CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

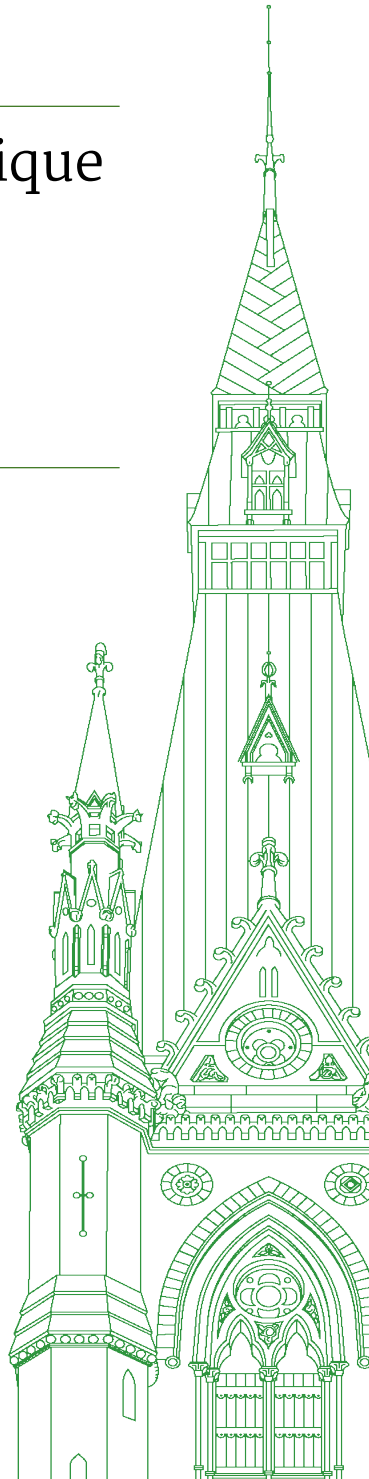
45e LÉGISLATURE, 1re SESSION

Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 010

Le jeudi 30 octobre 2025



Président : Jean-Yves Duclos

Comité permanent de la sécurité publique et nationale

Le jeudi 30 octobre 2025

● (1105)

[*Français*]

Le président (L'hon. Jean-Yves Duclos (Québec-Centre, Lib.)): Je déclare la séance ouverte.

Bonjour à tous. Je vous souhaite la bienvenue à cette 10e réunion du Comité permanent de la sécurité publique et nationale de la Chambre des communes.

Avant de présenter nos distingués invités et de leur permettre de se prononcer sur l'important sujet de cette rencontre, j'aimerais inviter M. Ramsay, à la suite de notre discussion terminale de mardi dernier, à préciser les travaux relatifs au projet de loi C-12.

Jacques Ramsay (La Prairie—Atateken, Lib.): Merci, monsieur le président.

Suivant les discussions que nous avons eues de façon informelle depuis mardi, j'aimerais modifier la proposition faite relativement au projet de loi C-12 de façon à ce qu'elle se lise comme suit:

> Nonobstant la motion adoptée par le Comité le mardi 28 octobre 2025, concernant l'étude du projet de loi C-12, Loi concernant certaines mesures liées à la sécurité de la frontière canadienne et à l'intégrité du système d'immigration canadien et d'autres mesures connexes liées à la sécurité,
>
> Que le Comité procède à l'étude article par article du projet de loi après la fin des témoignages des témoins lors de la quatrième séance, et
>
> Que le Comité ne s'ajourne pas avant que l'étude article par article soit terminée.

Le président: Je vois que Mme DeBellefeuille veut prendre la parole. Ce sera ensuite au tour de M. Caputo.

Madame DeBellefeuille, nous vous écoutons.

Claude DeBellefeuille (Beauharnois—Salaberry—Soulanges—Huntingdon, BQ): Merci, monsieur le président.

J'invoque le Règlement.

Nous ne penchons pas sur des travaux de comité. Nous sommes ici pour étudier le projet de loi C-8.

Nous avons une motion au sujet de l'étude du projet de loi C-12 dont nous avons débattu mardi passé, et que nous avons modifiée et adoptée. Par conséquent, je ne pense pas qu'il soit conforme à la procédure que, ce matin, devant nos témoins et en public, nous revenions sur une décision qui a été prise mardi.

Je vous rappelle, monsieur le président, que nous avons consacré une demi-heure aux travaux du Comité, mardi, pour planifier les travaux relatifs à l'étude du projet de loi C-12, et que nous nous sommes entendus. Je considère qu'il est inacceptable de reprendre cette discussion ce matin.

J'invoque donc le Règlement parce que c'est hors sujet. Nous étudions le projet de loi C-8, qui n'a aucun rapport avec le projet de loi C-12.

Le président: C'est effectivement un choix de la présidence de régler ce problème, parce qu'il est pressant, pour le greffier et les analystes parlementaires, d'avoir une idée de ce qui s'en vient. C'est donc pour une raison d'efficacité que je souhaite que le Comité clarifie la confusion qui a pu se produire mardi, étant donné que nous n'avons pas pris tout le temps nécessaire pour tenir cette discussion mardi dernier.

Claude DeBellefeuille: Monsieur le président, j'accepte difficilement votre explication, parce qu'après avoir débattu de la motion pendant une demi-heure, nous nous sommes entendus. Maintenant, vous voulez que nous nous entendions rapidement sur quelque chose qui a été débattu pendant 30 minutes.

Ce que je comprends, monsieur le président, c'est qu'il y a eu des discussions et que les conservateurs sont probablement d'accord sur votre proposition, et vous vous sentez à l'aise de ne pas suivre le Règlement. Pour ma part, je trouve que c'est une très mauvaise façon de diriger le Comité, si vous me permettez de le dire.

Je ne vous en veux pas personnellement. Vous êtes un peu coincé. Vous décidez de ne pas le mettre au programme des travaux de comité pour que nous puissions avoir le temps de nous entendre, mais, ce matin, parce qu'il y a eu une négociation entre les libéraux et les conservateurs, vous ne pouvez pas me demander, tout à coup, d'accepter docilement ce changement, en trois ou quatre minutes, sans intervenir.

Cela ne respecte pas le Règlement, c'est hors sujet et je conteste votre décision.

Le président: Madame DeBellefeuille, vous avez entièrement le droit d'exprimer votre point de vue là-dessus. Toutes ces discussions sont le fruit de conversations tenues hors de ce comité, mais elles tiennent aussi compte de l'ensemble des travaux du Comité, y compris des travaux qui sont encore plus importants pour vous.

Je sais qu'il y a eu des conversations, et on arrivera peut-être dans un moment au projet de loi C-8 et à l'étude sur la frontière que nous aimerions bientôt terminer.

Il faut donc prendre en considération l'ensemble de ces facteurs pour maximiser l'efficacité des travaux du Comité. Je considère personnellement que, pour aider le greffier et les analystes, et les députés à faire leur travail correctement, il est utile de clarifier maintenant cette confusion.

Claude DeBellefeuille: Je vous dis simplement que je ne trouve pas cela acceptable.

Je pense que nous avons eu une bonne entente lors de la dernière réunion. Les conservateurs sont prêts à appuyer l'amendement. Je le tiens pour acquis. Les libéraux se sentent très à l'aise de revenir sur une question qui a été réglée à la dernière réunion. Au fond, c'est un test de confiance.

Le Bloc québécois n'a pas l'intention de bloquer le projet de loi C-12. Nous vous l'avons dit, et nous avons même facilité son débat. Nous n'avons pas du tout l'intention de faire de l'obstruction ou de déposer une liasse d'amendements. Tout le monde s'entend. J'ai l'impression qu'il en va de même chez les conservateurs.

Je me bats pour une question de principe. Si vous procédez comme vous voulez le faire aujourd'hui, cela créera un précédent.

C'est vous, le gardien de l'ordre et de la procédure. Je m'attends à ce que vous ne participiez pas à des discussions informelles partisanes. Vous devez être neutre.

● (1110)

Le président: Vous avez tout à fait raison.

Je vous rassure, madame DeBellefeuille, je ne participe pas à ces discussions. J'en reçois les conclusions et les directives de la part de l'ensemble des membres de ce comité. Mon travail, c'est de vous aider et de nous aider, comme députés, à accomplir le meilleur travail possible. Il faut trouver un certain équilibre et, parfois, faire des compromis.

Si on veut procéder à l'étude des projets de loi C-12 et C-8 et achever l'étude importante sur la gestion de la frontière, il faut que les analystes et le greffier puissent faire leur travail efficacement. C'est pour cela que je présente cette occasion ce matin.

M. Caputo a la parole.

Frank Caputo (Kamloops—Thompson—Nicola, PCC): Merci, madame DeBellefeuille. Je comprends votre position.

[*Traduction*]

J'aimerais prendre une minute pour exposer très clairement, je l'espère, la position des conservateurs.

Les conservateurs appuieront cette motion concernant le projet de loi C-12 — c'est là que nous arrivons au projet de loi C-8 —, pourvu que l'on indique clairement que le ministre comparaîtra sur les projets de loi C-12 et C-8 lors de deux réunions distinctes. Mes collègues m'ont assuré, si j'ai bien compris, que le ministre comparaîtra lors d'une réunion consacrée au projet de loi C-12, puis lors d'une autre réunion consacrée au projet de loi C-8. Si c'est le cas, nous pouvons appuyer les deux propositions.

[*Français*]

Le président: M. Ramsay a la parole.

[*Traduction*]

Jacques Ramsay: Monsieur Caputo, nous avions compris que ce serait deux heures au total: une heure pour le projet de loi C-12 et une heure pour le projet de loi C-8. Vous pourriez peut-être expliquer au Comité pourquoi vous voulez que cela se fasse lors de deux réunions distinctes.

Frank Caputo: J'avais compris qu'il s'agissait d'une entente avec les leaders parlementaires. C'est pour cette raison que j'avance cela. J'essaie simplement de donner suite à l'entente.

Le président: Habituellement, les ministres comparaissent en comité pendant une heure lors de l'examen d'un projet de loi ou d'une étude. C'est ce que le ministre fera. Nous n'avons pas encore établi à quel moment il le fera, mais il sera ici pendant une heure au sujet du projet de loi C-8. Il s'est également engagé à témoigner pendant une heure au sujet du projet de loi C-12.

Monsieur Ramsay, nous vous écoutons.

Jacques Ramsay: Nous serons d'accord avec M. Caputo. Si c'est ce que souhaitent les conservateurs, le ministre comparaîtra lors de deux réunions distinctes.

Le président: D'accord. Ce n'est pas seulement ce que souhaitent les conservateurs; c'est aussi la procédure normale. Parfois, il n'est peut-être pas possible de s'y conformer, mais c'est ce à quoi on s'attend, la plupart du temps.

[*Français*]

Cela étant dit, je peux procéder au vote sur la motion proposée au sujet du projet de loi C-12.

Qui est en faveur de cette motion sur le projet de loi C-12?

Qui n'est pas en faveur de cette motion sur le projet de loi C-12?

Monsieur Ramsay, souhaitez-vous parler du projet de loi C-8, qui est à l'ordre du jour de la discussion d'aujourd'hui?

Jacques Ramsay: Oui, puisque M. Caputo a abordé le sujet.

Nous avons aussi une motion au sujet du projet de loi C-8 qui a été envoyée aux conservateurs et au Bloc québécois. Elle se lit ainsi:

> Que, en relation avec l'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, le Comité consacre quatre réunions aux comparutions des témoins, incluant le ministre de la Sécurité publique;
>
> Que le Comité consacre au plus deux réunions à l'étude article par article; et
>
> Que le Comité termine la réunion restante de l'étude sur la gestion de la frontière Canada-États-Unis et fournisse les directives de rédaction aux analystes, conformément à la motion adoptée le jeudi 18 septembre 2025, avant de reprendre l'étude du projet de loi C-8.

Le président: Merci, monsieur Ramsay.

Y a-t-il consensus ou unanimité sur cette motion?

● (1115)

Claude DeBellefeuille: Est-il prévu que la ministre de l'Industrie comparaisse? Dans le projet de loi C-8, on lui octroie beaucoup de pouvoirs. Sinon, je proposerai un amendement.

Il me semble que je n'ai rien entendu à cet égard dans la motion lue par M. Ramsay.

Le président: Dans la motion que j'ai et qui vous a été, je l'espère...

Claude DeBellefeuille: Ce n'est pas ce qui m'a été remis.

Le président: La motion indique « Que le Comité consacre quatre réunions aux comparutions des témoins, incluant le ministre de la Sécurité publique » et « Que le Comité consacre au plus deux réunions à l'étude article par article ».

La ministre de l'Industrie n'y est pas mentionnée.

Claude DeBellefeuille: Exactement.

Comme je constate que la ministre de l'Industrie n'est pas mentionnée dans la motion, je propose un amendement.

Je considère que, dans le projet de loi C-8, on octroie un grand pouvoir à la ministre de l'Industrie, qui gère les télécommunications. Je trouverais raisonnable qu'elle se présente devant le Comité pour répondre à nos questions pendant une heure.

Je propose donc un amendement à la motion afin que la ministre comparaisse.

Le président: Comme on le sait, le Comité n'a pas le pouvoir de forcer un ministre ou une ministre à comparaître.

Claude DeBellefeuille: Les lois dont parle le projet de loi concernent son ministère.

Le président: Oui, mais nous sommes d'accord sur le fait que nous ne pouvons pas forcer un ministre ou une ministre à comparaître. Par contre, nous pouvons l'inviter à venir et, pour ce faire, il faut faire un amendement à la motion.

Claude DeBellefeuille: Monsieur le président, je m'excuse, mais j'aimerais que vous suiviez les procédures du Comité. Je viens de formuler un amendement. Normalement, nous devrions en débattre et trancher là-dessus.

Le président: Oui.

Claude DeBellefeuille: Formellement, je propose ceci: « Que la motion soit modifiée par adjonction, après les mots « ministre de la Sécurité publique », de ce qui suit : « et la ministre de l'Industrie ».

Je veux que ce soit ajouté à la motion. Je ne pense pas que cela pose problème.

Monsieur le président, voulez-vous, s'il vous plaît, animer le débat pour que le Comité puisse trancher là-dessus?

Le président: Très bien.

Il y a deux choses. En premier lieu, nous avons clarifié le fait que, dans la motion actuelle, il n'y a pas d'invitation à la ministre de l'Industrie. En second lieu, Mme DeBellefeuille soumet un amendement à cette motion pour inviter la ministre de l'Industrie, en plus de l'invitation au ministre de la Sécurité publique.

Cet amendement est jugé recevable.

Monsieur Ramsay ou monsieur Caputo, avez-vous des commentaires à faire là-dessus?

[*Traduction*]

Frank Caputo: Pouvons-nous obtenir la version écrite, s'il vous plaît?

Le président: Oui. Il va sans dire que la traduction et l'interprétation compliquent parfois les choses. Si vous me le permettez, je vais essayer de résumer cet amendement en anglais. La motion reste la même...

[*Français*]

Claude DeBellefeuille: Les interprètes me disent à l'oreille qu'elles n'ont pas reçu le texte de la motion. C'est quand même une base. Si elles pouvaient avoir le texte, ce serait plus facile de l'interpréter.

Le président: Est-ce que quelqu'un de l'équipe des libéraux peut...

Une voix: Je propose de suspendre la réunion.

Le président: D'accord.

Nous allons faire une pause quelques instants, le temps de nous assurer que les interprètes ont une copie de la motion.

● (1120)

Nous avançons, mais pas aussi vite que certains le croyaient.

J'informe les différents membres de l'équipe qu'il n'y a pas d'entente claire entre les partis sur la motion relative au projet de loi C-8. Cela nous amène à reporter cette discussion à un peu plus tard étant donné que nous avons des témoins importants à entendre.

Voilà donc ce qui va se passer.

● (1125)

[*Traduction*]

Voilà qui m'amène à quelque chose qui est sans doute un peu plus opportun: nous accueillons maintenant quatre témoins importants.

[*Français*]

Je vais commencer par souhaiter la bienvenue à tous nos témoins.

De l'Échange canadien de menaces cybernétiques, nous recevons Mme Jennifer Quaid, directrice exécutive.

De l'ISC2 inc., M. Philip Stupak, directeur principal de la défense des intérêts, se joint à nous.

Du Bureau du commissaire au renseignement, nous recevons l'honorable Simon Noël, commissaire au renseignement, et M. Justin Dubois, directeur exécutif et avocat général.

Enfin, du Commissariat à la protection de la vie privée du Canada, nous recevons M. Philippe Dufresne, commissaire à la protection de la vie privée du Canada, et M. Marc Chénier, sous-commissaire et avocat général principal.

Vous disposez de cinq minutes pour faire vos présentations.

Madame Quaid, la parole est à vous.

[*Traduction*]

Jennifer Quaid (directrice exécutive, Échange canadien de menaces cybernétiques): Merci beaucoup, monsieur le président, et bonjour.

Permettez-moi d'abord de dire que le projet de loi C-8 constitue une étape importante dans la modernisation du cadre de cybersécurité du Canada en corrigeant des lacunes de notre stratégie de cyberdéfense. Il favorise à la fois la reddition de comptes organisationnelle et la résilience à l'échelle nationale, et il met le Canada au diapason d'autres pays.

C'est un privilège pour moi d'être ici aujourd'hui pour représenter l'Échange canadien de menaces cybernétiques, un organisme créé par des entreprises canadiennes dans le seul but de renforcer la cyberrésilience grâce à la collaboration. Nous avons plus de 200 membres, qui représentent 15 secteurs et plus de 1,5 million d'employés. Bon nombre de nos membres représentent les secteurs des infrastructures essentielles touchés par ce projet de loi, tandis que...

[*Français*]

Le président: Madame Quaid, il y a malheureusement un problème technique du côté du son.

Nous allons suspendre la réunion pendant quelques minutes afin de régler le problème le plus rapidement possible.

Voilà. Il semble que ce soit réglé.

Madame Quaid, vous avez la parole.

[*Traduction*]

Jennifer Quaid: Nous avons plus de 200 membres, qui représentent 15 secteurs et plus de 1,5 million d'employés. Bon nombre de nos membres représentent les secteurs des infrastructures essentielles touchés par ce projet de loi, tandis que d'autres — grandes et petites entreprises confondues — composent leur chaîne d'approvisionnement. Les membres se joignent à l'Échange canadien de menaces cybernétiques parce qu'ils veulent échanger de l'information sur les cybermenaces afin de contribuer à accroître la sensibilisation et la résilience d'autres parties, à anticiper les menaces et à prévenir les atteintes à la cybersécurité et la nécessité correspondante de les signaler, ce que ce projet de loi régit. Cependant, leur capacité à échanger des renseignements est limitée.

À l'heure où le Canada renforce sa position en matière de cybersécurité à l'échelle nationale, un concept stratégique mérite une plus grande attention: les dispositions qui offrent une protection contre des poursuites. Il est vrai que le projet de loi à l'étude n'en fait pas mention, mais elles jouent un rôle essentiel dans la promotion de la transparence, la coopération et la résilience dans l'ensemble de notre écosystème numérique. Lorsque nous parlons de cybersécurité, nous nous concentrons souvent sur la technologie: les pare-feu, le chiffrement et l'intelligence artificielle. Or, l'un des outils les plus puissants dont nous disposons pour renforcer nos moyens de défense n'est pas du tout technologique. Il s'agit de la collaboration et de l'échange de renseignements sur les cybermenaces. Cela permet à d'autres parties de mieux se protéger et de prévenir toute atteinte.

Cette collaboration et ces échanges doivent jouir d'une protection législative. Les dispositions qui protègent les organisations contre des poursuites créent un climat de confiance. Nous devons veiller à ce que les organisations qui essaient de faire la bonne chose en communiquant des renseignements utiles sur des auteurs de cyberattaques et leurs techniques ne soient pas punies. Cette protection contribue à empêcher que d'autres parties ne soient victimes d'une atteinte.

Le signalement obligatoire se fait plus tard. Ce qui nous intéresse, c'est la prévention. En l'absence de dispositions qui protègent les gens et les organisations contre des poursuites, trop nombreux sont ceux qui hésitent à parler d'incidents ou de vulnérabilités qui n'atteignent pas le seuil de signalement aux organismes de réglementation. Ils craignent qu'il n'y ait des poursuites, des atteintes à leur réputation ou encore des sanctions et choisissent donc de ne pas divulguer des renseignements essentiels. Par conséquent, les mêmes attaques peuvent avoir des répercussions dans d'autres secteurs et au-delà des frontières. Les auteurs de cyberattaques peuvent continuer d'utiliser les mêmes techniques. Nous l'avons constaté à maintes reprises au cours de la dernière année. Les dispositions dont je parle changent la donne. Elles permettent aux entreprises d'échanger de l'information sur les menaces avec le gouvernement et entre elles, sachant qu'elles seront protégées si elles agissent de manière responsable. Elles n'ont pas à craindre des conséquences juridiques.

L'idée n'est pas de tolérer la négligence ou de protéger les acteurs malveillants, mais plutôt de favoriser un comportement responsable, et de créer la certitude juridique propice à la transparence et la coopération. Au bout du compte, cette protection renforce notre résilience collective. Elle nous permet d'apprendre les uns des autres et d'assurer une collaboration entre les secteurs pour bâtir la confiance nécessaire afin de défendre les Canadiens et les organisations canadiennes. En intégrant des dispositions qui protègent les personnes et les organisations contre des poursuites dans nos politiques et nos cadres législatifs de cybersécurité, nous pourrons créer une culture où le signalement, l'apprentissage et la collaboration seront considérés non pas comme des risques, mais comme des responsabilités. C'est ainsi que nous pourrons passer d'une approche réactive en matière de cybersécurité à un Canada numérique réellement résilient.

Dans le domaine de la cybersécurité, le silence est la véritable menace. Les dispositions qui offrent une protection contre des poursuites font en sorte que l'on peut parler sans crainte et faire ce qui s'impose afin de nous protéger tous.

Je vous remercie.

● (1130)

[*Français*]

Le président: Madame Dandurand, vous avez la parole.

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

Je regarde le temps passer. Je trouve ce groupe très intéressant, mais nous avons retiré beaucoup de temps aux témoins à cause des discussions que nous avons eues au préalable.

Serait-il possible de séparer le temps qu'il reste entre les deux groupes de témoins pour leur donner 45 minutes chacun et pour que nous ayons la chance d'entendre davantage les témoins du premier panel? Sinon, j'ai l'impression que nous ne pourrons pas parler à tout le monde.

[*Traduction*]

Le président: Pour que vous sachiez à quoi vous attendre, je vous informe que la dernière heure et demie sera divisée en deux parties. Nous consacrerons 45 minutes à ce groupe de témoins, et 45 au suivant. Je suppose que personne ne s'y oppose.

Sur ce, je vous remercie, madame Quaid.

Monsieur Stupak, vous avez cinq minutes.

Philip Stupak (directeur principal de la défense des intérêts, ISC2, Inc.): Bonjour, monsieur le président et honorables membres du Comité. Je m'appelle Philip Stupak. Je suis directeur principal de la défense des intérêts à ISC2, l'association professionnelle des professionnels de la cybersécurité. Avant de me joindre à ISC2, j'ai eu le privilège de servir au sein de l'administration Biden-Harris à titre de directeur national adjoint de la cybersécurité à la Maison-Blanche.

ISC2 est la plus grande association de professionnels de la cybersécurité au monde et représente plus de 265 000 membres et associés à l'échelle mondiale. Notre deuxième plus grand bassin de membres se trouve ici même au Canada, avec plus de 14 000 membres. Nous offrons neuf certifications professionnelles, dont la plus reconnue est celle de professionnel agréé en sécurité des systèmes d'information, ou CISSP, largement considérée par les employeurs comme la norme d'excellence en matière d'expertise en cybersécurité.

Je comparais aujourd'hui au nom de nos membres du monde entier pour exprimer le ferme soutien des professionnels de la cybersécurité au projet de loi C-8, Loi concernant la cybersécurité. Nous vivons une période d'incertitude inouïe. Pendant une grande partie de notre histoire commune, la géographie a été un facteur de dissuasion naturel profitant au Canada et aux États-Unis. L'immensité des océans Atlantique et Pacifique offrait une mesure de protection difficile à contourner pour nos adversaires. Cette époque est révolue.

La cyberattaque de Stuxnet en 2010 contre les centrifugeuses iraniennes a démontré, pour la première fois, que la frontière entre le monde numérique et le monde physique peut être franchie et entraîner des conséquences tangibles et réelles. Aujourd'hui, 15 pays possèdent des forces navales hauturières capables de projeter leur puissance au-delà des océans. Huit possèdent des armes nucléaires, et 170 nations sont dotées de cybercapacités. Nous avons déjà vu les effets des cyberattaques ici, au Canada. Les patients des hôpitaux du Sud-Ouest de l'Ontario ont été forcés de reporter des chirurgies et des rendez-vous, ce qui a coûté des millions de dollars et retardé les soins. Les renseignements personnels de 516 000 patients ont été compromis, mais nous savons que les cyberattaques peuvent causer des dommages encore plus importants à plus grande échelle.

Il faut une semaine à des forces navales pour traverser le Pacifique ou quelques minutes à un missile pour atteindre sa cible, mais une cyberattaque pourrait — sans avertissement et sans que l'on sache qui en sont les auteurs — ramener les systèmes hospitaliers à l'époque des flambeaux et des scies à métaux, et la communication à l'époque des expéditions à cheval. Ce ne sont pas là des conjectures. Il faut s'y préparer.

Nos adversaires travaillent activement à saper les infrastructures essentielles. Même des perturbations mineures causées par des armes numériques ou des logiciels malveillants prépositionnés dans des secteurs essentiels pourraient entraîner des interruptions de services, un effondrement des communications, des pannes de courant, des pénuries d'eau et une paralysie des transports au moment et à l'endroit choisis par un acteur qui nous veut du mal. Dans le pire des scénarios, une telle attaque pourrait ramener les sociétés modernes dans des conditions s'apparentant à celles de l'ère préindustrielle.

Cependant, je tiens à être clair: nos adversaires ne sont pas invincibles. Avec de la prévoyance, de la coordination et des mesures stratégiques, nous pouvons et devons nous défendre. Le projet de loi C-8 est une étape essentielle pour veiller à ce que ces moyens de défense soient en place avant qu'ils ne soient nécessaires. Les modifications à la Loi sur les télécommunications sont particulièrement importantes. En interdisant les fournisseurs présentant de grands risques, en écartant l'équipement compromis et en exigeant une préapprobation pour certaines technologies, le projet de loi renforce le secteur qui sous-tend tous les autres secteurs. Les faiblesses dans le domaine des télécommunications affaiblissent tous les autres domaines.

La création de la Loi sur la protection des cybersystèmes essentiels est tout aussi prudente. Elle établit des bases de référence minimales en matière de cybersécurité dans les secteurs les plus essentiels du Canada. J'encourage respectueusement le Comité à envisager d'ajouter les systèmes d'approvisionnement en eau sous réglementation fédérale à cette liste, compte tenu de leur importance fondamentale pour la santé et la sécurité nationales. J'encourage également le gouvernement fédéral à travailler avec ses partenaires provinciaux, territoriaux et municipaux pour veiller à ce que les infrastructures essentielles relevant de leur compétence reçoivent le même niveau de cyberprotection envisagé dans le projet de loi C-8. Une main-d'œuvre qualifiée est essentielle pour exécuter les mesures prévues dans cette loi. Chaque jour, ISC2 forme et certifie des fonctionnaires et des professionnels chargés des infrastructures essentielles qui seront nécessaires pour mettre en œuvre le projet de loi C-8.

Nous ne pouvons pas nous permettre de croire que les menaces qui pèsent sur le mode de vie canadien sont lointaines ou hypothétiques. Elles sont réelles, elles sont présentes et elles exigent une action ferme. La responsabilité de se défendre contre ces menaces incombe en partie à ce comité. Le projet de loi C-8 représente une étape réfléchie, modérée et nécessaire pour nous défendre.

Merci.

● (1135)

[*Français*]

Le président: Monsieur Noël, vous avez la parole.

L'hon. Simon Noël (commissaire au renseignement, Bureau du commissaire au renseignement): Merci, monsieur le président.

Je remercie également les députés de cette invitation.

Je suis accompagné aujourd'hui de Justin Dubois, directeur exécutif et avocat général au Bureau du commissaire au renseignement.

[*Traduction*]

Afin de replacer mes commentaires sur ce projet de loi dans leur contexte, il est utile d'expliquer brièvement mon rôle en tant que commissaire au renseignement.

[*Français*]

Mon rôle est d'approuver ou non certaines activités de sécurité nationale et de renseignement prévues par le Centre de la sécurité des télécommunications, ou CST, et le Service canadien du renseignement de sécurité; ces activités sont respectivement autorisées par le ministre de la Défense nationale et le ministre de la Sécurité publique.

[*Traduction*]

Mon approbation indépendante est nécessaire, car les activités autorisées par les ministres peuvent être contraires à la loi ou porter atteinte aux attentes raisonnables des Canadiens en matière de protection de la vie privée. Ce n'est qu'avec mon approbation que les activités peuvent être menées.

● (1140)

[*Français*]

Le poste de commissaire que j'occupe a été créé en 2019. Le mandat confié au commissaire par le législateur à cette époque est un élément particulièrement pertinent pour l'étude de ce projet de loi. Il comprend la possibilité pour le CST de réagir efficacement aux cyberincidents touchant les systèmes fédéraux et les systèmes désignés comme importants pour le gouvernement du Canada. L'une de mes fonctions consiste plus précisément à examiner les autorisations ministérielles qui permettent au CST de mener des activités de cybersécurité sur ces systèmes.

[*Traduction*]

Mon approbation est également nécessaire parce que les activités de cybersécurité menées par le CST entraînent la collecte d'énormes quantités d'informations, y compris des informations pour lesquelles les Canadiens ont des attentes raisonnables en matière de protection de la vie privée. Pour mener efficacement ses activités de cybersécurité, le CST doit recueillir ces informations.

J'approuve seulement l'autorisation ministérielle lorsque je suis convaincu que le ministre a trouvé un équilibre raisonnable entre la sécurité du Canada et la vie privée des Canadiens. Cela implique notamment de veiller à ce que des mesures appropriées soient mises en place pour protéger la vie privée des Canadiens.

[*Français*]

Dans le cadre de mes fonctions de commissaire, je constate l'énorme valeur qu'a une approche nationale en matière de cybersécurité. Le Canada doit disposer des outils nécessaires pour protéger ses systèmes électroniques essentiels. Cependant, ces outils doivent s'accompagner de garanties appropriées et d'une surveillance indépendante.

[*Traduction*]

À mon avis, certains éléments de ce projet de loi pourraient être améliorés par une surveillance indépendante qui renforcerait la protection de la vie privée. Voici un élément qui touche de près à mon rôle de commissaire. Ce projet de loi vise à mieux protéger nos cybersystèmes essentiels. Le CST est notre expert national en matière de cybersécurité. Grâce à ce projet de loi, il recevra des informations sur les cyberincidents.

D'après mon expérience en tant que commissaire — forte de plus de trois ans et de 45 décisions rendues —, pour que le CST puisse analyser et comprendre un cyberincident, il doit avoir accès à des informations sur cet incident. Comme vous l'ont dit d'autres témoins, il peut y avoir des situations où les informations obtenues sont uniquement de nature technique et où leur communication au CST ne soulève aucune préoccupation en matière de protection de la vie privée. Cependant, pour bien comprendre le cyberincident, le CST peut dans d'autres situations avoir besoin d'accéder à des informations — y compris des informations techniques — pour lesquelles les Canadiens ont des attentes raisonnables en matière de protection de la vie privée. J'ai vu de tels cas.

La technologie et les cybermenaces évoluent plus rapidement que les lois. Le projet de loi devrait offrir la souplesse nécessaire pour s'adapter en conséquence et permettre l'échange de ces renseignements avec une surveillance appropriée.

[*Français*]

Dans le système actuel, avant de recueillir ces informations, le CST doit obtenir une autorisation ministérielle ainsi qu'une approbation du commissaire. Le législateur avait choisi de mettre en œuvre ce processus en 2019, mais il ne l'a pas fait en 2025.

[*Traduction*]

Le mécanisme proposé consiste à adopter un règlement indiquant quels renseignements sur les cyberincidents doivent être communiqués au CST et comment ils doivent l'être. Comme vous le savez, il n'y a pas de surveillance indépendante de la réglementation. Une mesure de surveillance simple et efficace possible consisterait à exiger chaque année une autorisation ministérielle établissant un cadre sur la façon dont le CST utilise et diffuse l'information, qui ferait ensuite l'objet d'un examen et d'une approbation par le commissaire au renseignement.

[*Français*]

Une cybersécurité efficace est essentielle pour les Canadiens. Le CST doit avoir accès à l'information dont il a besoin pour mener à bien son travail, de même que la surveillance nécessaire pour permettre cet accès.

[*Traduction*]

J'appuie l'intention du projet de loi, mais je pense que des mesures de protection supplémentaires ciblées qui n'imposent pas de lourde charge administrative à nos agences renforceraient la confiance des Canadiens dans le fait que ces mesures destinées à les protéger ne portent pas elles-mêmes atteinte de manière inutile à leur vie privée.

[*Français*]

Le président: Monsieur Noël, il ne vous reste que quelques secondes.

L'hon. Simon Noël: Merci.

Le président: Je suis désolé de vous interrompre aussi brusquement. Je vous remercie de votre intervention.

Je donne maintenant la parole à M. Dufresne.

Philippe Dufresne (commissaire à la protection de la vie privée du Canada, Commissariats à l'information et à la protection de la vie privée au Canada): Merci, monsieur le président.

Je vous remercie de m'avoir invité à comparaître aujourd'hui afin de vous faire connaître mon point de vue sur les répercussions 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.

Je suis accompagné de Marc Chénier, sous-commissaire et avocat général principal.

Il ne fait aucun doute que nous continuons d'être confrontés à un contexte difficile de cybermenaces, dans lequel les conséquences des cyberincidents sont de plus en plus perturbatrices et généralisées.

[*Traduction*]

Les atteintes aux infrastructures essentielles, comme celle qui a touché Nova Scotia Power en mai dernier, sont particulièrement inquiétantes, car elles peuvent compromettre des systèmes et des services essentiels à la santé, à la sécurité et à la prospérité économique des Canadiens. De tels incidents peuvent donner lieu à un accès non autorisé à des renseignements personnels ou à leur divulgation, ce qui peut entraîner des répercussions importantes sur la vie privée et un risque réel de préjudice grave pour les personnes touchées.

Pour ces raisons, j'appuie l'objectif du projet de loi C-8 qui vise à protéger les systèmes et les services essentiels à la sécurité nationale ou à la sécurité publique contre les menaces et les faiblesses en matière de cybersécurité.

Comme dans le projet de loi C-26 avant lui, on reconnaît dans le projet de loi C-8 que des mesures doivent être prises pour protéger les infrastructures essentielles contre les cybermenaces, qui deviennent de plus en plus poussées et complexes. Cette démarche est nécessaire du point de vue de la sécurité et de la protection de la vie privée.

[*Français*]

Bien que des mesures de protection renforcées en matière de cybersécurité puissent contribuer à réduire la probabilité que des atteintes à la vie privée surviennent et portent à conséquence, il est essentiel de s'assurer que les nouveaux pouvoirs créés pour améliorer la cybersécurité prévoient les limites nécessaires et qu'ils n'ont pas de répercussions imprévues sur la protection de la vie privée.

Je suis heureux de constater que le projet de loi C-8 comprend les améliorations apportées à son prédécesseur, le projet de loi C-26, notamment des balises supplémentaires relatives aux pouvoirs d'adopter des décrets ou des arrêtés qui sont proposés et aux nouvelles obligations d'avis et de déclaration.

● (1145)

[*Traduction*]

Ces améliorations contribueront à atteindre un meilleur équilibre entre les objectifs du projet de loi en matière de cybersécurité et les droits et intérêts en matière de protection de la vie privée.

Toutefois, il subsiste certains risques pour la protection de la vie privée, notamment des seuils plus bas pour l'exercice de certains pouvoirs ayant des répercussions potentielles sur la vie privée; l'absence d'un mécanisme visant à garantir que le Commissariat soit avisé des atteintes graves à la cybersécurité qui ont une incidence sur la vie privée des Canadiennes et des Canadiens; et des exigences minimales insuffisantes en matière de protection de la vie privée pour l'échange de renseignements avec des gouvernements étrangers.

Pour mitiger ces risques et atteindre l'équilibre nécessaire entre la sécurité et la protection de la vie privée, je recommanderais, premièrement, que le projet de loi impose une norme uniforme selon laquelle la collecte, l'utilisation ou la communication de renseignements personnels doivent être à la fois nécessaires dans les circonstances pour réaliser les fins énoncées et proportionnelles aux avantages procurés.

Deuxièmement, je recommanderais que les ententes d'échange de renseignements conclus au titre de la loi prévoient des mesures minimales de protection de la vie privée afin de renforcer la gouvernance et la reddition de comptes et d'assurer une norme uniforme en la matière lorsque des renseignements sont échangés avec des pays étrangers.

Troisièmement, je recommanderais que les autorités gouvernementales compétentes — y compris le Centre de la sécurité des télécommunications, ou CST — soient tenues d'aviser le Commissariat lorsqu'elles sont informées d'incidents de cybersécurité qui entraînent une atteinte importante à la vie privée, afin que nous puissions collaborer et coordonner nos efforts pour protéger la vie privée des Canadiennes et des Canadiens.

[*Français*]

Bien que cela ne vise pas uniquement le projet de loi C-8, je tiens aussi à réitérer ma recommandation générale selon laquelle les institutions gouvernementales devraient légalement être tenues de réaliser des évaluations des facteurs relatifs à la vie privée et de consulter le Commissariat au sujet de tout nouveau programme ou de toute nouvelle initiative qui a des répercussions sur la vie privée des Canadiennes et des Canadiens.

Je vous remercie de m'avoir donné l'occasion de présenter mon point de vue sur ce projet de loi. C'est avec plaisir que je répondrai à vos questions.

Le président: Je vous remercie, monsieur Dufresne.

Nous en sommes maintenant à accorder la parole aux députés, en commençant par le M. Caputo pour six minutes.

[*Traduction*]

Frank Caputo: Merci beaucoup à tous les témoins.

Par où commencer? J'aimerais commencer par MM. Noël et Dufresne.

Vous avez tous les deux beaucoup parlé de ce qui ne se trouve pas dans ce projet de loi.

Je suis désolé. Je vais revenir en arrière avant d'oublier. Malheureusement, vous serez parmi nous pendant quelques minutes seulement aujourd'hui. Ce que je vous demanderais, si cela vous convient, c'est que, ce dont nous n'aurons pas le temps de parler, surtout... Vous nous avez donné des exemples détaillés d'enjeux sur lesquels la loi est muette. Dans les faits, il est vraiment question de deux enjeux ici: les aspects du projet de loi qui posent problème — les passages qu'il faudrait modifier — et ce qui est absent du projet de loi.

Cette liste existe peut-être déjà, mais il me serait exceptionnellement utile que vous énumériez ces aspects. Sinon, nous devrons passer en revue les transcriptions. Je ne sais pas si votre bureau a les ressources pour le faire. Je pense qu'il serait très utile que vous nous disiez: « À notre avis, le projet de loi doit inclure ceci et cela. » Cela nous aiderait énormément à l'étape de l'étude article par article et des amendements.

Je vous laisse y réfléchir.

Je vais me concentrer sur ce qui se trouve dans le projet de loi. Je vais accorder deux minutes à chacun d'entre vous. Veuillez nous renvoyer à des dispositions précises, si vous le pouvez, parce que vous avez parlé de généralités jusqu'à présent. Si un article en particulier vous déplaît, pouvez-vous le nommer et dire: « À mon avis, cet article pose problème parce que... »? Est-ce que je m'exprime clairement?

Monsieur Dufresne, voulez-vous utiliser les deux premières minutes? Nous passerons ensuite à M. Noël.

Philippe Dufresne: Bien sûr. Merci, monsieur Caputo.

J'ai souligné trois thèmes pour les recommandations: la nécessité et la proportionnalité; les ententes d'échange de renseignements et le contenu minimal à cet égard; et les pouvoirs entourant l'échange de renseignements.

Pour la nécessité et la proportionnalité, je vais commencer par les points positifs. Des amendements ont été apportés au pouvoir de prise de décret du ministre dans l'article de la Loi sur les télécommunications. Le paragraphe 15.1(2) proposé mentionne ce qui suit:

> La portée et la teneur des dispositions du décret sont raisonnables eu égard à la gravité de la menace, notamment d'ingérence, de manipulation, de perturbation ou de dégradation.

On n'utilise pas les mots « nécessité et proportionnalité, » mais la disposition répond à l'objectif parce qu'elle porte sur ce qu'on essaie de réaliser et sur la question de savoir si le décret serait proportionnel à l'objectif.

En revanche, si on examine les pouvoirs conférés au ministre de l'Industrie en vertu de l'article 15.4 proposé, ce dernier aurait la capacité d'obliger toute personne à fournir à lui-même ou à toute personne désignée « selon les modalités qu'il précise, les renseignements à l'égard desquels il a des motifs raisonnables de croire qu'ils sont pertinents. » Ici, on n'emploie pas le critère de nécessité et de proportionnalité, mais bien celui de pertinence, qui est différent.

Plus loin dans le projet de loi, il est question d'échanges de renseignements avec des gouvernements étrangers en fonction de la nécessité. Dans la partie du projet de loi qui porte sur la cybersécurité, il est question de la capacité d'émettre des directives à cet égard. Soit seule la nécessité est mentionnée, soit ni la nécessité ni la proportionnalité ne sont mentionnées.

Mon principal argument est le suivant: dans ces articles, il y a un précédent pour inclure une disposition de nécessité et de proportionnalité valable. C'est l'article proposé que j'ai cité. Fait intéressant: même dans le projet de loi sur la cybersécurité, au paragraphe 147(1) proposé, on retrouve l'exigence de produire un rapport annuel. À l'alinéa 147(2)f) du projet de loi proposé, on lit que le rapport devrait inclure « une explication de la nécessité des directives, de leur caractère proportionnel et raisonnable et de leur utilité. » Je pense que c'est un exemple qui démontre pourquoi cette proportionnalité est nécessaire. On reconnaît déjà que la proportionnalité devrait être expliquée dans le rapport; le pouvoir devrait aussi respecter le caractère proportionnel.

Dans les ententes d'échange de renseignements, nous devrions donc préciser les types de restrictions limitant la communication de renseignements avec d'autres pays.

● (1150)

Frank Caputo: Merci beaucoup. Si vous avez d'autres commentaires, veuillez nous les faire parvenir par écrit. Plus ils seront précis et concrets, plus ils seront utiles.

Monsieur Noël, nous vous écoutons.

L'hon. Simon Noël: Oui. Je serai précis.

Mes connaissances portent sur le CST. Je sais quels renseignements sont communiqués au CST pour qu'il puisse mener ses cyberactivités.

Où est le cadre? Regardez l'article 17 proposé dans la partie 2 du projet de loi. Rien n'y est stipulé. On dit qu'il y aura un jour une réglementation.

À l'heure actuelle, en vertu de la loi dont je suis responsable et qui régit le CST, lorsqu'un incident de cyberactivité survient, le ministre intervient et rend une décision. Il passe à l'action, puis on me communique la décision. Je l'approuve, je l'amende et je la modifie, puis les résultats sont communiqués.

Je veux aussi soulever ce point. J'ai entendu les fonctionnaires vous dire plus tôt cette semaine qu'il s'agit de renseignements techniques. Je conviens qu'il s'agit de renseignements techniques, mais je sais aussi que si l'on veut obtenir un résultat positif après un incident aussi grave, il faut examiner l'information. Je l'ai constaté dans toutes les cyberopérations auxquelles j'ai participé.

Vous me demandez s'il y a d'autres changements à apporter. Je n'entrerai pas dans les détails — je me limiterai à ce commentaire —, mais il est évident que les perquisitions et saisies sans mandat posent problème. Je vais laisser le soin à d'autres d'en parler.

[*Français*]

Le président: Merci, monsieur Noël.

[*Traduction*]

Frank Caputo: Merci.

L'hon. Simon Noël: Les renseignements personnels suscitent aussi des inquiétudes chez moi.

Frank Caputo: Si nous n'abordons pas ces points, veuillez envoyer vos commentaires au Comité par écrit. Je vous en serais très reconnaissant.

Merci.

Le président: C'est un commentaire pertinent, monsieur Caputo.

Je donne maintenant la parole à M. Ramsay.

Jacques Ramsay: Monsieur Stupak, votre témoignage est excellent. J'aimerais savoir si le projet de loi C-8 est une version canadienne d'un projet de loi similaire qui existe ailleurs. En ce qui concerne les points de référence, qu'y a-t-il dans le projet de loi C-8 qui n'est dans aucun texte de loi à l'étranger, et qu'y a-t-il dans des textes de loi à l'étranger qui ne se trouve pas dans le projet de loi C-8?

Pouvez-vous nous en dire plus à ce sujet, surtout par rapport à nos principaux partenaires?

Philip Stupak: En ce qui concerne les points de référence, l'une des premières choses que ferait le projet de loi C-8 — et je pense que c'est très judicieux — est de consolider certains pouvoirs du ministre. C'est important.

À l'heure actuelle, de nombreux pays sont dotés d'un régime épars pour définir la politique de cybersécurité et réagir aux incidents de cybersécurité. En confiant ces pouvoirs au ministre, la responsabilité est entre les mains d'une seule personne. Lorsque le poste de directeur national de la cybersécurité aux États-Unis a été créé, c'était à la demande de notre sénat. Le sénateur Angus King, du Maine, a déclaré dans une citation célèbre qu'il voulait ce poste parce qu'il voulait avoir « une seule gorge à étrangler. »

L'un des éléments importants du projet de loi C-8, c'est qu'il crée une uniformité chez un seul ministre. Bien entendu, d'autres ministres et d'autres ministères participeront à la mise en œuvre de ces mesures, mais il est important qu'une seule personne chapeaute tout cet enjeu.

Ce qui diffère quelque peu — du moins par rapport au système américain, et c'est ce dont je peux parler —, c'est la capacité d'ordonner à l'industrie de prendre certaines mesures. J'aurais aimé avoir cette possibilité. C'est sans contredit un pouvoir qui me faisait défaut pendant mon mandat à la Maison-Blanche. Je ne pouvais pas ordonner à l'industrie de prendre des mesures précises. Je pense que c'est utile, surtout en réaction à un cyberincident, alors que chaque minute compte. C'est un élément qui est absent de notre système, mais que vous avez ici, et je pense que c'est utile.

● (1155)

Jennifer Quaid: J'approuve entièrement les paroles de M. Stupak.

Comme je l'ai indiqué, ce qui ne figure pas dans le projet de loi, ce sont les dispositions qui protègent les personnes et les organisations contre des poursuites et qui sont présentes dans la version américaine de cette mesure législative. Ces dispositions ont joué un rôle essentiel, car elles ont permis aux organisations d'échanger des renseignements à cet égard — et on ne parle pas d'atteintes à la protection des renseignements personnels. Ces atteintes sont renvoyées à l'organisme de réglementation et aux autorités compétentes, comme il se doit et conformément à la législation. On parle ici de renseignements sur des activités qui ne constituent pas d'atteintes à la protection des renseignements personnels, mais qui restent néanmoins des attaques. Ces informations peuvent aider d'autres organisations à se défendre contre des attaques parfaitement identiques.

Pensez un instant à Scattered Spider. Nous en avons tous entendu parler dans les médias. Son succès tient au fait que nous n'échangeons pas de renseignements sur la manière dont il pénètre dans un système et sur ce qu'il fait par la suite. Si nous pouvions le faire, nous contribuerions à renforcer tous les moyens de défense.

Jacques Ramsay: J'aimerais que M. Stupak commente l'affirmation de l'honorable Simon Noël selon laquelle, il faut habituellement examiner le contenu, lorsqu'une cyberattaque technique survient. Que pensez-vous de cette affirmation?

Philip Stupak: Je ne crois pas que je souscrirais nécessairement à cette affirmation. Je pense que l'on peut souvent lutter contre ces cyberattaques, en trouvant la façon de les contrer, généralement à un niveau plus technique.

Nous avons mis en place des mesures de protection adéquates afin que ces pirates n'aient pas accès aux informations confidentielles qu'ils recherchent. Bien entendu — et je le dis avec tout le respect que je vous dois —, j'estime qu'il peut arriver qu'il soit nécessaire d'examiner le contenu. Cependant, je ne dirais pas que c'est toujours le cas. Nous communiquons fréquemment des TTP, c'est-à-dire des tactiques, des techniques et des procédures, pour lutter contre une attaque, et ces TTP ne concernent pas le contenu.

L'hon. Simon Noël: Pour répondre très brièvement à la question, je dirais que, d'après mon expérience, dans le cas d'au moins 12 cyberincidents survenus au Canada, il y a finalement eu intrusion dans le contenu, à tel point que ces intrusions ont été signalées aux organismes compétents. Je m'en tiendrai là.

C'est là mon expérience personnelle, en tant que Canadien qui se trouve dans une position très particulière. Je ne dis pas que ce contenu est mêlé à toutes les informations techniques communiquées, mais je soutiens que, dans des cas exceptionnels, le contenu est montré.

[*Français*]

Jacques Ramsay: Monsieur Noël, puisque nous parlons de ce sujet, les attaques auxquelles vous faites référence provenaient-elles de l'extérieur du pays et étaient-elles commises par d'autres nations?

L'hon. Simon Noël: Oui.

Le président: Merci, monsieur Ramsay.

Madame DeBellefeuille, vous avez maintenant la parole pour six minutes.

Claude DeBellefeuille: Merci beaucoup, monsieur le président.

Monsieur Dufresne, vous avez beaucoup parlé de l'article 15 en disant qu'il y a toute une prévision concernant les rapports, mais qu'il faudrait peut-être mieux encadrer les pouvoirs du ministre et faire la corrélation entre les pouvoirs. J'aimerais parler de l'article 34, dont le titre est « Ordre ». On met de côté l'article 15, mais l'article 34 donne beaucoup de pouvoirs au surintendant, qui peut ordonner par écrit ce qu'il veut à un exploitant. Vous n'avez pas parlé de cet article, mais il m'inquiète.

Dans une certaine partie du projet de loi, on prévoit tout un processus de transparence, mais je vais vous donner un exemple extrême de ce que permettrait tout ce qui découle de l'article 34. Un surintendant pourrait demander à un fournisseur de baisser son chiffrement. On pourrait ainsi avoir accès à des conversations de clients de différents fournisseurs sans rendre de comptes ni demander d'autorisation à quiconque. Personne ne le saurait.

Mon interprétation est-elle juste lorsque je dis que beaucoup de pouvoirs sont donnés, mais qu'il n'y a aucune reddition de comptes et qu'un citoyen ne dispose d'aucune façon de savoir que sa conversation a été lue et vue par les autorités?

● (1200)

Philippe Dufresne: Cet article vise précisément les pouvoirs du surintendant. Des articles visent la Banque du Canada et le ministre de l'Industrie. On parle de vérification réglementaire, de vérification des livres. Des textes réglementaires accordent ce type de pouvoir à des autorités en matière de vérification. Ce n'est pas l'objet de ma présence ici et cela ne fait pas partie de mes principales préoccupations.

Je soulignerai toutefois que ma troisième recommandation propose que ces organismes puissent partager les informations et notifier mon bureau lorsqu'il y a des cyberattaques et lorsqu'ils sont mis au courant d'informations qui pourraient toucher la vie privée des Canadiens et des Canadiennes. Je ne pense pas que ces enquêtes visent ce type d'information. Cependant, si c'est le cas, il faut que nous en soyons avisés.

Je veux revenir à la discussion qu'on a eue auparavant afin de savoir si cela touche les renseignements personnels ou non. Je pense que la loi reconnaît, en un sens, que ce peut être le cas parce qu'on parle des renseignements personnels. On les inclut dans les renseignements confidentiels.

Pour ce qui est de la question des comparables à l'international, en Europe, on demande aux institutions d'aviser les autorités de protection des données, ce qui est absent ici. Je pense donc qu'on pourrait faire mieux.

Claude DeBellefeuille: Par exemple, Microsoft est-elle considérée comme une entreprise offrant un service essentiel au gouvernement du Canada? Au fond, tout notre système d'exploitation relatif à Internet est géré par Microsoft. Dans le cadre du projet de loi C-8, Microsoft pourrait-elle recevoir un ordre du surintendant des institutions financières et s'y soumettre?

Philippe Dufresne: Les systèmes critiques sont indiqués à l'annexe 1 du projet de loi. Ce sont les services de télécommunication, les systèmes de pipelines, les systèmes d'énergie nucléaire, les systèmes de transport, les systèmes bancaires et les systèmes de compensations. La question se poserait sur ce plan. Compte tenu de la nature de ses activités, Microsoft fait-elle partie des services de télécommunications ou non? Il faudrait examiner les activités concernées. À partir du moment où on tombe sous cette catégorie, il est possible d'émettre des ordonnances pour assurer la cybersécurité.

Selon moi, on devrait renforcer ce critère pour qu'il y ait une proportionnalité relative aux renseignements personnels ainsi qu'une notification envoyée à mon bureau. Mon point de vue vient un peu renforcer les commentaires du juge Noël. Il faut une vérification indépendante, car ça augmente la confiance des Canadiens.

La loi permet aussi d'échanger des renseignements à l'étranger, alors c'est bien que la loi exige une entente écrite. C'est une amélioration, mais on pourrait aller plus loin. Il y a un exemple dans le projet de loi C-12, dans lequel une disposition type permet d'exiger davantage pour la conclusion des ententes internationales. Il y a un minimum d'exigences sur la portée de ce qu'on peut faire.

On pourrait ajouter ces éléments, ce qui renforcerait la confiance.

Claude DeBellefeuille: Merci.

Monsieur Dufresne, je voudrais vous poser un peu plus de questions sur le sujet dont M. Caputo vous a parlé.

Les éléments que vous nous apportez sont très pertinents, d'autant plus qu'ils établissent un lien avec le projet de loi C-12, que nous devons étudier.

Vous pourriez nous donner des exemples de dispositions du projet de loi que nous pourrions améliorer pour protéger la vie privée. Selon moi, la démocratie est basée sur la protection de la vie privée, et le modèle des États-Unis n'en est pas un qui m'inspire. Cette protection est importante pour nous. Encore une fois, je crois que nous avons la chance d'améliorer l'ancien projet de loi C-26 pour le rendre encore plus moderne et assurer aux Québécois et aux Canadiens une meilleure protection de leurs renseignements personnels.

Je lis souvent des enquêtes de l'agence qui cherche à déterminer si les agences sont conformes quant à l'utilisation des renseignements personnels, et je me rends compte qu'elles commettent plusieurs infractions. Ainsi, le projet de loi C-8 doit se rapprocher de la perfection.

Nous allons donc profiter de vos propositions afin d'améliorer concrètement le projet de loi en les intégrant comme amendements.

● (1205)

Philippe Dufresne: Je vais vous faire mes propositions avec plaisir.

Sur le plan international, je veux parler du Royaume-Uni, qui est un pays appartenant au Groupe des cinq. Les Britanniques exigent un élément de nécessité, de pertinence et de proportionnalité. Ils ont donc créé un précédent dans ce domaine.

Claude DeBellefeuille: Je vous remercie.

Le président: Je vous remercie beaucoup de ce bel échange.

Monsieur Lloyd, vous disposez de cinq minutes.

[*Traduction*]

Dane Lloyd (Parkland, PCC): Merci.

Je vais commencer par interroger M. Dufresne.

Allez-vous fournir au Comité les amendements que vous recommandez pour répondre aux préoccupations que vous avez exposées aujourd'hui?

Philippe Dufresne: Cela a été demandé au cours des échanges, alors nous vous communiquerons les détails ultérieurement.

Dane Lloyd: Merci.

Vous avez été légiste parlementaire et avocat pendant plusieurs années, n'est-ce pas?

Philippe Dufresne: Oui.

Dane Lloyd: Vous avez également siégé à la Commission des droits de la personne en tant que conseiller juridique?

Philippe Dufresne: C'est exact.

Dane Lloyd: Comme cela a duré de nombreuses années, on peut dire que vous avez beaucoup d'expérience dans ce domaine.

Nous avons eu l'occasion d'interroger le ministère au sujet des pouvoirs conférés au ministre à l'article 15 proposé, en particulier le pouvoir d'obliger les entreprises de télécommunications à retirer leurs services à une personne donnée. Le ministère nous a assuré que le champ d'application de la loi ne concernait pas la liberté d'expression ni les contenus qui ne constituent pas une menace pour l'intégrité du système de télécommunications.

Pensez-vous que la portée et l'exigence concernant le caractère raisonnable de cette mesure législative sont assez claires pour limiter les possibilités d'utiliser ces pouvoirs législatifs de façon abusive?

Philippe Dufresne: En ce qui concerne l'article auquel vous faites allusion, qui porte sur le pouvoir de rendre des ordonnances en vertu de la Loi sur les télécommunications, je dirais qu'un ajout a été apporté au paragraphe 15.2(3) proposé afin d'exiger que sa portée et sa teneur soient « raisonnables eu égard à la gravité de la menace, notamment d'ingérence, de manipulation, de perturbation ou de dégradation ».

Je pense que cette disposition n'utilise pas les termes « nécessité et proportionnalité », mais elle reflète ce sens de l'équilibre, et je considère donc qu'elle atteint mon objectif, qui est de garantir votre sécurité et votre vie privée. Il faut trouver un juste équilibre, et nous ne voulons pas d'un jeu à somme nulle, où l'on va trop loin en limitant le pouvoir de l'organisme de protéger les Canadiens, où l'on va trop loin en portant atteinte à la vie privée des Canadiens. Je suis satisfait de cet article.

Ce sont les autres articles qui m'inquiètent, en ce qui concerne certains des autres pouvoirs qu'ils confèrent. Dans ces articles, on ne parle que de nécessité ou de pertinence, et je voudrais qu'elles soient renforcées afin d'introduire la notion clé de proportionnalité.

Dane Lloyd: Pourriez-vous développer davantage ce dont vous venez de parler, c'est-à-dire les articles que vous voudriez voir renforcés?

Philippe Dufresne: Lorsque nous examinons les notions de nécessité et de proportionnalité dans mon bureau, nous appliquons un critère semblable à celui prévu dans la Charte des droits et libertés. Ce critère permet de trouver un équilibre entre les droits fondamentaux et les impératifs importants de l'intérêt public. Vous devez vous poser les questions suivantes: quel est votre but? Quel est votre objectif? Est-il suffisamment important? Quelle est votre mesure? Votre mesure est-elle efficace?

Dane Lloyd: Pourriez-vous préciser les mesures contenues dans le projet de loi dont vous parlez?

Philippe Dufresne: Dans ce contexte, nous avons le pouvoir de demander à une organisation de ne pas faire appel à un certain fournisseur. Une entreprise particulière liée à un pays particulier peut poser un problème de sécurité nationale. Dans ce cas, vous allez examiner les mesures que vous mettez en place. Allez-vous trop loin? Faites-vous quelque chose qui va trop loin par rapport à la menace?

Si vous affrontez une menace majeure, vous pourrez prendre des mesures plus rigoureuses. Si la menace est plus faible, plus contenue, vous devez vous assurer de ne pas causer des dommages collatéraux.

Dane Lloyd: Vous ne croyez pas que cette proportionnalité ait été prise en compte.

Philippe Dufresne: Je pense que cette notion de proportionnalité a été intégrée dans l'article qui porte sur le pouvoir de prendre des ordonnances, mais je ne crois pas qu'elle ait été intégrée ailleurs, en ce qui concerne les exigences en matière d'information ou le domaine cybernétique.

Dane Lloyd: D'accord. Je vous remercie.

Je vais maintenant me tourner vers le commissaire au renseignement.

Vous avez soulevé des questions très intéressantes au sujet des perquisitions et des saisies sans mandat, et vous avez parlé du contenu. Je sais que le ministère s'est donné beaucoup de mal pour nous assurer qu'il ne s'intéresse pas vraiment au contenu qui est acheminé par les réseaux, mais plutôt à la question de savoir si une action constitue ou non une menace pour les réseaux eux-mêmes.

Pourriez-vous nous en dire davantage à propos de vos préoccupations concernant les perquisitions et les saisies sans mandat, ainsi que le contenu? Pourriez-vous nous donner plus de précisions à ce sujet?

L'hon. Simon Noël: Les perquisitions et les saisies sans mandat relèvent clairement de l'article 8 de la Charte. C'est une évidence pour tout juge. Cela ressort d'autant plus clairement que des sanctions ont été prévues à cet effet dans la loi. Cela soulève d'autres questions, et c'est la Cour suprême qui le dit.

Si vous examinez le contenu actuel du projet de loi, vous constatez que vous n'avez rien.

● (1210)

Dane Lloyd: Pouvez-vous donner un exemple de situation dans laquelle ce droit prévu à l'article 8 pourrait être invoqué en vertu de cette mesure législative? Pouvez-vous nous fournir un exemple précis?

L'hon. Simon Noël: Dans toute perquisition et saisie, si des agents pénètrent sans mandat dans un bureau, ouvrent des portes et commencent à fouiller les lieux, il est évident qu'il s'agit d'une intrusion.

Il y a deux façons d'entrer dans un bureau. La première consiste à entrer et à dire: « Pourriez-vous me donner les documents suivants? » L'autre façon consiste à...

Dane Lloyd: Vous ne croyez pas que ces mesures de protection sont...

L'hon. Simon Noël: ... dire que vous intervenez parce que vous voulez récupérer tel ou tel document. En général, les forces de police ont besoin de...

Dane Lloyd: N'ont-ils pas d'autres outils législatifs au Canada pour le faire de toute façon?

L'hon. Simon Noël: Le Code criminel contient certes certaines dispositions à ce sujet, mais si vous consultez le Code criminel, vous constaterez qu'un mandat sera nécessaire.

[*Français*]

Le président: Merci, monsieur Noël et madame Lloyd.

Madame Acan, vous avez la parole.

Sima Acan (Oakville-Ouest, Lib.): Merci, monsieur le président.

Je partagerai le temps dont je dispose avec Mme Dandurand s'il en reste à la fin.

[*Traduction*]

Je vous remercie d'être venus aujourd'hui.

Ma question sera destinée à M. Stupak.

Je vous remercie d'avoir témoigné et d'avoir souligné l'importance du projet de loi.

Je partage votre point de vue concernant les conséquences d'une cyberattaque contre nos infrastructures d'un point de vue financier et sécuritaire. En vertu du projet de loi C-8, des exploitants désignés seront tenus d'adopter des programmes cybernétiques complets et de signaler les incidents qui sont essentiels pour établir des mesures de protection de base.

Vous avez exprimé votre soutien sans faille au projet de loi C-8. Compte tenu de votre expérience et de votre connaissance approfondie des lois semblables qui sont en vigueur en Europe ou dans les pays membres du groupe des cinq, en particulier aux États-Unis, vous avez pu constater ce qui fonctionne et ce qui ne fonctionne pas en matière de politique fédérale et de développement du milieu de travail.

Je voudrais poser deux questions pour mettre l'accent sur la capacité de mise en œuvre et les normes professionnelles. Premièrement, dans quelle mesure le personnel actuellement responsable de la cybersécurité au Canada est-il prêt à répondre aux exigences techniques et de conformité prévues par le projet de loi C-8?

Deuxièmement, d'un point de vue international, dans quelle mesure le projet de loi C-8 coïncide-t-il avec les cadres similaires adoptés dans des pays alliés, et dans quels secteurs le Canada devrait-il donner la priorité à l'harmonisation afin de réduire les problèmes de conformité pour les entreprises internationales?

Philip Stupak: Je vous remercie d'avoir posé ces deux questions, car elles sont extrêmement pertinentes.

En ce qui concerne la main-d'œuvre, le Canada dispose d'une main-d'œuvre très solide. Vous disposez d'une main-d'œuvre impressionnante qui possède les outils et les capacités nécessaires pour mettre en œuvre le projet de loi C-8.

Je vais être honnête. Nous avons tous besoin de davantage de ressources. Nous avons besoin d'un plus grand nombre de professionnels dans ce domaine. Nous avons besoin d'un plus grand nombre de travailleurs qui détiennent des certifications qui attestent qu'ils ont les compétences nécessaires pour accomplir le travail qui doit être fait. C'est important. Trop souvent, nous mettons l'accent sur l'éducation et sur la question de savoir si une personne est titulaire ou non du diplôme nécessaire, mais ce que nous recherchons vraiment, ce sont les compétences nécessaires pour accomplir ce travail.

Des efforts sont actuellement déployés dans le cadre de la National Initiative for Cybersecurity Education, ou NICE, par exemple pour définir les fonctions que chaque rôle dans le domaine de la cybersécurité devrait remplir, puis la manière dont ces fonctions peuvent être remplies. Ce travail est en cours. Je pense que ces efforts ne sont pas encore suffisamment énergiques au niveau transfrontalier, mais l'important, c'est que vous ayez la capacité de commencer à mettre en œuvre ces mesures. Vous allez devoir renforcer l'éducation, renforcer la formation et renforcer la certification.

En ce qui concerne les cadres internationaux, comme vous adoptez une approche sectorielle et que cette approche vise un secteur particulier, je pense que vous êtes tout à fait en phase avec les États-Unis et la manière dont nous avons toujours procédé, c'est-à-dire en examinant chaque secteur et ce qui doit être fait au sein de ce secteur. Tous les secteurs ne sont pas égaux. Pour parler franchement, dans mon pays, le secteur de l'eau n'est pas au même niveau que celui des services financiers. Vous devez adopter cette approche, car tout le monde n'est pas prêt à faire la même chose au même moment.

Je comparerais cela aussi aux normes de la directive NIS2 de l'Union européenne. Je ne recommanderais pas que vous procédiez de cette façon, car cette approche est beaucoup plus axée sur la vérification, et il est impossible de vérifier toutes les infrastructures critiques aussi souvent que nécessaire. De plus, le régime de conformité n'est tout simplement pas encore assez mûr ou robuste pour respecter la directive NIS2.

J'aime le fait que le projet de loi adopte une approche plus sectorielle, qui s'apparente davantage à celle des États-Unis et un peu moins à celle de l'Union européenne.

Sima Acan: Je vous remercie.

[*Français*]

Marianne Dandurand (Compton—Stanstead, Lib.): Monsieur le président, je remercie ma collègue de partager son temps de parole avec moi.

Nous avons entendu des commentaires très intéressants de la part des commissaires.

Monsieur Stupak et madame Quaid, quel genre d'information est habituellement échangé?

À quoi ressemblent les indicateurs de compromission et en quoi diffèrent-ils des données typiques?

● (1215)

[*Traduction*]

Jennifer Quaid: Les informations partagées dans le cadre du projet de loi seraient celles provenant d'une cyberattaque réussie, d'une atteinte à la protection de renseignements personnels, si vous préférez, une cyberattaque qui a eu des répercussions sur des renseignements d'identification d'une personne ou qui a entraîné la fuite, le vol ou la destruction d'autres informations. Il est essentiel que le gouvernement soit au courant de ces incidents et que ces cyberattaques soient signalées, car nous ne connaîtrons pas réellement l'ampleur du problème à moins qu'elles ne soient signalées.

L'information à laquelle je faisais allusion va au-delà de cela. Je m'intéresse aux informations concernant des attaques qui n'ont peut-être pas été aussi fructueuses. Il s'agit de renseignements liés à des situations où des organisations ont été touchées par des cyberattaques, mais il n'y a pas eu d'atteintes à la protection des renseignements personnels. Leurs moyens de défense ont tenu le coup, si vous voulez. Leurs moyens de défense extérieure ont échoué, mais leurs moyens de défense intérieure ont tenu bon. Ce sont ces informations qu'il est important de partager avec la communauté au sens large.

Les dispositions qui protègent les personnes et les organisations contre des poursuites ne devraient jamais se limiter au partage d'informations avec les mêmes organismes de réglementation et les mêmes représentants gouvernementaux que ceux visés par le projet de loi. Ces dispositions doivent protéger les personnes et les organisations lorsqu'elles partagent des informations avec la communauté au sens large.

Je vais vous donner très rapidement un exemple...

Le président: En quelques secondes, madame Quaid.

Jennifer Quaid: ... en une seconde. L'un de nos membres très importants me dit souvent qu'il peut partager des renseignements cybernétiques, comme des tactiques, des techniques et des procédures, ou TTP, ou des indicateurs de compromission, ou IC, avec le Financial Services Information Sharing and Analysis Center, ou FS-ISAC, aux États-Unis, qui est une association de partage d'informations pour les services financiers, mais qu'il ne peut pas communiquer ces renseignements au Canada parce qu'il n'est pas protégé dans ce pays, ce qui est frustrant.

Le président: Je vous remercie, madame Quaid.

Marianne Dandurand: J'aurais aimé entendre l'opinion de M. Stupak à ce sujet...

Le président: Je suis désolé de vous interrompre, madame Dandurand.

Il reste deux minutes et demie pour l'intervention de Mme DeBellefeuille. Ensuite, ce sera malheureusement la fin de cette partie de la réunion.

[*Français*]

Claude DeBellefeuille: Merci beaucoup, monsieur le président.

Monsieur Noël, on le sent, il y a beaucoup de pression de la part de la GRC et du Service canadien du renseignement de sécurité, ou SCRS, pour avoir accès plus facilement à l'information, aux renseignements. Comme on le dit, il faut trouver l'équilibre entre la sécurité, l'intervention pour protéger et la protection de la vie personnelle.

Pour ma part, je sens beaucoup de pression pour emprunter une direction qui, pour nous, les élus, est un peu insécurisante. Va-t-on perdre confiance en nos institutions, qui ne nous rendent plus de comptes ou ne le veulent pas, ou aimeraient idéalement être tenues au moins de transparence possible? À cet égard, elles plaident que si on en donne trop, on prête flanc au manque de sécurité et on ouvre la porte aux puissances extérieures qui ne veulent pas nécessairement notre bien.

Trouvez-vous normal que, au Comité, on puisse recevoir l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, parce que c'est à lui qu'il revient de surveiller si les agences se conforment à la loi? Si on donne plus de pouvoirs aux ministres ou aux surintendants sans qu'ils aient de comptes à rendre, l'Office ne pourra pas faire son travail, car tout sera opaque.

Quelle est votre position sur cette pression qu'on sent actuellement pour élargir et restreindre, à la fois la transparence?

L'hon. Simon Noël: Je sympathise avec vous pour ce que vous exprimez.

Nous vivons de toute évidence dans un monde où les cyberattaques sont devenues les nouveaux outils de guerre. Quand on regarde les mauvais acteurs — il peut s'agir d'un pays ou de quelqu'un qui demande une rançon, par exemple —, on constate qu'ils ont des outils extraordinaires pour pouvoir percer nos protections et accéder à ce à quoi ils le veulent bien.

Si vous voulez bien protéger les électeurs de votre circonscription, vous devez donner au gouvernement et à la police les mêmes outils pour leur permettre de combattre ces mauvais acteurs.

Cela étant dit, votre défi est de trouver les mesures qui prendront en considération votre préoccupation en tant que députée, la vie privée des gens et de l'autre côté, la sécurité nationale.

● (1220)

Le président: Je suis désolé, monsieur Noël, c'est tout le temps que nous avons.

L'hon. Simon Noël: J'arrête là, mais je pense avoir tout dit.

Je vous remercie.

Le président: Nous vous sommes très reconnaissants du temps que vous nous avez consacré aujourd'hui, mais surtout des efforts que vous avez mis afin de vous préparer à cette rencontre. Nous vous saluons et vous remercions.

Nous allons passer à notre autre groupe d'invités. Je suspends donc la séance pour quelque temps. Vous pouvez vous dépêcher d'aller chercher de la nourriture, si vous voulez, avant l'arrivée des autres invités.

● (1220)

_____(Pause)_____

● (1225)

Le président: Nous reprenons la séance puisque nous avons le quorum.

Je souhaite la bienvenue à quatre témoins importants.

Nous recevons Josh Dehaas, conseiller à la Canadian Constitution Foundation; Aaron Shull, directeur général et avocat général du Centre for International Governance Innovation; Luc Lefebvre, président et cofondateur de Crypto Québec, qui se joint à nous par vidéoconférence; et Sharon Polsky, présidente du Conseil du Canada de l'accès et la vie privée.

Vous êtes tous les quatre les bienvenus. Vous disposez de cinq minutes pour faire vos présentations.

Monsieur Dehaas, vous avez la parole.

[*Traduction*]

Josh Dehaas (conseiller, Canadian Constitution Foundation): Merci, monsieur le président.

Je m'appelle Josh Dehaas. Je suis avocat auprès de la Canadian Constitution Foundation, ou CFF. La CCF est un organisme de bienfaisance non partisan qui se consacre à la défense des droits et libertés des Canadiens au moyen de l'éducation, de la communication et des litiges. La CCF est surtout connue pour avoir contesté avec succès l'invocation de la Loi sur les mesures d'urgence en février 2022. La Cour fédérale a estimé que cette invocation était ultra vires et violait le droit à la liberté d'expression ainsi que la protection contre des fouilles ou des saisies abusives.

La CCF est très préoccupée par un aspect particulier du projet de loi C-8. L'article 15.2 proposé permettrait au gouvernement d'imposer des restrictions inconstitutionnelles à la liberté d'expression, à la liberté de réunion et à la liberté d'association. Le paragraphe 15.2(1) proposé conférerait au ministre de l'Industrie un nouveau pouvoir dangereux qui lui permettrait d'ordonner à des fournisseurs de services de télécommunications de couper l'accès à Internet ou à des services téléphoniques à des particuliers face à « toute menace » pesant sur le système de télécommunication, qui comprend toutes les infrastructures Internet, téléphoniques et radiophoniques du Canada. Il ne serait pas nécessaire que cette menace soit systémique ou même grave.

Les paragraphes 15.2(5) et 15.2(8) proposés permettraient de garder secrets les détails des ordonnances du ministre sous peine d'amendes colossales. Même s'il peut y avoir des circonstances où le ministre a besoin du pouvoir d'ordonner la coupure de serveurs malveillants du système, il est dangereux pour les libertés civiles de permettre au ministre de couper l'accès à Internet à des Canadiens sans application régulière de la loi et de garder ces ordonnances secrètes.

Prenons l'exemple d'un manifestant dont le ministre soupçonne qu'il pourrait se livrer à une attaque par déni de service distribué, une forme courante de désobéissance civile utilisée par les militants politiques. En vertu de l'article 15.2 proposé, le ministre pourrait ordonner la coupure des services Internet et téléphoniques de ce dissident et exiger que cette décision demeure secrète. Le seul recours de cette personne serait d'engager un avocat à grands frais pour contester l'ordonnance du ministre. Cette décision resterait en vigueur jusqu'à ce qu'un tribunal examine l'affaire et ordonne le rétablissement des services. La personne concernée pourrait même ignorer qu'elle a droit à une révision judiciaire de la décision, car la loi n'exige pas qu'elle soit informée de son droit de contester cette décision devant les tribunaux.

Pour être clair, les attaques par déni de service distribué constituent de réels risques pour la cybersécurité. Elles constituent une infraction pénale. Cependant, toute personne simplement soupçonnée de vouloir participer à une telle forme de désobéissance civile pourrait être réduite au silence. Sans Internet ni téléphone, elle serait effectivement privée de toute expression en ligne, et on l'empêcherait d'exercer des activités politiques protégées par la Constitution, comme le fait d'exprimer son opposition à une politique ou de rencontrer d'autres personnes en ligne, ce qui constituerait une violation de la liberté d'expression, de la liberté de réunion et de la liberté d'association.

Bien que cette loi semble être une tentative de bonne foi de prévenir ou d'endiguer les cyberattaques, elle ne comprend pas de mesures de protection adéquates pour empêcher les abus. Les lois adoptées de bonne foi sont souvent utilisées pour violer les droits des citoyens, en particulier pendant des périodes d'agitation politique et sociale. Par exemple, le gouvernement fédéral a ordonné aux institutions financières de geler des centaines de comptes bancaires, sans application régulière de la loi, lors de l'invocation de la Loi sur les mesures d'urgence. Cela a empêché certains manifestants et leurs conjoints de payer leurs factures au beau milieu d'un hiver très rigoureux et a violé leurs droits en vertu de l'article 8 de la Charte. Le gouvernement a également utilisé cette loi pour empêcher les manifestants de se tenir simplement sur la Colline du Parlement avec un drapeau canadien ou une pancarte d'opposition à la vaccination obligatoire, violant ainsi leur droit à la liberté d'expression.

En d'autres termes, nous ne pouvons pas simplement faire confiance aux gouvernements lorsqu'ils détiennent ce genre de pouvoir. Le projet de loi doit comporter de meilleures mesures de protection contre de tels abus.

La CCF propose cinq amendements qui réduiraient ce risque de violation des libertés civiles.

Premièrement, la CCF propose que le paragraphe 15.2(1) proposé soit modifié afin de préciser que le pouvoir de suspendre des services ne peut être exercé qu'en cas de risques systémiques graves.

Deuxièmement, la CCF propose que la loi stipule explicitement qu'il est possible d'obtenir une révision judiciaire de l'ordonnance et que les services peuvent être rétablis immédiatement par un juge.

Troisièmement, la CCF propose que la loi limite le caractère secret de toute ordonnance en exigeant qu'elle soit publiée dans la *Gazette du Canada* dans les 90 jours qui suivent, à moins que le ministre n'obtienne une ordonnance de la Cour fédérale interdisant la divulgation d'une partie ou de la totalité de son contenu.

Quatrièmement, la CCF propose que ces ordonnances ne puissent être gardées secrètes que si un juge de la Cour fédérale estime qu'il existe des motifs raisonnables de croire que la divulgation d'une partie ou de la totalité de l'ordonnance porterait atteinte aux relations internationales, à la défense nationale ou à la sécurité nationale, ou mettrait en danger la sécurité d'une personne.

Enfin, la CCF propose que, lorsque le juge estime qu'il est nécessaire d'assurer l'équité de la procédure pour une personne touchée par une telle décision, il puisse nommer un amicus curiae pour aider cette personne.

● (1230)

Je vous remercie d'avoir pris le temps de m'écouter. C'est avec plaisir que je répondrai à toutes vos questions.

[*Français*]

Le président: Merci, monsieur Dehaas.

Monsieur Shull, vous avez la parole pour cinq minutes.

[*Traduction*]

Aaron Shull (directeur général et avocat général, Centre for International Governance Innovation): Merci, monsieur le président. Je remercie également les membres du Comité.

Je vais faire deux choses aujourd'hui. Je vais passer en revue certains articles particuliers du projet de loi qui, selon moi, méritent d'être examinés plus en détail et qui pourraient être modifiés. Ensuite, je parlerai d'un outil politique pratique visant à encourager la conformité. Je vais proposer un crédit d'impôt à l'investissement dans le domaine de la cybersécurité pour les entreprises canadiennes. Nous vivons actuellement un moment d'édification du pays unique dans l'histoire de notre pays, et je pense qu'un crédit d'impôt est la solution à adopter.

Les collègues qui m'ont précédé ont fait du bon travail, mais je voudrais revenir sur quelques points.

Les paragraphes 15.1(3) et 15.2(5) proposés sont des dispositions relatives à non-divulgation qui permettent au gouverneur en conseil ou au ministre d'imposer le secret autour des ordonnances, sans qu'aucun critère d'orientation ne soit appliqué. C'est le point sur lequel je souhaite revenir. Le secret doit être l'exception, et non la règle. Je pense que vous devriez imposer des critères prévus par la loi qui doivent être pris en compte avant de déterminer s'il convient ou non de rendre une ordonnance secrète.

S'il n'en tenait qu'à moi, je proposerais les critères suivants: la mesure dans laquelle la divulgation pourrait raisonnablement compromettre l'efficacité de l'ordonnance ou mettre en péril la sécurité nationale; la disponibilité de moyens moins restrictifs, y compris la publication partielle ou différée de l'ordonnance, pour atteindre le même objectif; l'incidence de la non-divulgation sur la transparence et la responsabilité des décisions gouvernementales; la nécessité de la non-divulgation compte tenu de l'urgence, de la nature et de la durée de la menace; et toute déclaration faite par les fournisseurs de services de télécommunications ou les organismes de réglementation concernés concernant la nécessité de la confidentialité.

Je n'ai rien contre le secret, et je comprends qu'il soit nécessaire dans ce cas-ci. Je dis simplement qu'il faut établir certains critères pour orienter la prise de ces décisions. Le projet de loi prévoit des critères pour la prise de décisions dans d'autres domaines, mais pas en ce qui concerne la non-divulgation.

Ensuite, je voudrais parler du paragraphe 15.1(8) proposé et du paragraphe 15.2(10) proposé, et je m'excuse d'entrer autant dans les détails. Je suis avocat, alors cela fait partie des risques de ma profession.

Dans le cas présent, la Couronne n'assumerait aucune responsabilité financière découlant d'une ordonnance. Je pense que c'est raisonnable, mais cela nous poserait un petit problème. Le fait de combiner les règles de non-indemnisation et les règles de non-divulgation nous conduirait à une situation où les sociétés cotées en bourse pourraient contrevenir aux lois sur les valeurs mobilières. Elles pourraient subir un changement important dans leurs livres comptables. Supposons qu'un fournisseur de services de télécommunications reçoive une ordonnance de retrait et de remplacement d'une valeur de 25 millions de dollars. Il ne pourrait pas divulguer cette information à ses actionnaires si l'ordonnance était secrète. À ce moment précis, il manquerait à une obligation fiduciaire et contreviendrait à la réglementation sur les valeurs mobilières. C'est un aspect du problème dont nous devrions tenir compte.

Il existe des moyens de remédier à cette situation. Je propose que la réglementation autorise le recouvrement des coûts dans des circonstances particulières et exceptionnelles. Vous devriez également créer un mécanisme de divulgation sécurisée pour les entreprises concernées afin qu'elles puissent communiquer ces informations à leurs organismes de réglementation et à leurs vérificateurs dans des conditions qui respectent les mesures de protection relatives aux informations classifiées.

Quelqu'un a parlé tout à l'heure des dispositions qui protègent les personnes et les organisations contre des poursuites. Je voudrais parler d'autres dispositions de protection, car si le projet de loi est adopté dans sa forme actuelle, il pourrait fonctionner comme... Nous avons besoin d'une forme limitée de protection juridique pour les dirigeants et les administrateurs de sociétés qui se conforment de bonne foi au projet de loi C-8, mais qui sont ensuite exposés à des poursuites en vertu des lois sur les valeurs mobilières. Nous devons nous assurer qu'ils peuvent le faire en toute sécurité, sans se faire face à un dilemme juridique très prononcé, qui ne leur permet pas de respecter simultanément leurs deux obligations.

Dans le paragraphe 15.21(1) proposé et le paragraphe 15.81(1) proposé, il y a un dédoublement en matière de rapport. Les deux paragraphes proposés exigeraient que le ministre fasse rapport au Parlement trois mois après la publication du rapport annuel. Je pense qu'il s'agit simplement d'une erreur de rédaction. Vous pourriez facilement la corriger, car les deux dispositions font la même chose.

Plus problématique encore, l'article 15.4 proposé prévoit l'obligation de fournir des renseignements. Il permettrait au ministre d'exiger de toute personne qu'elle fournisse des renseignements. Cet article n'a aucune importance du point de vue de la conformité, mais vous allez vous heurter à des contestations en vertu des articles 7 et 11(c) de la Charte si les renseignements sont utilisés pour intenter des poursuites judiciaires plus tard. Vous devriez ajouter un article qui porte explicitement sur l'immunité et qui est inspiré de la Loi sur la concurrence. Cela garantirait que les renseignements ne sont utilisés qu'à des fins réglementaires, et non pour intenter des poursuites criminelles. Cela préserverait votre confidentialité sans affaiblir l'application de la loi. Cet article figure dans la Loi sur la concurrence.

En ce qui concerne l'article 15.9 proposé et le contrôle judiciaire, il y a également un problème. Le juge serait forcé de restituer toute information non pertinente fournie par le ministre. Cela pose un problème, car lorsqu'un juge examine une affaire dans le cadre d'un contrôle judiciaire, il vérifie si tous les renseignements sur lesquels s'est appuyé le ministre sont pertinents. Les juges pourraient se retrouver dans une situation délicate, où ils ne seraient pas autorisés à examiner tous les documents dont ils ont besoin pour déterminer la pertinence. C'est un aspect qu'il convient d'examiner. C'est un peu comme si on envoyait un joueur de hockey sur la glace avec un seul patin et pas de bâton. Il faut s'assurer que le juge dispose de tous les renseignements dont il a besoin, et je pense qu'un simple amendement pourrait résoudre ce problème.

● (1235)

Passons maintenant à l'article 142 proposé dans le cadre de la Loi sur la protection des cybersystèmes essentiels et au paragraphe 73(3.3) proposé dans le cadre de la Loi sur les télécommunications. Je ne sais pas si cela a été fait intentionnellement, mais en vertu de la Loi sur les télécommunications, l'entreprise n'est responsable que si l'employé qui a commis l'infraction agissait dans les limites de ses fonctions ou de ses pouvoirs, alors qu'en vertu de la Loi sur la protection des cybersystèmes essentiels, cette condition n'existe pas. Cela signifie que deux entreprises pourraient être assujetties à des normes de responsabilité différentes. Je pense que cette incohérence mérite également d'être réexaminée.

Je vous remercie de votre attention.

[*Français*]

Le président: Merci, monsieur Shull.

Monsieur Lefebvre, vous disposez aussi de cinq minutes.

Luc Lefebvre (président et cofondateur, Crypto Québec): Monsieur le président, membres du Comité, je me présente devant vous aujourd'hui en tant que président et cofondateur de Crypto Québec, un organisme à but non lucratif et une entreprise d'économie sociale qui promeut les meilleures pratiques et qui synthétise les enjeux en matière de sécurité de l'information, de renseignement et de géopolitique.

Je vous remercie de m'accueillir à titre de témoin dans le cadre de l'étude du projet de loi C-8.

Une partie de la mission de Crypto Québec est de contribuer à un environnement numérique où la sécurité des infrastructures et des données s'articule autour de la protection des droits fondamentaux, et ce, en tenant compte avant tout des réalités québécoises ainsi que des pratiques industrielles internationales. À ce titre, je tiens à souligner que le Québec dispose déjà d'un corpus législatif robuste en matière de protection des renseignements personnels — je pense notamment à la loi 25 —, ainsi que d'institutions responsables, comme la Commission d'accès à l'information, la CAI, qui exerce une vigilance active relativement à la conformité et aux droits des citoyens. Je rappelle aussi que beaucoup de pratiques, de normes et de certifications existent en sécurité de l'information et encadrent les activités des infrastructures critiques au Québec à cet égard.

C'est donc dans cet esprit de double exigence à l'égard de la vie privée et de la sécurité que je formule aujourd'hui mes observations sur le projet de loi C-8. À l'heure où les adversaires des démocraties font connaître clairement et publiquement leur intention de semer le doute au sein de la population en ce qui concerne ses relations avec ses institutions gouvernementales, notre réponse doit également se traduire par une plus grande transparence.

Le projet de loi confère au gouvernement fédéral le pouvoir d'ordonner à des fournisseurs de services de télécommunications et à des opérateurs de systèmes vitaux de faire ou de s'abstenir de faire quoi que ce soit, et ceci peut constituer un secret d'État. Ce mécanisme soulève deux défis majeurs. Premièrement, il n'y a pas de garde-fous clairs en matière de nécessité, de proportionnalité, de durée et de recours pour les ordres délivrés. Ces défis ont été soulevés amplement dans les mémoires déposés. Deuxièmement, la confidentialité indéfinie de ces ordres crée un régime où, au-delà de l'objectif légitime de sécurité, la transparence et la reddition de comptes deviennent difficiles, voire impossibles.

Au Québec, la protection des renseignements personnels s'appuie sur des principes clairs: l'évaluation des facteurs relatifs à la vie privée, la documentation des mesures, la transparence quant aux interventions touchant les droits des individus, et finalement, le consentement. Ce modèle ne doit pas être affaibli par l'adoption d'un régime fédéral moins exigeant. Je recommande donc que tout ordre délivré en vertu du projet de loi C-8 fasse l'objet d'un résumé public et de rapports annuels déposés devant un comité ou l'Assemblée nationale, et qu'il soit assujetti à des critères de proportionnalité explicitement inscrits dans la loi.

Le Québec a démontré sa compétence en matière de vie privée et de sécurité numérique. La loi 25, ainsi que la loi 5, par exemple, qui concerne précisément les renseignements de santé, imposent des obligations strictes aux organisations publiques et privées concernant l'évaluation des facteurs relatifs à la vie privée, le consentement, la notification d'incidents, la localisation des données et le respect de la langue et des droits des citoyens québécois.

Le projet de loi C-8 pourrait créer un régime parallèle ou un régime qui chevauche celui du Québec pour les entités québécoises ou industrielles, à l'international, qui sont actives dans des secteurs vitaux, comme l'énergie, les télécommunications et les transports. Cela pose un risque de fragmentation, de dilution des responsabilités et de confusion pour les citoyens, ce qui soutiendrait nos adversaires dans leurs efforts. Il est essentiel que le cadre fédéral reconnaisse explicitement que les organisations exerçant leurs activités au Québec sont soumises à la loi 25 et que les normes québécoises restent au moins aussi protectrices que les exigences fédérales, ce qui n'est pas présentement garanti.

Contrairement au reste du Canada, le Québec possède une gouvernance avancée en ce qui a trait à la sécurité de l'information de ses systèmes. Tout d'abord, il a un ministère consacré à la cybersécurité, soit le ministère de la Cybersécurité et du Numérique, qui travaille à assurer un haut niveau de sécurité au sein de toutes les entités dont il est responsable. Ensuite, il a la Commission d'accès à l'information, une entité indépendante chargée de la protection des renseignements personnels qui, contrairement au reste du Canada, a certains pouvoirs punitifs en cas d'infraction ou de non-respect des lois. Le projet de loi C-8 viendrait empiéter sur les activités de ces deux institutions et n'assurerait aucunement un niveau de sécurité aussi élevé ou plus élevé. Au contraire, le projet de loi C-8 représenterait un recul pour le Québec.

Par ailleurs, un autre point critique est que le texte n'interdit pas explicitement le fait de contraindre un fournisseur à affaiblir le chiffrement ou à installer des mécanismes de surveillance internes. Cela touche directement la confiance des usagers, la sécurité des communications et la résistance aux menaces numériques. Au Québec, nous prônons un modèle où la sécurité n'est pas assurée au détriment de la vie privée, mais par le renforcement des contrôles, du chiffrement, de la gouvernance et des audits.

Je recommande que le projet de loi C-8 comprenne une interdiction explicite d'affaiblir le chiffrement, qu'il y ait une distinction claire entre les mesures de cybersécurité et les mesures de surveillance, et que toute collecte ou tout partage de données sensibles soit signalé aux autorités québécoises compétentes lorsqu'il s'agit d'entités au Québec.

En conclusion, je formule cette invitation: protégeons nos infrastructures critiques, mais faisons-le en respectant les droits des citoyens, en préservant les compétences québécoises et en nous assurant que le cadre adopté est clair, transparent, cohérent, proportionné et crédible. Le projet de loi C-8 représente une occasion, mais aussi un défi. Au Québec, nous avons déjà une feuille de route solide. Mettons-la à profit pour construire un modèle canadien qui soit fiable et digne de confiance. Le Québec peut y jouer un rôle central.

Je vous remercie de votre attention. Je suis prêt à répondre à vos questions.

● (1240)

Le président: Merci, monsieur Lefebvre.

Madame Polsky, la parole est maintenant à vous pour cinq minutes.

[*Traduction*]

Sharon Polsky (présidente, Conseil du Canada de l'accès et la vie privée): Je vous remercie de m'avoir invitée à m'entretenir avec le Comité aujourd'hui.

Je m'appelle Sharon Polsky. Je suis présidente du Conseil du Canada de l'accès et la vie privée, un organisme sans but lucratif qui est indépendant et non partisan et qui n'est financé ni par le gouvernement ni par l'industrie.

Depuis son lancement il y a une trentaine d'années, Internet s'est immiscé dans nos vies. J'ai passé ces années à conseiller des gouvernements, des petites et moyennes entreprises, ainsi que des sociétés qui font partie du palmarès Fortune 100, afin d'observer comment elles appliquaient la loi et les politiques et déterminer les risques pratiques inévitablement causés par la nature humaine, mais aussi, de plus en plus fréquemment, par Internet lui-même.

Le député Caputo a demandé des précisions, et j'espère pouvoir lui donner satisfaction. Le préambule indique que le projet de loi vise à protéger les fournisseurs de services de télécommunication et les systèmes essentiels, et confère au ministre le pouvoir de leur ordonner de faire ou de s'abstenir de faire quoi que ce soit afin de protéger le système canadien de télécommunication. C'est une intention louable, mais le projet de loi manque de mécanismes de protection adéquats pour prévenir les abus ou les attaques idéologiques. Cette nouvelle loi, qui ajoute la promotion de la sécurité du système de télécommunication canadien comme objectif stratégique, oblige les entreprises à combler les lacunes inhérentes à leurs systèmes, ce qu'elles auraient dû faire depuis longtemps pour se conformer aux lois sur la protection des renseignements personnels et à d'autres lois.

Reformuler la demande ne changera pas grand-chose, même avec les sanctions administratives pécuniaires. Mais je reviendrai là-dessus dans un instant.

En vertu de l'article 7 de la partie 2 qui est proposé, une catégorie d'exploitants peut être déclarée et toute personne ou organisation peut être déclarée membre de cette catégorie. Le projet de loi s'applique aux entreprises qui relèvent de la compétence législative du Parlement, et le paragraphe 9(1) proposé englobe les autres intervenants, c'est-à-dire les entreprises et les personnes dont les produits ou les services soutiennent les entreprises sous réglementation fédérale.

En matière de responsabilité, la vérificatrice générale a fait remarquer que « les lacunes dans les mécanismes de défense de cybersécurité empêchent le gouvernement de protéger les renseignements essentiels et de gérer les risques liés à la cybersécurité ». Ces lacunes subsisteront même si ce projet de loi est adopté.

Les normes, les lois et les cadres déjà en place — et les évaluations de la protection des renseignements personnels, de la sécurité et des risques désormais réalisées ou censées l'être — ne peuvent empêcher les pannes telles que celles que nous avons connues la semaine dernière, des pannes qui ont paralysé la moitié d'Internet, et d'autres pannes qui, hier encore, ont paralysé l'autre moitié et bloqué chaque fois des services partout dans le monde, à cause d'un seul problème technique. C'est tout ce qu'il a fallu, car les exigences en matière de responsabilité sont insuffisantes.

Quelle responsabilité peut-il y avoir quand l'existence même des ordonnances peut être gardée secrète et que le gouverneur en conseil peut ordonner que les ordonnances ne soient pas publiées? Cela laisse tout le monde dans l'ignorance et témoigne d'un manque de transparence antidémocratique et d'un obstacle à la responsabilité.

L'article 15.21 proposé exige que le ministre révèle combien de fois des ordonnances secrètes ont été prises au cours de l'année précédente et fournisse d'autres détails, mais les statistiques sont une maigre consolation, surtout si l'on tient compte des pouvoirs étendus en matière de collecte et de partage de renseignements qui sont conférés dans le projet de loi.

La partie 2 du projet de loi C-8 permet à tout service ou système d'être désigné comme un service ou un système essentiel et exige des exploitants désignés qu'ils s'emploient à « atténuer les risques associés à la chaîne d'approvisionnement ou aux tiers ». Elle ne précise pas quels risques doivent être atténués, mais devrait le faire.

Le paragraphe 20(6) proposé pour la Loi sur la protection des cybersystèmes essentiels interdit à un exploitant désigné ou à une catégorie d'exploitants d'intercepter des communications, mais les tiers qui fournissent des services essentiels ne sont pas visés par cette interdiction. Cela pourrait facilement se traduire par la mise en place de portes dérobées permettant de contourner le cryptage. Le gouvernement et d'autres ont déployé des efforts considérables au fil des ans pour contourner le cryptage. Le projet de loi C-8 doit être rédigé en termes clairs afin de garantir que les pouvoirs étendus qu'il confère ne puissent aucunement être utilisés par quiconque pour compromettre ou contourner le cryptage, une interdiction d'autant plus urgente que le libellé vague du projet de loi C-2 accorderait des pouvoirs ministériels étendus qui permettraient d'ordonner que des changements soient apportés dans les réseaux de télécommunication du Canada.

Le projet de loi stipule que les sanctions administratives pécuniaires ont pour seul but de promouvoir la conformité, et elles ne sont pas censées être punitives. Elles profiteront aux grands fournisseurs, qui pourront récupérer ces coûts auprès de leur large clientèle, consolider davantage leur position dominante et continuer à échapper à leurs responsabilités. Pendant ce temps, d'autres fournisseurs feront faillite.

La mise en œuvre des changements doit être surveillée, mesurée et obligatoire, avec des sanctions semblables à celles prévues par la loi Sarbanes-Oxley, y compris en ce qui concerne la responsabilité personnelle — et non celle de l'entreprise —, afin de rendre la responsabilité incontournable et d'inciter les acteurs à adopter de bons comportements dès le départ.

Je me demande comment un organisme de réglementation canadien pourra contrôler la conformité alors que Rogers vient d'annoncer qu'il exploitera son réseau sans fil depuis l'Inde.

Des ordonnances peuvent être prises concernant toute menace, y compris celle d'ingérence et de manipulation. Nous savons que les élections ont été influencées par le contenu des réseaux sociaux. L'intelligence artificielle appliquée à l'actualité déforme souvent les faits. Cette information sera-t-elle considérée comme de la manipulation ou une menace, et la plateforme sera-t-elle soumise à une censure?

● (1245)

Je me demande selon quels critères objectifs et quels calculs on mesure la gravité de la manipulation. Le projet de loi doit l'indiquer clairement.

Enfin, le fait d'ordonner que quelqu'un se voie refuser l'accès à Internet parce que le ministre considère que ses actes ou ses propos constituent une menace ou une manipulation reviendra à le priver de services téléphoniques, car ces services reposent désormais sur Internet. Tous les membres de son foyer ne pourront pas parler à leurs amis, appeler un service de transport adapté, composer le 911 ou demander l'admission à une université. Ce traitement est injuste et disproportionné, et c'est ce que permet le projet de loi C-8.

Le projet de loi C-8 doit être modifié, sinon nous revivrons ce que mes grands-parents ont fui il y a 100 ans, après la révolution russe: des personnes placées à l'isolement en raison de leurs opinions, ce qui est assimilé à une bonne pratique en matière de gouvernance.

Le président: Madame Polsky, je suis désolé de vous interrompre, mais c'est tout le temps dont nous disposions pour cette partie initiale de la réunion.

Cela nous permet de nous tourner vers le député Lloyd, afin de lui donner la parole pendant six minutes.

Dane Lloyd: Merci.

Je remercie tous les témoins qui sont présents aujourd'hui.

J'aime vraiment quand les gens proposent des idées d'amendements. Cela facilite notre travail. Je sais que les analystes tapaient à toute vitesse pendant ces interventions et qu'ils sont très satisfaits de toutes les idées qui ont été proposées.

Je vais commencer par vous interroger, monsieur Dehaas, à propos d'une observation que vous avez formulée. Pensez-vous qu'une attaque par déni de service relève de la liberté d'expression?

● (1250)

Josh Dehaas: Je tiens à être très clair à ce sujet, monsieur le président. Je ne pense pas qu'une attaque par déni de service distribué relève de la liberté d'expression.

Ce que je veux dire, c'est qu'une personne soupçonnée d'avoir participé à ce type d'attaque pourrait faire face à des conséquences très graves en vertu de l'article 15.2 proposé, sans qu'une application régulière de la loi ait été mise en place, très...

Dane Lloyd: Je vous suis reconnaissant de cette précision. Merci.

Je me pose simplement une question. Nous avons accueilli ici le commissaire à la protection de la vie privée, et il était préoccupé par le projet de loi C-26. Il a indiqué que la question de la nécessité et de la proportionnalité avaient été largement prises en compte par l'ajout d'une exigence concernant le caractère raisonnable. Les représentants du gouvernement nous ont dit que l'exigence concernant le caractère raisonnable avait été clairement définie dans une affaire jugée par la Cour suprême.

Pourquoi pensez-vous que cette exigence n'est pas appropriée ou suffisamment stricte pour protéger les citoyens contre les abus du ministre?

Josh Dehaas: L'exigence de caractère raisonnable est importante. C'est un bon ajout au projet de loi.

Le problème, c'est que l'article 15.2 proposé stipule que « toute menace » pourrait donner lieu à ce type de décret. « Toute menace » n'est tout simplement pas un seuil suffisamment élevé. Le juge examinerait la question et se demanderait s'il s'agit d'une décision raisonnable, compte tenu du pouvoir qui est accordé au ministre de prendre ce type de mesure en cas de menace, aussi minime soit-elle, qu'elle soit grave ou insignifiante.

Dane Lloyd: Le caractère raisonnable n'imposerait-il pas que la réponse soit proportionnelle au niveau de la menace, ou cela n'est-il pas clair?

Josh Dehaas: Ce serait raisonnable au regard de ce qui est écrit dans la disposition 15.2. Un juge, examinant cela ultérieurement, se demanderait s'il s'agit d'une décision proportionnée, sur la base de ce pouvoir, qui est très large.

Le paragraphe 15.1(2) proposé traite de la portée et du fond. Il s'agit toujours de la portée et du fond par rapport à la disposition elle-même. Je pense qu'il serait utile d'ajouter les mots « grave » et « systémique » à l'article 15.2.

Dane Lloyd: Cette modification m'intéresse beaucoup. Je vous remercie de l'avoir proposée.

Nous parlons des décrets secrets. Le ministère est venu nous assurer que, dans 99 % des cas, il n'y aurait aucune justification pour un décret secret. Cependant, dans 1 % des cas, la divulgation d'un décret constituerait en soi une menace pour le système de télécommunications, mais vous ne semblez pas convaincu que cela constitue une garantie suffisante.

Vous avez donné l'exemple d'un manifestant soupçonné de vouloir commettre une attaque par déni de service. Quelle exigence de caractère raisonnable le ministre devrait-il respecter pour émettre un décret secret interdisant à cette personne d'accéder à Internet?

Josh Dehaas: Je pense que cela serait difficile à justifier.

Je pense qu'il existe des cas où un décret secret serait justifié. Il pourrait, par exemple, s'agir de menaces pour la sécurité nationale provenant d'autres pays ou d'acteurs étrangers qui veulent prendre le contrôle d'une partie du système. La façon dont cela est rédigé permettrait au ministre de le faire et de garder le secret suffisamment longtemps, jusqu'à ce que la crise responsable de cette situation soit passée.

Prenons l'exemple d'un manifestant qui souhaite prendre le contrôle du site Web du premier ministre au moyen d'une attaque par déni de service. Il se pourrait qu'un groupe planifie de le faire dans le cadre d'une manifestation. Le ministre pourrait prendre cette mesure à titre de sanction, sans procédure régulière, et garder cela secret. Nous ne saurions peut-être jamais que cela s'est produit, donc...

Dane Lloyd: Bien qu'il existe actuellement une obligation de notification, êtes-vous en train de dire que cette obligation n'est probablement pas assez stricte?

Josh Dehaas: Je dis qu'elle doit être plus stricte, oui.

Dane Lloyd: Je vais passer à autre chose.

Dans le projet de loi, il a été question des pouvoirs de décryptage.

Monsieur Shull, je n'ai rien vu dans le projet de loi concernant les pouvoirs de décryptage, mais il semble que les gens disent que, comme on donne au ministre le pouvoir de contraindre les entreprises de télécommunications à faire ou à ne pas faire quelque chose, cela pourrait indirectement conduire au décryptage. Avez-vous quelque chose à dire à ce sujet?

Aaron Shull: Le projet de loi ne mentionne pas explicitement la possibilité de déchiffrer les données, mais vous avez raison de dire que le libellé est vague. Je présume que l'on pourrait se retrouver dans cette situation. C'est pourquoi je disais qu'il fallait être précis en ce qui concerne les critères.

Il y a des méchants qui font des choses répréhensibles et nous devons être en mesure de les arrêter. Nous sommes tous d'accord là-dessus, mais dans quelles circonstances? Soyons clairs sur les critères établis afin que, lorsque nous devrons déterminer si telle ou telle mesure était raisonnable, nous sachions à quoi nous en tenir.

Dane Lloyd: D'accord.

Je me souviens de la question que je voulais poser à M. Dehaas.

Supposons qu'une personne soit bannie d'Internet parce que le gouvernement pense qu'elle va commettre un attentat. Je pense qu'elle doit être consultée et informée par le gouvernement qu'elle a été bannie. N'est-ce pas clair?

● (1255)

Josh Dehaas: Dans la plupart des cas, le gouvernement le ferait et cette personne le saurait, mais cela n'est pas clair pour moi dans le projet de loi. J'estime que cela pourrait être clarifié.

Dane Lloyd: Le fait de demander réparation devant les tribunaux est-il un crime en soi? Si vous estimez que cela est injustifié, que l'on viole vos droits garantis par la Charte et que vous vous adressez à un juge, est-ce une violation du décret secret? Est-ce un crime en soi?

Josh Dehaas: Non, ce ne serait pas le cas. Un contrôle judiciaire serait toujours possible.

Le problème ici, c'est qu'un profane peut ne pas s'en rendre compte et être intimidé par le fait qu'il n'est pas tout à fait clair qu'il ne peut pas demander un contrôle judiciaire et que cela constituerait une violation du décret. Même si le contrôle judiciaire est en principe toujours possible, cela devrait être clarifié.

Dane Lloyd: Merci.

[*Français*]

Le président: Je vous remercie beaucoup tous les deux.

Madame Dandurand, vous avez la parole pour six minutes.

Marianne Dandurand: Merci, monsieur le président.

Je compare les témoignages que nous entendons aujourd'hui à ceux que nous avons entendus la semaine dernière de la part de témoins experts, et certaines choses me font un peu sursauter.

Monsieur Dehaas, une des choses que nous avons entendues de la part de votre organisation est que le projet de loi C-8 pourrait permettre au gouvernement de déconnecter des Canadiens d'Internet parce qu'ils ont critiqué le gouvernement. Un certain témoin expert, la semaine dernière, a dit que les propos tenus par les Canadiens à titre individuel n'entraient absolument pas dans le champ d'application du projet de loi. On dit aussi que celui-ci contient des notions de proportionnalité et de nécessité d'arrêter une attaque pour que la loi soit appliquée.

Que répondez-vous à ça?

[*Traduction*]

Josh Dehaas: Je pense que le gouvernement, en toute bonne foi, n'est peut-être pas particulièrement intéressé par ce type de censure. Le problème, c'est que la loi stipule qu'elle s'applique à toute menace pesant sur le système de télécommunications, ce qui laisse beaucoup de place à l'interprétation.

Un tribunal jugerait-il que la loi le permet? Probablement pas, mais le risque, c'est que le gouvernement le fasse quand même. Par exemple, en cas de crise, lorsque les tensions sont vives, ce genre de chose peut arriver. C'est pourquoi il est important de préciser qu'il s'agit de menaces graves, de menaces qui visent le système proprement dit et non la seule liberté d'expression individuelle.

[*Français*]

Marianne Dandurand: D'accord.

Madame Polsky, je vais vous poser le même genre de question. Vous disiez que le projet de loi allait éventuellement permettre de la recherche à l'aveuglette. L'expert dont je parlais plus tôt disait que rien de ce que vous mentionnez comme menace ne pourrait être applicable. Ce que vous craignez dépasse largement le champ d'application du projet de loi. Il n'y a donc pas de pêche à l'aveuglette possible.

De votre côté, que répondez-vous à ça?

[*Traduction*]

Sharon Polsky: Il est certes important de protéger nos infrastructures nationales essentielles et de prévoir des dispositions à cet fin, mais il faut fixer des limites appropriées, car le libellé actuel de la loi est suffisamment vague, comme l'a dit mon collègue, pour laisser place à l'interprétation.

Sans limites précises et en l'absence d'un cadre défini, qu'est-ce qui constitue une menace? Tout peut être justifié. C'est très facile. Nous avons affaire à la nature humaine, et si quelqu'un se sent menacé, il est facile de dire ce qu'il faut dire, de trouver des preuves, de porter des accusations, de faire ce que l'on veut et de laisser la personne se défendre après coup.

C'est dangereux. Il faut donc utiliser un libellé plus clair afin d'éviter d'ouvrir la porte à toutes sortes d'interprétation.

[*Français*]

Marianne Dandurand: Le projet de loi contient une section qui définit bien ce qu'on considère comme étant une menace. Cela fait référence à ce qui est contenu dans la loi. Certains experts se sont penchés sur cette question.

Je vais m'adresser à M. Shull.

J'aimerais parler des comparaisons avec d'autres administrations à l'étranger. On a dit que l'Union européenne, les États-Unis et l'Australie avaient déjà des approches pour concilier la cybersécurité, la protection de la vie privée, la transparence et la surveillance.

Selon vous, le projet de loi C-8 nous permet-il de nous conformer efficacement aux meilleures pratiques dans le monde concernant la cybersécurité?

[*Traduction*]

Aaron Shull: Je pense que c'est un bon projet de loi. Ne vous méprenez pas. Je demande que certaines dispositions soient modifiées, car je pense que certains aspects du projet de loi pourraient être renforcés, mais je suis absolument convaincu que nous avons besoin de ce projet de loi.

Je vais prendre un peu de recul et dire que lorsque nous parlons de protection des renseignements personnels, nous parlons de renseignements personnels identifiables. Ce projet de loi concerne le système lui-même, pas seulement les personnes. Le mal fondamental auquel nous essayons de remédier est que nous connectons tout ce que nous pouvons à Internet, y compris les systèmes d'approvisionnement en eau et les réseaux d'électricité. Nous ne parlons pas vraiment de technologie opérationnelle, mais je peux vous dire d'entrée de jeu que c'est ce que font les méchants. Ils se positionnent d'avance sur nos infrastructures névralgiques dans le but de nous paralyser en cas de conflit ou de faire pression. C'est très grave et nous devons nous prémunir contre cela.

Ce que je veux dire, c'est que je soutiens pleinement ce projet de loi. Il n'a besoin que de quelques petits changements pour l'améliorer un peu.

● (1300)

[*Français*]

Marianne Dandurand: Je vous remercie.

Revenons à la comparaison avec les autres administrations de l'étranger. Avons-nous des leçons à recevoir? Certaines d'entre elles sont-elles déjà rendues plus loin? Serions-nous des chefs de file si nous mettions en application votre suggestion?

[*Traduction*]

Aaron Shull: Tout à fait. Les comparaisons les plus pertinentes seront toujours celles avec les États-Unis, l'Australie et le Royaume-Uni. Nous ne disposons actuellement d'aucun mécanisme obligeant les fournisseurs d'infrastructures essentielles à signaler les incidents, et nous n'avons aucune autorité législative pour exiger des fournisseurs de télécommunications qu'ils retirent leurs équipements défectueux. Nos alliés, eux, en ont, ce qui signifie que nous sommes déjà en retard par rapport au reste de la classe.

Le simple fait de faire adopter ce projet de loi est un pas dans la bonne direction.

[*Français*]

Le président: Madame Dandurand, il vous reste 15 secondes de temps de parole en tout.

Marianne Dandurand: Je vais donc vous les laisser.

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

Claude DeBellefeuille: Merci, monsieur le président.

Je remercie les témoins de leurs témoignages. Je pense qu'il s'en dégage un certain consensus sur le fait que c'est une bonne loi, mais qu'il y a des améliorations à y apporter, surtout à l'article 15. On devra peut-être resserrer ou mieux encadrer les pouvoirs du ministre. Il y a des rapports et une reddition de comptes, mais ils ne correspondent pas aux pouvoirs des ministres. C'est ce que je remarque et que je retiens aujourd'hui. Je vous remercie infiniment.

Monsieur Lefebvre, j'aimerais vous poser une question afin que le Comité puisse mieux comprendre un élément. Vous avez parlé de chiffrement. Nous n'avons pas de connaissances à ce sujet, mais je pense que c'est un aspect important pour vous, car vous soulignez que c'est complètement absent du projet de loi.

Pouvez-vous nous expliquer pourquoi vous trouvez important qu'on indique dans le projet de loi qu'il est interdit de modifier les normes de chiffrement?

Luc Lefebvre: En fait, le projet de loi ne parle pas précisément du chiffrement. En ce moment, dans les démocraties occidentales, on a tendance à vouloir diminuer le chiffrement. Les forces de l'ordre et les agences de renseignements insistent pour qu'il y ait une diminution du chiffrement concernant les applications de messagerie et tout ce qui peut être lié aux communications. On parle des télécommunications et de ce genre de chose. Il y a une très grande tendance en ce moment, que ce soit au Royaume-Uni ou aux États-Unis, à vouloir diminuer ce chiffrement.

Au fond, nous recommandons surtout de prendre de l'avance. Le Canada veut-il être un chef de file avec la mise en place du projet de loi C-8? S'il veut devenir un chef de file, il doit prendre les devants et préciser que ces pouvoirs, qui sont assez extraordinaires, ne seront pas utilisés afin de diminuer le chiffrement, ce qui pourrait porter atteinte à la protection de la vie privée et des renseignements personnels des Canadiens.

Pour toutes ces raisons, je pense qu'il faudrait le préciser.

Claude DeBellefeuille: Je pense que le chiffrement est ce qui empêche les compagnies ou le gouvernement d'avoir accès à nos conversations personnelles. Si on réduit les normes, ils pourraient y avoir accès sans qu'on le sache. Le chiffrement est donc une protection, une mesure qu'on doit conserver pour ne pas permettre une intrusion facile par les autorités à nos échanges par courriel ou sur WhatsApp, Messenger, Facebook, etc. C'est ce que j'ai compris.

Lors de la séance précédente, on a beaucoup parlé des chevauchements avec le Québec, et les fonctionnaires du ministère nous ont dit qu'ils étaient conscients de ces chevauchements et des doubles emplois, mais ils disaient que tout allait se régler dans la partie réglementaire où, on allait essayer de réduire le plus possible ces chevauchements.

Étant une députée du Bloc québécois, je sais que, quand le Canada veut faire ça avec les provinces, le résultat est tout le temps qu'il veut imposer ses vues et que les provinces doivent s'y plier et s'y conformer. La preuve, c'est qu'actuellement, quelques milliards de dollars restent dans les coffres de l'État fédéral, alors que les municipalités en ont besoin. Cependant, faute d'entente avec le Québec parce qu'Ottawa veut imposer ses normes, l'argent n'est actuellement pas décaissé, alors que ça permettrait particulièrement aux municipalités de construire des infrastructures.

Pourriez-vous me dire où se situe votre plus grande crainte quant à ce chevauchement et au dédoublement? Quel est le problème principal?

● (1305)

Luc Lefebvre: Bien sûr, dans les faits, il y a des différences fondamentales entre la loi 25 sur la protection des renseignements personnels des citoyens du Québec et le projet de loi C-8. Ce dernier ne couvre pas très particulièrement les risques d'atteinte à la protection de la vie privée. Il n'est probablement pas assez clair, notamment au sujet de la proportionnalité, par exemple, dont nous avons parlé. En revanche, la loi 25 du Québec y accorde énormément d'importance.

En fait, la logique de l'approche québécoise en matière de sécurité de l'information, de protection des renseignements personnels et de protection des infrastructures est très orientée vers la protection de la vie privée. Cette protection est vraiment centrale dans l'approche québécoise, tandis que celle que propose le projet de loi C-8 est très technique. Au fond, elle est très orientée vers la protection des opérations des infrastructures critiques, mais elle tient peu compte de la protection de la vie privée. On a parlé précédemment de tous les petits détails qui pourraient permettre que des individus soient ciblés. La protection de la liberté d'expression et ce genre de chose ne sont pas tant définies dans le projet de loi C-8. C'est donc certainement un défi.

Pour ce qui est des chevauchements, il est clair que le projet de loi C-8 empiéterait sur beaucoup des compétences, notamment celles du ministère québécois de la Cybersécurité et du Numérique, ou MCN, qui est responsable d'assurer la sécurité de toutes les infrastructures critiques du Québec, des ministères et des organismes paragouvernementaux. Il y aurait donc un chevauchement évident. Il resterait à voir si le MCN pourrait conserver ultimement certains droits, certains pouvoirs, alors qu'il en a déjà peu, d'une certaine manière. Conserverait-il ses pouvoirs, au regard du projet de loi C-8 ou vis-à-vis du fédéral? On a l'impression que le projet de loi C-8 prévaudrait sur ce plan.

Il y a un endroit où il n'y a pas de chevauchement. Le MCN n'a pas tant de pouvoirs sur le plan de l'imposition de certaines obligations sécuritaires aux entreprises privées, comme les télécoms. Le projet de loi C-8 présenterait donc un avantage à cet égard puisqu'il n'y a pas de chevauchement, mais vraiment, il faudrait faire de la mise en correspondance, ce qu'on appelle du « mappage », dans le milieu du contrôle. Il s'agit de...

Le président: Monsieur Lefebvre, je suis désolé de vous interrompre encore une fois, mais c'est tout le temps que nous avons.

[*Traduction*]

John Brassard (Barrie-Sud—Innisfil, PCC): Monsieur le président, j'invoque le Règlement.

[*Français*]

Le président: Messieurs les témoins, je vous remercie de votre présence, et du temps que vous avez mis à vous préparer pour cette rencontre, aujourd'hui. C'est tout le temps que nous avons pour vous.

John Brassard: J'invoque le Règlement.

Le président: Comme le temps est écoulé, je vais ajourner la réunion. Nous nous reverrons mardi prochain.