avant la fin de l'examen article par article.

[*Français*]

La vice-présidente (Claude DeBellefeuille): Y a-t-il des questions ou des clarifications nécessaires au sujet de l'amendement proposé par Mme Acan?

Frank Caputo: Madame la présidente, j'aimerais avoir l'amendement en anglais, s'il vous plaît.

[*Traduction*]

J'aimerais le recevoir par écrit, s'il vous plaît.

[*Français*]

La vice-présidente (Claude DeBellefeuille): C'est parfait. De toute façon, il reste deux minutes avant la fin des services d'interprétation, alors je suggère de suspendre la séance. Au retour, nous aurons l'amendement sous les yeux.

● (1305)

(Pause)

● (1305)

La vice-présidente (Claude DeBellefeuille): Nous reprenons nos travaux.

Chers témoins, mes collègues du Comité me permettront de vous remercier. Vous pouvez partir. Nous vous remercions infiniment de vos témoignages dans le cadre du projet de loi C-8.

Nous étions en train de débattre de l'amendement.

Monsieur Ramsay, souhaitez-vous intervenir?

Jacques Ramsay: Je propose d'ajourner la discussion à la prochaine fois.

La vice-présidente (Claude DeBellefeuille): Vous proposez donc d'ajourner le débat à mardi prochain, est-ce bien ça?

● (1310)

Jacques Ramsay: Oui.

La vice-présidente (Claude DeBellefeuille): Est-ce que le Comité est d'accord pour reprendre cette discussion mardi?

Des députés: D'accord.

La vice-présidente (Claude DeBellefeuille): C'est parfait. La séance est levée.