CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

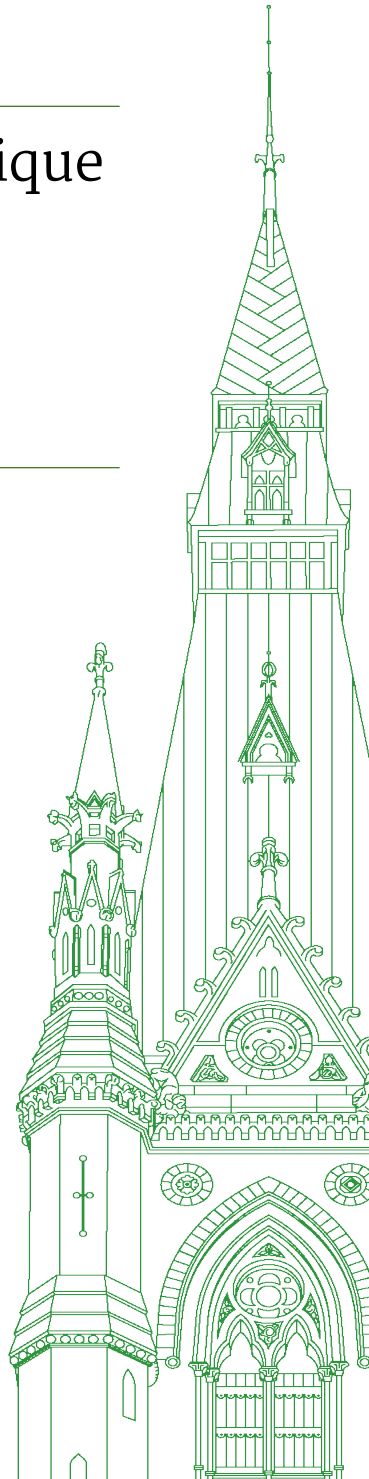
44e LÉGISLATURE, 1re SESSION

Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 093

Le jeudi 8 février 2024



Président : M. Heath MacDonald

Comité permanent de la sécurité publique et nationale

Le jeudi 8 février 2024

● (0815)

[*Traduction*]

Le président (M. Heath MacDonald (Malpeque, Lib.)): La séance est ouverte.

Je vous souhaite la bienvenue à la 93e réunion du Comité permanent de la sécurité publique et nationale de la Chambre des communes. Conformément au Règlement, la réunion d'aujourd'hui se déroule de façon hybride. Les membres du Comité y participent en personne, dans la salle, et à distance, en utilisant l'application Zoom.

J'aimerais faire quelques commentaires à l'intention des témoins et des membres du Comité.

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

Pour éviter les retours de son dérangeants pendant la réunion, nous demandons à tous les participants d'éloigner leur oreillette du microphone. De tels incidents peuvent blesser gravement les interprètes et nuire à nos délibérations.

Je vous rappelle également que tous les commentaires doivent être adressés à la présidence.

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

J'aimerais souhaiter la bienvenue à nos témoins du premier groupe.

Nous accueillons John de Boer, directeur principal, Affaires gouvernementales et politiques publiques, Canada, chez BlackBerry. Nous recevons également Jennifer Quaid, directrice exécutive d'Échange canadien de menaces cybernétiques. Nous accueillons enfin Francis Bradley, président-directeur général d'Électricité Canada.

Les témoins disposent chacun de cinq minutes pour leur déclaration préliminaire. Nous passerons ensuite aux questions des députés.

Bienvenue à tous.

J'invite maintenant M. de Boer à faire sa déclaration préliminaire. Allez-y.

M. John de Boer (directeur principal, Affaires gouvernementales et politiques publiques, Canada, BlackBerry): Merci, monsieur le président.

Au nom de BlackBerry, je suis ravi de m'adresser aux membres du Comité aujourd'hui.

Depuis plus de 35 ans, BlackBerry a inventé et élaboré des solutions fiables pour donner aux gens, aux gouvernements et aux entreprises la capacité de rester en sécurité et productifs.

Aujourd'hui, nous sommes un chef de file en matière de logiciels et de services de cybersécurité. Nous protégeons plus de 500 millions de systèmes dans le monde. Nos clients comprennent tous les gouvernements du G7, l'OTAN, 45 entreprises du palmarès de Fortune 100, 9 des 10 plus grandes banques mondiales et de nombreuses entités d'infrastructures essentielles.

Les infrastructures essentielles constituent une cible de choix pour les cybercriminels et les auteurs de cybermenaces parrainés par des États. Chez BlackBerry, nous le savons de première main. Entre septembre et décembre 2023, nous avons mis fin à plus de 5,2 millions de cyberattaques, dont 62 % ciblaient des infrastructures essentielles.

Pas plus tard qu'hier, le Centre canadien pour la cybersécurité, de concert avec des partenaires du Groupe des cinq, a publié un avis confirmant que des auteurs de cybermenaces parrainés par la République populaire de Chine avaient compromis des entités dans de nombreux secteurs d'infrastructures essentielles aux États-Unis, y compris les communications, l'énergie, les transports, ainsi que les infrastructures d'approvisionnement en eau et de traitement des eaux usées.

Selon le directeur de la U.S. Cybersecurity and Infrastructure Security Agency, il se peut que ce ne soit « que la pointe de l'iceberg ». Le cybercentre du Canada estime que « si les infrastructures américaines devaient être perturbées, il est possible que le Canada soit aussi touché, en raison de l'intégration transfrontalière ».

En plus de fournir des services essentiels, les entités d'infrastructures essentielles hébergent de grandes quantités de renseignements de nature délicate, y compris de la propriété intellectuelle, des dessins techniques et des renseignements personnels, qui sont des cibles attrayantes pour les auteurs de cybermenaces.

À l'heure actuelle, mis à part les obligations liées à la Loi sur la protection des renseignements personnels et les documents électroniques, la LPRPDE, le Canada n'a aucune loi en place pour régir les entités d'infrastructures essentielles, et encore moins pour les obliger à signaler les incidents de cybersécurité, à s'y préparer et à les prévenir.

La Loi sur la protection des cybersystèmes essentiels contribuera à stimuler les investissements nécessaires pour améliorer la cyberrésilience et à faire en sorte que les entités d'infrastructures essentielles puissent fonctionner en cas de perturbations et se rétablir rapidement.

Pour revenir à une comparaison plus large, le Canada accuse un retard par rapport à ses pairs du G7 en matière de cybersécurité. Le gouvernement des États-Unis et des gouvernements en Europe ont déjà pris des mesures réglementaires qui relèvent la barre en matière de cybersécurité des infrastructures essentielles. En mars 2022, le président Biden a adopté la Cyber Incident Reporting for Critical Infrastructure Act, qui exige que les entités d'infrastructures essentielles visées signalent les incidents de cybersécurité au gouvernement dans les 72 heures, et les paiements par suite d'attaques par rançongiciel, dans les 24 heures. En octobre 2022, l'Union européenne a approuvé une loi exigeant que les exploitants de services essentiels mettent en œuvre des mesures de cybersécurité de base et avisent les autorités nationales des incidents graves de cybersécurité dans les 72 heures.

Le Canada est actuellement en décalage par rapport à ses plus proches alliés en matière de cybersécurité. Cette mesure législative contribuera à combler l'écart. Le signalement des cyberincidents aidera le gouvernement et les entités du secteur privé à partager rapidement des renseignements pertinents, à avertir et à protéger d'autres victimes potentielles et à déployer rapidement des ressources et de l'aide pour limiter les dommages causés par les cyberincidents.

Dans le cadre de l'étude du projet de loi par le Comité, BlackBerry aimerait formuler trois recommandations pour renforcer la loi.

Tout d'abord, il faudrait harmoniser les exigences en matière de signalement des cyberincidents avec celles de nos principaux alliés, notamment les États-Unis. Cela aidera à réduire le fardeau inutile imposé aux entités déclarantes et à faire en sorte que les ressources des entités confrontées à un incident soient consacrées à l'atténuation des effets des cyberincidents. Deuxièmement, il faudrait fournir des garanties aux entités visées que l'information qu'elles fournissent n'engage pas leur responsabilité. Troisièmement, il faudrait veiller à ce que les entités visées par les exigences en matière de signalement des cyberincidents ne fassent pas l'objet de mesures punitives pour les efforts de bonne foi qu'elles ont déployés pour se conformer à la loi.

En conclusion, cette loi aidera à combler les lacunes dans la capacité de notre pays de prévenir les cyberattaques, d'améliorer sa connaissance de la situation, de favoriser une intervention rapide et efficace et d'aider à créer une culture de cybersécurité proactive, axée sur la prévention à grande échelle.

BlackBerry est prêt à travailler avec ce comité pour renforcer la cyberrésilience du Canada.

● (0820)

Merci.

Le président: Merci, monsieur de Boer.

Madame Quaid, vous êtes la suivante. Je vous en prie.

Mme Jennifer Quaid (directrice exécutive, Échange canadien de menaces cybernétiques): Bonjour, monsieur le président.

Merci à tous.

J'ai l'honneur d'être ici aujourd'hui à titre de représentante d'Échange canadien de menaces cybernétiques, un organisme créé par des entreprises canadiennes pour offrir à ses membres un environnement sécuritaire où ils peuvent échanger de l'information sur les cybermenaces et collaborer en mettant en commun des pratiques exemplaires et des idées. L'objectif est de renforcer la cyberrésilience et de créer un environnement économique plus solide pour tous. Nos 170 membres, qui représentent 15 secteurs et plus de 1,5 million d'employés, échangent activement de l'information sur les cybermenaces, afin d'aider à accroître la sensibilisation et la résilience d'autres parties et à prévenir les atteintes et la nécessité correspondante de les signaler.

Bon nombre de nos membres représentent les secteurs des infrastructures essentielles touchés par cette loi, tandis que d'autres assurent leur chaîne d'approvisionnement. Bon nombre d'entre eux sont des petites et moyennes entreprises, comme celles qui constituent une grande partie de l'économie canadienne.

Je félicite le gouvernement d'avoir concentré son attention sur la création d'une loi qui aidera à renforcer le secteur des infrastructures essentielles du Canada. Je crois qu'avec quelques petites modifications, le projet de loi nous donne l'occasion d'en faire plus pour favoriser la résilience des entreprises canadiennes et renforcer l'économie canadienne au-delà des six secteurs d'infrastructures essentielles mentionnés.

Certains ont parlé avec éloquence des questions de protection de la vie privée et des risques réels liés à la responsabilité attribuée à nos dirigeants principaux de la sécurité de l'information. Ce sont tous de très bons points, que nous appuyons.

J'aimerais parler de trois suggestions économiques qui sont faciles à mettre en œuvre et qui auront une incidence importante sur la cyberrésilience partout au Canada.

Premièrement, la loi devrait être modifiée pour inclure un libellé qui encourage toutes les organisations à partager volontairement des renseignements sur les cybermenaces et à collaborer avec d'autres pour renforcer la résilience. Cela peut se faire avec l'ajout d'un libellé dans le préambule et deux petits changements connexes. Je me ferai un plaisir de fournir au Comité une partie du texte proposé plus tard.

Le deuxième changement consiste à faire de l'adhésion à une association canadienne d'échange d'information sur les cybermenaces une dépense admissible au titre des programmes gouvernementaux. Par exemple, aux termes de la Politique des retombées industrielles et technologiques du Canada, l'appartenance à une organisation ne fait pas partie des critères d'inclusion admissibles. Ce changement inciterait les entreprises à participer à une organisation de partage et de collaboration, afin d'accroître leur sensibilisation à la cybersécurité et leur résilience de façon continue. Ce serait un petit changement qui aurait un impact important et qui ne coûterait rien au gouvernement.

Troisièmement, le projet de loi exige seulement que des organisations précises communiquent des renseignements sur les cyberincidents aux organismes qui les réglementent ou au gouvernement. Nous avons ici l'occasion de créer un environnement juridique qui permet à toutes les entreprises, y compris celles qui sont précisées, d'échanger des renseignements au-delà de ce que les dispositions législatives exigent d'elles. Des membres canadiens et des entreprises canadiennes représentés par l'ECMC ont des filiales américaines qui échangent actuellement aux États-Unis des renseignements qu'elles ne peuvent pas partager au Canada parce qu'elles ne sont pas protégées par la loi. Elles s'inquiètent de la responsabilité civile liée à la communication volontaire de renseignements qui pourraient en aider d'autres à prévenir des incidents.

L'objectif du projet de loi C-26 est de prévenir d'autres cyberincidents. Le signalement obligatoire des incidents ne suffit pas. Il ne protégera pas suffisamment d'organisations assez rapidement. En ajoutant une protection au chapitre de la responsabilité civile, le projet de loi pourrait régler ce problème. Les entreprises pourraient être autorisées à partager des renseignements au-delà de ce qui est strictement nécessaire pour se conformer et améliorer la cybersécurité et la résilience de l'économie dans son ensemble d'une manière rentable et significative. Sans cette protection, des renseignements essentiels continueront d'être communiqués à des organisations à l'extérieur du Canada.

En créant et en appuyant l'ECMC, le milieu des affaires du Canada démontre continuellement sa volonté et son désir de partager l'information sur les cybermenaces et de faire profiter les entreprises canadiennes de son expertise et de son expérience. Vous pouvez l'aider à en faire plus. Vous pouvez lui permettre d'en faire plus. S'ils sont adoptés dans le cadre de ce projet de loi, ces trois changements assureront une chaîne d'approvisionnement plus sécuritaire pour les infrastructures essentielles, ce qui est l'objet du projet de loi, et pour toutes les entreprises canadiennes, grandes et petites.

Merci.

● (0825)

Le président: Merci, madame Quaid. Vous avez terminé juste à temps.

Monsieur Bradley, vous êtes le suivant. Je vous en prie.

[*Français*]

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

Je suis le PDG d'Électricité Canada, qui était connu sous le nom de l'Association canadienne de l'électricité. Nos membres sont des compagnies qui produisent, transportent et distribuent l'électricité dans toutes les provinces et tous les territoires du Canada.

Mes commentaires aujourd'hui se concentreront sur la partie 2 du projet de loi C-26, qui édicte la Loi sur la protection des cybersystèmes essentiels.

[*Traduction*]

Avant d'aller plus loin, je tiens à souligner les efforts déployés par les ministères fédéraux pour rédiger le projet de loi C-26 et le temps qu'ils ont consacré à mobiliser les intervenants au cours des deux dernières années. Les problèmes que le projet de loi tente de régler sont difficiles à résoudre, avec beaucoup d'éléments changeants et de vastes répercussions dans un contexte de menaces en constante évolution.

Bien que je salue les efforts déployés, je dois ajouter ma voix à celles des témoins que vous avez déjà entendus et qui ont insisté sur l'importance de bien faire les choses. Même si nous reconnaissons l'urgence d'adopter ce genre de mesure législative, il est essentiel d'envisager attentivement des amendements et de résister à la pression de précipiter l'examen du projet de loi.

Les exigences de sécurité obligatoires peuvent contribuer à renforcer notre posture globale au chapitre de la sécurité, mais l'approche adoptée par le projet de loi C-26 risque d'avoir l'effet contraire, en augmentant très peu la sécurité pour notre secteur et en ajoutant de façon redondante des couches supplémentaires d'exigences réglementaires. J'aimerais souligner aujourd'hui trois domaines où le projet de loi laisse à désirer et où des améliorations s'imposent.

Premièrement, le projet de loi doit s'harmoniser avec les cadres réglementaires existants. Le secteur de l'électricité est unique en ce sens que les actifs visés par le projet de loi C-26 sont déjà réglementés par la North American Electric Reliability Corporation, ou NERC. Cela pose un risque de conflits au chapitre de la réglementation, alourdit le fardeau des exploitants et introduit de la confusion et de l'ambiguïté en matière de conformité, ce qui, au bout du compte, nuit à l'objectif du projet de loi C-26 d'améliorer la sécurité de nos systèmes essentiels.

La semaine dernière, un témoin a recommandé que, dans le cadre du projet de loi, on adopte une approche fondée sur le risque et on impose moins d'exigences à ceux qui ont déjà de solides programmes de cybersécurité. Selon cette approche, les organisations bien établies pourraient consacrer plus de ressources à la prévention des incidents plutôt qu'aux activités liées à la conformité, et les organismes de réglementation pourraient mieux concentrer leur temps sur les exploitants présentant un risque élevé. Compte tenu de la solide posture de notre secteur au chapitre de la sécurité et des normes actuelles de la NERC, nous croyons qu'une approche fondée sur le risque dans le cadre du projet de loi C-26 serait un pas dans la bonne direction.

Le projet de loi doit aussi améliorer les exigences en matière de rapports. La référence au signalement immédiat des cyberincidents devrait être révisée. Les obligations de déclaration ne devraient pas détourner les exploitants d'infrastructures essentielles de leurs efforts d'intervention et de rétablissement pendant et après les incidents. Les exigences en matière de rapports doivent être bien définies et cohérentes, et le calendrier de production des rapports doit être suffisamment souple pour permettre l'utilisation efficace des ressources limitées pendant l'intervention et la reprise en cas d'incident.

Toujours au sujet des exigences en matière de déclaration, les objectifs de la loi seraient mieux servis si une protection juridique pour les exploitants était incluse. Les dispositions d'exonération sont un élément important de la promotion de l'échange de renseignements entre l'industrie et le gouvernement, de la mise en œuvre réussie des nouvelles exigences en matière de déclaration et de la promotion de l'échange volontaire de renseignements.

Le dernier aspect que je veux aborder est l'effet non voulu du projet de loi sur la collaboration actuelle entre l'industrie et le gouvernement. L'imposition d'exigences obligatoires pourrait entraîner un refroidissement des relations de l'industrie avec les ministères et organismes gouvernementaux. En l'absence de mesures de protection appropriées, les juristes conseilleront probablement aux exploitants de ne partager que l'information nécessaire pour se conformer à la loi, et rien de plus.

Cela irait à l'encontre des objectifs du projet de loi, mais il y a deux ou trois choses que vous pourriez faire pour atténuer ces risques. Premièrement, il faut établir des limites claires quant à la façon dont le gouvernement peut utiliser les renseignements recueillis aux termes de cette loi. Plusieurs dispositions du projet de loi permettraient l'échange de renseignements entre un éventail de personnes et d'entités, mais ne limitent pas explicitement la façon dont les destinataires utiliseront les renseignements recueillis.

Deuxièmement, le cybercentre devrait être exclu de la loi et exempté de l'obligation de déclarer à d'autres entités les renseignements obtenus en vertu de la loi. Les exploitants d'infrastructures essentielles entretiennent actuellement une relation de collaboration positive avec le cybercentre. Cela repose sur la conviction que ce dernier ne divulgue pas les renseignements des exploitants aux organismes de réglementation, aux organismes d'application de la loi ou à d'autres ministères. Il est essentiel de protéger le cybercentre contre les obligations de partage de l'information pour maintenir cette relation de collaboration.

● (0830)

[*Français*]

De nombreux autres aspects du projet de loi C-26 mériteraient également qu'on s'y attarde, mais c'est tout le temps de parole dont je dispose ce matin.

Cependant, je vous encourage à consulter notre mémoire, qui contient 14 recommandations sur la manière d'améliorer le projet de loi C-26.

Merci beaucoup.

[*Traduction*]

Le président: Merci, monsieur Bradley.

Je vous remercie tous.

Nous allons passer directement aux séries de questions. Le premier tour sera de six minutes, et nous commençons par M. Lloyd. Monsieur Lloyd, la parole est à vous.

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

Je tiens à remercier tous les témoins de leur présence ici aujourd'hui et de leurs témoignages. Nous prenons note de ce que vous nous dites et nous tiendrons compte de vos interventions dans le cadre de notre examen du projet de loi.

Cependant, il y a un autre problème urgent auquel nous faisons face dans ce pays, et c'est le vol de voitures. Afin de permettre au Comité de continuer à travailler sur le projet de loi C-26, mais dans un souci d'efficience pour s'attaquer au problème urgent du vol d'automobiles au pays, j'ai l'intention de présenter la motion dont j'ai donné avis lors de la dernière réunion du Comité. Cependant, par suite de discussions avec les autres partis présents, nous avons proposé des amendements à cette motion, afin que le Comité puisse s'occuper simultanément du projet de loi C-26 et de l'enjeu très important du vol de voitures.

Nous savons qu'en 2022, la dernière année où des statistiques sur les assurances contre le vol d'automobiles ont été rendues publiques, les réclamations pour le vol d'automobiles ont totalisé 1,2 milliard de dollars. Nous savons que plus de 100 000 véhicules ont été volés au Canada l'an dernier. Il s'agit d'un problème qui va en s'aggravant. Le nombre de vols a augmenté de 50 % d'une année à l'autre dans les provinces de l'Ontario et du Québec. C'est un problème pancanadien, l'Alberta se classant au troisième rang pour ce qui est du vol de voitures. Il s'agit d'une question très importante dans la circonscription que je représente et je suis très inquiet.

Il faut éduquer les gens pour qu'ils sachent quels outils sont à leur disposition pour protéger leurs véhicules contre le vol. Cependant, en même temps, si le gouvernement fédéral ne prend pas de mesures pour sécuriser nos ports et mettre les récidivistes derrière les barreaux, je crains que nous ne voyions une augmentation de l'impudence de ces actes criminels, y compris de la violence contre nos citoyens, si des mesures ne sont pas immédiatement prises pour mettre immédiatement le holà sur ce flot sans précédent de véhicules de Canadiens qui quittent le pays, en particulier à partir du port de Montréal.

Je crois comprendre, monsieur le président, que mon collègue, Larry Brock, est le prochain intervenant sur la liste. Afin que ce comité puisse poursuivre son étude très importante du projet de loi C-26, tout comme l'étude qui a déjà été convenue par ce comité le 23 octobre, sur la motion de notre collègue du Bloc québécois, Mme Michaud, je vais céder la parole à mon collègue, M. Brock, afin qu'il puisse proposer l'amendement approprié.

Merci, monsieur le président.

● (0835)

Le président: Monsieur Brock. Je vous en prie.

M. Larry Brock (Brantford—Brant, PCC): Merci, monsieur le président.

Selon l'amendement proposé, tous les mots après le mot « Comité » dans le premier paragraphe...

M. Peter Julian (New Westminster—Burnaby, NPD): Monsieur le président, j'invoque le Règlement.

Le président: Monsieur Julian.

M. Peter Julian: Nous n'avons pas la motion. Il n'y a pas de motion, alors un amendement ne peut pas être proposé s'il n'y a pas de motion.

M. Dane Lloyd: J'ai proposé la motion dans mon intervention tout à l'heure.

Le président: Avez-vous proposé la motion?

M. Peter Julian: Non, il ne l'a pas fait.

M. Dane Lloyd: La motion a été distribuée au Comité. Elle a été distribuée mercredi.

M. Peter Julian: La motion n'a pas été proposée.

Le président: Pouvez-vous lire la motion, monsieur Lloyd?

M. Dane Lloyd: Oui, monsieur le président.

Le président: Merci.

M. Dane Lloyd: Monsieur le président, la motion originale se lit comme suit:

> Que le Comité fasse rapport à la Chambre de sa reconnaissance du fait que la convocation d'un Sommet national de politiciens et d'initiés pour discuter des vols d'autos ne permettra pas de prévenir ces vols. Il reconnaît également que la prévention des vols d'autos relève entièrement de la responsabilité fédérale de l'Agence des services frontaliers du Canada (ASFC), de la Gendarmerie royale du Canada (GRC), de Transports Canada et de Sécurité publique Canada.
>
> Et recommande à la Chambre que le gouvernement:
>
> A) Annule immédiatement les modifications apportées au projet de loi C-5, qui permet aux voleurs d'autos la détention à domicile au lieu de purger une peine d'emprisonnement.
>
> B) Renforce les dispositions du Code criminel pour s'assurer que les voleurs d'autos récidivistes restent en prison.
>
> C) Fournit à l'ASFC et à nos ports les ressources nécessaires pour empêcher les autos volées de quitter le pays.

C'est ma motion, monsieur le président.

M. Peter Julian: J'invoque le Règlement.

Le président: Oui, monsieur Julian.

M. Peter Julian: Monsieur le président, je dirais que cet amendement est irrecevable pour deux raisons.

La Chambre a déjà étudié hier une motion à peu près semblable, et le Parlement, la Chambre des communes, a décidé de ne pas y donner suite. Comme vous le savez, cela arrive très rarement, monsieur le président. Lorsqu'un projet de loi est rejeté, vous ne pouvez pas, le lendemain, suggérer en comité qu'il soit étudié. Dans ce cas-ci, il s'agissait d'une motion de l'opposition, et elle a été rejetée. Aujourd'hui, les conservateurs proposent essentiellement la même motion au Comité.

Il n'y a pas de précédent à cela, monsieur le président. Il est honteux que, lorsque le Parlement prend une décision, les membres du Comité essaient de revenir essentiellement sur le même sujet. Il est vrai que si cela se produisait dans trois ou quatre ans, on pourrait dire: « Eh bien, les choses ont considérablement changé depuis que le Parlement a examiné cette question, alors nous devrions en discuter davantage. » Dans ce cas-ci, c'était hier. C'est hier soir, il y a 14 heures, que le Parlement a décidé que la motion n'était pas pertinente.

J'ai proposé un amendement au nom du NPD, comme vous vous en souviendrez, monsieur le président, pour lutter contre le crime organisé et le blanchiment d'argent et rétablir les compressions dans les programmes de prévention du crime que le gouvernement Harper avait mis en place. Les conservateurs ont rejeté cette proposition, de sorte que la motion qui a été présentée hier à la Chambre était extrêmement faible et contenait beaucoup de désinformation. C'est pourquoi le Parlement l'a rejetée. Nous ne pouvons pas revenir le lendemain et examiner essentiellement la même motion.

Comme vous le voyez, monsieur le président, l'intention serait de faire une recommandation à la Chambre. Une décision a été prise par la Chambre. La motion d'aujourd'hui vise à recommander la même chose à la Chambre. Il y a un problème de répétition, celle-ci étant très clairement interdite dans tous nos manuels de procédures. On ne peut pas continuer à soulever la même question sous la même forme.

Deuxièmement, je dirais que, parce qu'il est question d'une recommandation à la Chambre, on essaie de faire indirectement ce qui est interdit directement. Autrement dit, on tente d'utiliser un comité pour réexaminer quelque chose qui l'a déjà été hier par la Chambre des communes.

Le président: Merci, monsieur Julian.

Nous allons suspendre la séance pendant quelques minutes pour que je puisse consulter le greffier.

● (0835)

_____(Pause)_____

● (0840)

Le président: Nous reprenons nos travaux.

Je prends en considération vos commentaires, monsieur Julian.

Après avoir parlé au greffier, je veux vous dire que la motion n'a pas été présentée au Comité avant... Je n'ai pas l'autre motion sous les yeux pour la comparer, alors mon pouvoir se limite essentiellement à dire que nous allons poursuivre l'étude de la motion et la maintenir pour l'instant.

M. Peter Julian: Monsieur le président...

M. Peter Schiefke (Vaudreuil—Soulanges, Lib.): Monsieur le président, je conteste cette décision.

Le président: Certainement.

M. Peter Julian: Vous m'avez devancé, monsieur Schiefke.

M. Peter Schiefke: Je suis désolé. Je trouve cela ridicule.

Le président: Monsieur Julian, voulez-vous intervenir ensuite? Je vous ai donné l'occasion de le faire. Vous étiez à peu près les deux en même temps.

M. Peter Julian: J'espère que nous pourrons voter là-dessus.

Nos témoins nous ont donné énormément de contenu, et j'ai des tonnes de questions. Très franchement, je suis un peu frustré par toutes les perturbations que les conservateurs ont causées au cours des dernières réunions sur un autre sujet, qu'ils ont ensuite décidé de laisser tomber pour essayer de passer à celui-ci.

Il est temps de commencer à poser des questions aux témoins.

M. Dane Lloyd: Est-ce un rappel au Règlement?

Le président: La décision de la présidence est contestée. Nous aurons un vote par appel nominal.

(La décision de la présidence est rejetée par 6 voix contre 5.)

Le président: La décision de la présidence a été rejetée.

Nous passons maintenant à...

● (0845)

M. Peter Julian: Monsieur le président, je propose que nous utilisions le temps dont nous disposons pour poser des questions aux témoins, qui nous ont livré des témoignages très importants.

Le président: C'est le processus, oui.

Monsieur Bittle, vous avez la parole. Je vous en prie.

M. Chris Bittle (St. Catharines, Lib.): C'est excellent. Merci beaucoup.

Merci beaucoup aux témoins d'être ici.

Il est vraiment décevant de voir que, sur des questions aussi importantes, les conservateurs tentent encore une fois de détourner l'attention, alors qu'ils prétendent se soucier de la sécurité.

Monsieur de Boer, vous avez parlé de déclaration obligatoire, non seulement ici, mais aussi en ce qui concerne le décret aux États-Unis. Le projet de loi C-26 exige que les secteurs touchés soient tenus de signaler tout incident de cybersécurité. Croyez-vous que c'est important, et si oui, pourquoi?

M. John de Boer: Par l'entremise du président, je vous remercie de la question.

Oui, c'est très important. En plus du décret, les États-Unis ont également adopté une loi distincte en 2022 l'exigeant. La raison pour laquelle c'est important, c'est que les infrastructures essentielles ont une incidence sur la vie de tous les Canadiens. Nous dépendons d'elles. Notre économie dépend d'elles. Il s'agit de notre sécurité économique et de notre sécurité nationale, et il serait important d'exiger que les entités signalent ces incidents dans un délai raisonnable — et je suggère d'harmoniser cela avec les États-Unis et l'Union européenne, où il est prévu de le faire dans les 72 heures. C'est fondamental.

M. Chris Bittle: Monsieur de Boer, M. Bradley a soulevé certaines préoccupations au sujet des rapports. Partagez-vous ces préoccupations?

M. John de Boer: Absolument. Je suis tout à fait d'accord pour dire qu'il faut assurer une protection au niveau de la responsabilité. Il faut aussi qu'il y ait une obligation de diligence raisonnable. Essentiellement, s'il y a eu des tentatives de bonne foi de signaler des incidents de cybersécurité ou de mettre en place des mesures de cyberprotection pour les prévenir, cela doit être respecté.

Nous avons affaire à des auteurs très aguerris. Le rapport publié hier par le gouvernement des États-Unis parle d'un auteur soutenu par la Chine qui agissait dans des infrastructures essentielles depuis neuf mois. Ces gens sont très rusés.

Nous devons travailler en équipe. J'appuie également ces amendements.

M. Chris Bittle: Merci beaucoup.

Madame Quaid, quelles sont les mesures de protection actuellement en place pour veiller à ce que nos fournisseurs d'infrastructures essentielles prennent des mesures pour s'assurer que leurs systèmes sont suffisants pour contrer les cyberattaques lancées par des organisations criminelles et des adversaires internationaux?

Mme Jennifer Quaid: Nos secteurs des infrastructures essentielles sont peut-être parmi les plus sophistiqués. Ils ont certaines des cyberdéfenses les plus avancées de tout le Canada, et ils s'alignent de très près sur les mêmes secteurs dans d'autres pays, particulièrement du côté de l'électricité, en raison des activités transfrontalières, de même que des finances et des télécommunications.

Quels sont les systèmes en place pour garantir cela? Leurs organismes de réglementation font preuve d'une diligence extraordinaire — ce qui me semble le bon mot — pour s'assurer qu'ils sont alignés et qu'ils ont de solides défenses en place.

Il n'y a vraiment rien que nous puissions ajouter à ce que les organismes de réglementation ont proposé, mais ces dispositions sont importantes parce que, pour faire suite à ce que M. de Boer disait, la production de rapports est l'un de nos plus grands défis. Nous n'avons pas de chiffres exacts. Nous ne savons pas quelle est l'ampleur du problème au Canada, parce que les méthodes de rapport diffèrent. Ce qui est défini comme un cyberincident est perçu différemment dans différents rapports, c'est-à-dire qui doit le signaler, quand cela doit être fait et ce qui est signalé. Nous n'avons pas de chiffres fiables, et cela fait partie de notre problème.

M. Chris Bittle: Quels seraient les risques, si le projet de loi n'était pas adopté ou si son adoption était trop retardée?

● (0850)

Mme Jennifer Quaid: Les risques sont énormes. Tout d'abord, nous perdrons la confiance de nos partenaires du Groupe des cinq. Nous perdrons la confiance qui règne dans les relations transfrontalières que nous avons avec la NERC, c'est-à-dire la North American Electric Reliability Corporation, la FERC, ou Federal Energy Regulatory Commission, et toutes les autres entités. Nous perdrons aussi des ressources et des revenus.

M. Chris Bittle: Merci beaucoup.

Selon vous, le projet de loi établit-il un juste équilibre en ne visant que les entreprises jugées essentielles à la sécurité nationale?

Mme Jennifer Quaid: Dans mon exposé, j'ai parlé du reste de l'économie.

En vérité, une grande partie du reste de l'économie soutient ces six secteurs: la chaîne d'approvisionnement, qui est visée par le projet de loi. Les infrastructures essentielles doivent maintenant connaître leur chaîne d'approvisionnement et assumer la responsabilité de ses signalements. Cela vaut pour toute la chaîne. C'est un très bon début.

M. Chris Bittle: Merci.

Monsieur Bradley, pour que ce régime soit une réussite, j'espère que vous conviendrez tous que les exploitants désignés doivent avoir l'assurance que les renseignements commerciaux confidentiels qu'ils fournissent au gouvernement sont traités correctement. Êtes-vous d'accord?

M. Francis Bradley: Oui.

M. Chris Bittle: Le projet de loi comprend actuellement un régime visant à protéger les renseignements confidentiels. Que pensez-vous du régime qu'il propose?

M. Francis Bradley: Ce qui nous préoccupe, c'est plutôt le fait que diverses entités au sein du gouvernement du Canada, en particulier le Centre canadien pour la cybersécurité, abordent différemment la protection et l'utilisation de l'information. Voilà ce qui nous préoccupe au premier chef au sujet de l'utilisation de l'information elle-même.

M. Chris Bittle: Merci beaucoup.

Le président: Madame Normandin, vous avez six minutes. Je vous en prie.

[*Français*]

Mme Christine Normandin (Saint-Jean, BQ): Merci, monsieur le président.

Je remercie également l'ensemble des témoins de leur présence très appréciée.

Je m'adresserai d'abord à M. Bradley.

Vous avez parlé du risque que la réglementation fasse double emploi avec la North American Electricity Reliability Corporation. Je me demandais si, à d'autres paliers, il y avait aussi ce risque de double emploi. Je sais que vous avez eu des discussions, notamment avec Hydro-Québec, avant de venir faire votre présentation. Ce genre de craintes a-t-il été mentionné pour ce qui est de la réglementation du Québec en matière de protection des renseignements personnels, par exemple?

Existe-t-il un risque qu'il y ait non seulement un double emploi, mais triple emploi dans certains aspects de la réglementation?

M. Francis Bradley: Je vous remercie beaucoup.

[*Traduction*]

Excellente question.

Mes observations et notre mémoire portent plus particulièrement sur l'interface entre le projet de loi et les exigences de la NERC, qui sont très lourdes. La députée a tout à fait raison. Il y a d'autres exigences qui entrent en jeu au niveau des différents ordres de gouvernement, ainsi qu'à l'échelle internationale. Il n'y a pas que le fait que le projet de loi C-26 entre en conflit avec la NERC. Il faut tenir compte d'autres niveaux également.

Ce qui nous préoccupe plus particulièrement, c'est le manque d'harmonisation entre les exigences de la NERC, qui existent depuis de nombreuses années, et ce qui est proposé dans le projet de loi C-26.

[*Français*]

Mme Christine Normandin: Merci beaucoup. Cela m'amène à poser une question à M. de Boer.

Vous avez également parlé de l'harmonisation. J'aimerais que vous nous parliez du Groupe des cinq et de l'harmonisation du rapport d'incident sur le plan international.

Il y a des normes à plusieurs paliers et cela devient extrêmement complexe. À quel palier l'harmonisation devrait-elle se faire en priorité, et pourquoi?

[*Traduction*]

M. John de Boer: Je recommanderais que nous nous alignions sur les États-Unis.

Comme je l'ai déjà dit, même le Centre canadien pour la cybersécurité a fait remarquer qu'un incident touchant les infrastructures essentielles aux États-Unis aurait des répercussions au Canada. Une grande partie de nos infrastructures essentielles — qu'il s'agisse de l'énergie, du transport ferroviaire ou, dans certains cas, des télécommunications — chevauchent les frontières. Nous devons nous aligner sur les États-Unis. C'est ce que je ferais: une exigence de signalement sous 72 heures.

Il faut aussi harmoniser nos définitions de la notion d'incident cybernétique. En ce moment, les États-Unis entreprennent une étude, confiée au CISA, soit l'auditeur informatique agréé, pour définir ce qu'est un « incident cybernétique » et cerner ce qui doit être signalé. Les États-Unis ont 52 régimes différents de signalement. Imaginons qu'une entité qui s'occupe d'un incident de cybersécurité soit tenue de signaler à 10 ou 15 entités différentes divers types d'incidents cybernétiques.

En l'absence d'harmonisation, le projet de loi, loin de régler le problème, contribuera à l'aggraver.

● (0855)

[*Français*]

Mme Christine Normandin: Merci beaucoup.

Madame Quaid, vous avez fait une recommandation visant à ouvrir davantage le projet de loi afin qu'il traite de la collaboration volontaire des entreprises. Cela impliquerait, par contre, un besoin de main-d'œuvre plus élevé pour mettre en œuvre le projet de loi C-26.

Cela a-t-il fait partie de vos réflexions? Le fait qu'il y ait une pénurie de main-d'œuvre généralisée constitue-t-il un problème potentiel? J'ai posé la question au Comité un peu plus tôt, et au Centre de la sécurité des télécommunications CST. On m'a confirmé que cela pouvait être un problème.

J'aimerais savoir si c'en est un pour vous aussi et si vous avez des pistes de solution pour le régler dans l'éventualité d'une réponse positive.

[*Traduction*]

Mme Jennifer Quaid: Je vous remercie de la question. Je suis très heureuse que nous puissions nous attaquer au problème de pénurie de main-d'œuvre.

J'ai proposé de permettre aux organisations au Canada de signaler les menaces, les attaques et les incidents, d'en parler publiquement et de donner de l'information à ce sujet sans que leur responsabilité légale soit engagée. Nous atténuerions ainsi l'impact sur la main-d'œuvre. Comme les entreprises pourraient échanger des renseignements, elles n'auraient pas toutes besoin d'avoir des spécialistes qui font exactement la même chose, et les petites organisations pourraient apprendre auprès des plus grandes comment se protéger avant une attaque.

J'espère qu'en permettant une collaboration plus étendue qui ne se limiterait pas au gouvernement, à l'abri de toute crainte d'engager leur responsabilité légale, nous aurons en fait un effet positif sans ajouter aux besoins en main-d'œuvre.

[*Français*]

Mme Christine Normandin: Merci beaucoup.

J'aimerais entendre toute personne qui veut aborder de la question de la responsabilité, quitte à ce qu'il y ait un deuxième tour.

Je crains que, si on élimine complètement la responsabilité des grandes entreprises, qui ont pourtant le potentiel d'avoir une équipe pour s'assurer de bien faire le travail, elles puissent se dédouaner, d'une certaine façon, de l'impression qu'elles ont de vouloir bien respecter le projet de loi C-26.

Risque-t-on d'enlever complètement l'idée de la responsabilité?

[*Traduction*]

Mme Jennifer Quaid: Mon collègue, Francis Bradley, a parlé d'une loi d'exonération, comme il y en a une aux États-Unis. C'est ce qu'ont les Américains. En rédigeant soigneusement une disposition semblable à ce qui existe aux États-Unis, nous trouverons cet équilibre délicat que nous recherchons toujours. On ne veut jamais éliminer toute responsabilité, mais on veut certainement soustraire les dirigeants principaux de la sécurité de l'information, qui sont très peu nombreux. L'un des témoins de la semaine dernière a dit que 75 % d'entre eux sont en train de partir.

Nous sommes exposés à des risques, mais il me semble possible, par un libellé bien étudié, de parvenir à un équilibre qui, sans éliminer toute responsabilité, protège les organisations de responsabilités légales lorsqu'elles tentent de communiquer de l'information pour protéger d'autres entités.

Le président: Merci, madame Normandin.

Monsieur Julian, vous avez la parole. Six minutes.

M. Peter Julian: Merci beaucoup, monsieur le président.

Merci aux témoins. Vous nous avez donné beaucoup de matière à réflexion. J'ai une foule de questions. J'espère qu'il n'y aura pas d'autres perturbations parce que, très franchement, mes collègues conservateurs n'ont pas encore posé une seule question sur le projet de loi C-26, et cela doit changer. Le projet de loi à l'étude est important.

J'ai deux questions à vous poser à tous les trois.

Tout d'abord, madame Quaid, vous avez dit que d'autres retards nous feraient perdre la confiance de nos partenaires. Le gouvernement a présenté le projet de loi en juin 2022. Nous sommes maintenant en février 2024. L'opposition officielle retarde et perturbe le processus législatif. Outre la perte de la confiance de nos partenaires, quelles sont les autres conséquences? D'autres témoins nous ont dit que, essentiellement, le Canada est de plus en plus ciblé par des attaques parce qu'il n'a pas de loi en place. Quelles sont les conséquences d'un retard prolongé? Ma question s'adresse à vous trois.

Ma deuxième question porte sur votre excellent mémoire, monsieur Bradley, au sujet de la consultation pendant le processus de réglementation. Jusqu'à maintenant, dans quelle mesure le gouvernement a-t-il consulté l'industrie au sujet du projet de loi? Dans quelle mesure y a-t-il eu des consultations pour faire en sorte que nous adoptions un bon projet de loi?

Je vais commencer par M. Bradley, qui sera suivi de M. de Boer et de Mme Quaid.

M. Francis Bradley: Merci beaucoup. Ce sont deux excellentes questions.

À propos de la première, portant sur les conséquences du retard — et il y a aussi un lien avec votre deuxième question —, nous avons entamé des discussions au sujet de cette lacune. Depuis une quinzaine d'années, notre secteur a des normes obligatoires de fiabilité et de protection des infrastructures essentielles. Nous nous sommes demandé ce qu'il en était dans les autres secteurs sur lesquels nous devons compter, puisqu'il y a interdépendance entre les secteurs. Certains ont des programmes robustes. D'autres, nous n'en savons rien.

Nous préconisons un dispositif plus important qui s'applique à différentes infrastructures essentielles, aux autres infrastructures dont nous dépendons. Nous avons une très grande confiance dans notre régime parce qu'il est d'application obligatoire et exécutoire. Nous souhaitons que quelque chose soit mis en place, et nous discutons avec le gouvernement depuis très longtemps au sujet des autres secteurs sur lesquels nous devons compter.

Le projet de loi C-26 comble cette lacune. Il y a chevauchement. J'en ai parlé dans mon exposé. La consultation? Nous discutons de la question avec divers organismes et ministères depuis plus de dix ans. Nous avons été largement consultés, bien sûr, mais il s'agit d'une lacune qui existe depuis un bon moment.

● (0900)

M. Peter Julian: À vous, monsieur de Boer.

M. John de Boer: Oui, j'abonde dans le même sens.

Les infrastructures essentielles sont ainsi qualifiées parce qu'elles sont indispensables dans notre vie quotidienne et le fonctionnement de notre économie. Elles sont essentielles, mais il y a autre chose. Si le public croit que le gouvernement n'a pas fait le nécessaire pour protéger les infrastructures essentielles et protéger nos vies, c'est la confiance même envers lui qui pourrait s'effriter.

L'abordabilité est un autre impact possible. Les cyberattaques alourdissent les coûts. À l'heure actuelle, il y a des pays — notamment le Royaume-Uni — où les assureurs refusent les entités qui ont été attaquées par un acteur parrainé par l'État. Tous ces coûts sont refilés aux consommateurs. Ce pourrait donc être aussi...

M. Peter Julian: Puis-je vous interrompre par une question? L'un de vous trois a-t-il des chiffres à nous donner sur les coûts, sur la hausse des coûts attribuable à l'absence de mesures à ce stade-ci?

M. John de Boer: Je peux vous en communiquer plus tard, en tout cas au sujet de l'augmentation des primes d'assurance et de l'abordabilité. Je peux trouver quelques chiffres pour le Comité.

Il y a toute une série de conséquences énormes qui sont fondamentales pour notre économie. Il suffit par exemple de voir ce qui se passe en Ukraine. Son réseau électrique a été paralysé. Prenez le cas d'Oldsmar, en Floride, où une cyberattaque a failli empoisonner le réseau d'alimentation en eau. On peut aboutir à des conséquences catastrophiques.

Des consultations, il y en a eu. Ce qui nous impatiente, c'est que le dossier a progressé bien trop lentement. Il faut aussi le considérer en tenant compte de la Stratégie nationale sur les infrastructures essentielles, qui n'a pas été mise à jour depuis 2009. Il faut harmoniser la définition d'infrastructure essentielle avec les entités qui exploitent des infrastructures essentielles, décrites dans le projet de loi, ce qui relève de la responsabilité de Sécurité publique Canada.

M. Peter Julian: Madame Quaid, je reviendrai à vous, mais vous serez malheureusement interrompue.

Mme Jennifer Quaid: D'accord. Je serai très brève.

Quelles seront les conséquences si le projet de loi n'est pas adopté? Voyez ce qui est arrivé au gazoduc Colonial. L'incident a entraîné au moins un décès confirmé. Quelles sont les conséquences? La mort. C'est simple. Si le gaz ne circule pas, si les systèmes téléphoniques ne fonctionnent pas, des gens ne survivront pas.

Il y a aussi les impacts supplémentaires, ainsi que le disait M. de Boer, comme la hausse des primes d'assurance. Il est de plus en plus difficile de souscrire une assurance. Ma propre prime de cyberassurance a augmenté de façon exponentielle, ce qui entraîne des coûts. Je devrai les répercuter sur les clients. Il coûte plus cher de faire des affaires. Des entreprises vont disparaître. Les petites et moyennes entreprises n'ont pas les moyens de subir une cyberattaque. Pour s'en remettre, il en coûte habituellement des millions. Il faut récupérer ces coûts quelque part.

Quant à la collaboration, si vous me le permettez...

Le président: Merci, monsieur Julian et madame Quaid.

M. Peter Julian: Je vous reviendrai.

Le président: Je suis sûr que vous aurez une autre occasion.

Voilà pour le premier tour. Nous passons maintenant au deuxième.

Monsieur Motz, vous avez cinq minutes.

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

Je remercie les témoins d'être là.

On l'a dit, cette mesure est pressante. Nous attendons depuis juin 2022, date à laquelle le projet a été présenté, et c'est encore la valse-hésitation.

Des témoins ont dit, jusqu'à maintenant, que nous devons nous demander ce qui est le plus important: précipiter l'adoption du projet de loi même s'il est défectueux, ou essayer au moins de le corriger pour en faire une mesure applicable et parvenir à faire quelques petites choses correctement. Je vous invite tous à donner vos réactions.

Je voudrais aussi que, dans cette réponse... Des témoins ont également déploré que le projet de loi soit vague à bien des égards et que l'on compte sur la réglementation pour combler les lacunes. On a recommandé l'ajout de définitions, un libellé différent qui clarifie le projet de loi, au lieu de s'en remettre à la réglementation, ce qui pourrait prendre encore un ou deux ans. C'est ce qui nous préoccupe tous.

Qu'en pensez-vous? Je vais commencer par vous, madame Quaid.

● (0905)

Mme Jennifer Quaid: Il faut trouver le juste équilibre. Le projet de loi est important, c'est incontestable. Il ne fait aucun doute non plus qu'il faut le modifier. Avec un peu d'effort, il est possible de le corriger suffisamment pour en faire une bonne loi, quitte à préciser les détails dans la réglementation. Avec de la concentration et des efforts, nous pouvons faire les choses correctement et tout de suite.

M. Glen Motz: Monsieur de Boer, à vous.

M. John de Boer: Je suis tout à fait d'accord. Nous devons agir dès maintenant.

Le projet de loi ne sera jamais parfait, mais il faut apporter les rajustements que nous avons proposés. Ils visent à préciser ce qui est considéré comme un cyberincident et à harmoniser la définition avec celle des États-Unis. Cela vaut aussi pour les délais de signalement. En temps de crise, il est vraiment essentiel que tout soit clair. Voilà donc ce qu'il faut faire.

Ce sont des solutions faciles. Il suffit probablement de quelques modifications. Je comblerais ces lacunes, je ferais adopter le projet de loi et je continuerais à travailler à d'autres éléments.

M. Glen Motz: Merci.

Monsieur Bradley, votre tour.

M. Francis Bradley: Merci beaucoup.

Monsieur le président, la question est excellente. Devons-nous adopter le projet de loi à la hâte ou le modifier pour qu'il soit bon? Je vous répondrai qu'il faut faire les deux. Adoptons ce projet de loi à toute vapeur, tout en tenant compte des 14 recommandations que nous avons formulées et en apportant les amendements qui leur donnent suite.

M. Glen Motz: Merci.

Je vais continuer avec vous, monsieur Bradley.

Vous avez écrit dans votre mémoire que le projet de loi risque d'améliorer fort peu la sécurité pour notre secteur. C'est quelque peu troublant. Il est certain que notre réseau électrique, avec un approvisionnement fiable en électricité, figure parmi les infrastructures les plus essentielles. Vous dites ensuite que le projet de loi devrait fournir des outils et des protocoles pour accroître la sécurité du secteur canadien des infrastructures. Quels sont ces protocoles et outils, si vous ne l'avez pas déjà précisé dans votre exposé liminaire?

M. Francis Bradley: Merci beaucoup.

Si le projet de loi C-26 n'améliore pas nettement la sécurité et s'il risque de faire diversion, ce n'est pas à cause de ce qu'il est en soi. C'est parce que la barre a été placée plus haut par les normes obligatoires auxquelles notre secteur est déjà assujetti dans le régime de la North American Electric Reliability Corporation. La barre est déjà placée plus haut.

Le projet de loi C-26 n'apporte aucune amélioration par rapport à ces normes. Il fait diversion. Il détourne l'attention vers une deuxième structure de signalement distincte au lieu d'utiliser ces ressources pour élaborer une réponse.

M. Glen Motz: D'accord. Merci.

Monsieur de Boer, la Chambre de commerce du Canada a fait remarquer qu'un ensemble de mesures disparates désavantagerait les entreprises si nous ne nous y prenons pas correctement. BlackBerry a produit un livre blanc en 2022. Le plus gros obstacle que vous avez relevé, et qui a déjà été signalé brièvement, c'est le manque de personnel qualifié et de ressources compétentes pour lutter contre ce problème au niveau des infrastructures essentielles d'abord, puis peut-être dans un contexte de menace plus vaste.

La situation a-t-elle évolué depuis 2022, depuis la rédaction du livre blanc?

M. John de Boer: Je copréside également, avec la Chambre de commerce du Canada, le programme « Cyber. Right. Now. » Par conséquent...

Le président: Je suis désolé de vous interrompre, mais je dois vous brusquer. Nous allons manquer de temps, et je veux m'assurer que tout le monde a l'occasion d'intervenir.

Monsieur Gaheer, vous avez la parole.

● (0910)

M. Iqwinder Gaheer (Mississauga—Malton, Lib.): Merci, monsieur le président.

Merci à tous les témoins d'avoir pris le temps de venir nous rencontrer.

Mes questions s'adressent surtout à M. Bradley, d'Électricité Canada.

Combien d'organisations votre organisation représente-t-elle?

M. Francis Bradley: Quarante entreprises en sont les membres principaux. On remarque parmi elles aussi bien les plus grandes entreprises d'électricité au Canada, comme Hydro-Québec, que des services publics municipaux ontariens.

M. Iqwinder Gaheer: Combien ont actuellement un programme de cybersécurité?

M. Francis Bradley: Tous.

M. Iqwinder Gaheer: Je suppose qu'il y a des différences entre les divers programmes.

M. Francis Bradley: Absolument. Selon la taille de l'organisation, il doit y avoir des différences, évidemment, mais tous ceux qui participent au système de production-transport d'électricité sont assujettis aux normes obligatoires de cybersécurité de la North American Electric Reliability Corporation. Par conséquent, ces entreprises ont des programmes de cybersécurité très robustes et cohérents.

M. Iqwinder Gaheer: D'accord.

Quelles sont les conséquences d'une cyberattaque réussie contre un exploitant d'infrastructure essentielle dans le secteur de l'énergie?

M. Francis Bradley: Comme l'a déjà dit ce groupe de témoins... Il ne s'agit pas du Canada, mais d'autres pays. Aux États-Unis, un pipeline est devenu inutilisable. En Ukraine, en 2015, pour la première fois au monde, nous avons été témoins d'une cyberattaque qui a fait perdre l'électricité aux abonnés. Ce n'est jamais arrivé chez nous, mais ce sont les conséquences que les cyberattaques peuvent avoir.

M. Iqwinder Gaheer: Évidemment, c'est un secteur tout à fait vital. Tous ceux qui sont ici présents doivent le comprendre. C'est pourquoi j'ai été un peu étonné lorsque, dans votre exposé liminaire, vous vous êtes prononcé contre les exigences obligatoires du projet de loi et contre le signalement immédiat.

Dans son témoignage, Mme Quaid a dit que les modalités de signalement varient et que les données ne sont pas fiables. Qu'en pensez-vous?

M. Francis Bradley: Lorsqu'un cyberincident survient, voulons-nous que notre personnel fasse des rapports pour les organismes de réglementation ou voulons-nous qu'il s'occupe de sécuriser les systèmes? D'abord et avant tout, nous voulons qu'il sécurise les systèmes, quitte à répondre ensuite aux exigences en matière de rapports.

Il s'agit d'abord et avant tout d'alléger le fardeau des rapports et de la réglementation. Deuxièmement, je m'inquiète du double emploi. Nous avons déjà des exigences en matière de signalement. Il est aussi question d'instaurer un deuxième régime de signalement.

M. Iqwinder Gaheer: Vous avez dit que cet autre régime obéit en fait à une norme plus élevée. Ne serait-il pas plus facile de respecter la norme inférieure proposée dans le projet de loi?

M. Francis Bradley: Oui, sauf que, si les définitions sont différentes, il faut avoir une structure de signalement distincte et utiliser des définitions différentes.

Il y a quelques années, lorsque le gouvernement a commencé à s'engager dans cette voie, j'ai dit, pas tout à fait à la blague, qu'il pourrait peut-être examiner les normes de cybersécurité de la NERC et envisager de les appliquer aux infrastructures essentielles d'autres secteurs au Canada. Cela nous aurait certainement facilité la vie si nous avions étudié le régime en place et envisagé de l'appliquer à d'autres secteurs.

M. Iqwinder Gaheer: Vous conviendrez sans doute, qu'il s'agisse de ce régime ou d'un autre, que les exigences de signalement obligatoire sont importantes, tout comme la collecte de renseignements.

M. Francis Bradley: Absolument.

M. Iqwinder Gaheer: Merci, monsieur le président.

Le président: Madame Normandin, vous avez deux minutes et demie.

[*Français*]

Mme Christine Normandin: Merci beaucoup, monsieur le président.

Ma question s'adresse à l'ensemble des témoins. J'aimerais qu'ils se sentent libres d'y répondre.

Le projet de loi C-26 établit un genre d'équilibre entre ce qui est déjà codifié par le projet de loi et l'aspect réglementaire. Je comprends que beaucoup de définitions vont émaner des règlements, des sanctions, de toutes les personnes visées, et ainsi de suite.

On sait que la cybernétique est un monde qui évolue très rapidement. Le fait de réglementer une bonne partie du secteur peut apporter une certaine flexibilité, mais cela peut aussi être un frein pour ce qui est de tenir à jour les plus petites entreprises et de les mettre au courant de ce qui se passe.

J'aimerais que vous nous parliez de cet équilibre entre les deux.

[*Traduction*]

M. John de Boer: Il reste encore à élucider quelques questions de définition. Si on veut préserver un juste équilibre en matière de sanctions et d'amendes, par exemple, il faut prévoir certaines conséquences dans les cas de négligence, lorsqu'une partie n'applique pas une norme fondamentale de cybersécurité.

Il faut aussi encourager les grandes entités qui exploitent des infrastructures essentielles à assurer la sécurité de leur chaîne d'approvisionnement, ce qui nécessite une étroite collaboration avec les PME.

J'ajouterais qu'aux États-Unis, le gouvernement a instauré un programme de subventions pour permettre aux entités responsables des infrastructures essentielles de mettre en place des exigences de base en matière de cybersécurité. Ce pourrait être une autre idée.

Enfin, à propos de juste équilibre, la loi doit privilégier la prévention. C'est ce qu'on fait en médecine. Il vaut mieux prévenir que guérir. Il est préférable d'investir dès le départ.

● (0915)

Mme Jennifer Quaid: Puis-je revenir sur les propos de M. de Boer au sujet des incitatifs pour les petites et moyennes organisations? Si nous permettons aux grandes organisations de les renseigner ouvertement, honnêtement et pleinement sur ce qu'elles observent et font, et les soutenir pour leur éviter d'être frappées par la même attaque, nous appliquerons ce principe: il vaut mieux prévenir que guérir. Ce sera utile.

Nous pourrions aussi encourager les entreprises qui ne sont pas nécessairement visées par le projet de loi — c'est un élément distinct —, mais qui font partie de la chaîne d'approvisionnement. Nous pouvons inciter les maillons de la chaîne d'approvisionnement à atteindre un niveau de maturité cybernétique au moyen d'incitatifs fiscaux ou d'allégements en matière d'assurance, s'ils ont des certifications.

Le président: Merci, madame Normandin.

M. Julian posera les dernières questions. Je vous en prie.

M. Peter Julian: Merci, monsieur le président.

Je tiens à féliciter M. Motz d'avoir posé la première question des conservateurs au sujet du projet de loi C-26, un mois après le début de son étude.

Je reviens à vous, madame Quaid, au sujet des consultations.

Il faut aussi se demander si nous sommes de plus en plus ciblés parce que nous ne faisons rien et tardons à adopter des mesures législatives importantes.

Ma troisième question porte sur votre recommandation concernant les dépenses liées à l'adhésion à Échange canadien de menaces cybernétiques, si j'ai bien compris. Quels sont les coûts? Vous avez dit qu'il n'y en avait pas, mais je suis sûr qu'il doit y en avoir. Avez-vous évalué les coûts et les avantages?

Trois questions pour une intervention de deux minutes.

Mme Jennifer Quaid: Je répondrai d'abord à la dernière, qui porte sur l'adhésion à Échange canadien de menaces cybernétiques.

En fait, j'ai parlé d'une organisation canadienne de cybercollaboration. Pas nécessairement la nôtre, même si ce serait merveilleux. En disant qu'il n'y avait pas de coûts, je pensais au gouvernement. Il n'y en a pas pour lui parce que cela s'inscrirait dans le programme des retombées industrielles et technologiques. Toute organisation ou entreprise qui travaille dans le cadre de ce programme ou est touchée par lui pourrait se joindre à une association de lutte contre les menaces, afin de mieux se renseigner sur ce qui se passe dans le cyberécosystème, comme sur les vecteurs d'attaque probables et les solutions en matière de rétablissement et de résilience.

C'est le premier point. Cela ne coûte rien au gouvernement. Il y a un coût pour nous, mais il est nominal pour les petites entreprises. C'est vraiment modique.

L'autre question que vous avez posée avant portait sur la consultation.

M. Peter Julian: Sur le processus de consultation.

Mme Jennifer Quaid: Il y a certainement eu des consultations il y a plusieurs années. Nous y avons également participé avec nos membres, parce que nous avons communiqué avec eux. Il y a eu des consultations en cascade, pour ainsi dire, mais il serait bien que le projet de loi C-26 aille de pair avec une stratégie nationale en matière de cybersécurité.

La consultation a eu lieu il y a plusieurs années et elle accuse maintenant un retard de deux ans. Je vois cela venir.

Quelle était la troisième question?

M. Peter Julian: Est-il vrai que, comme certains témoins l'ont dit, le Canada est de plus en plus ciblé parce qu'il n'a pas mis en place des mesures de cybersécurité?

Mme Jennifer Quaid: C'est peut-être un peu brutal. Le Canada est de plus en plus ciblé parce qu'il paie les rançons. Il y a des pays qui ne se font pas attaquer parce qu'ils ne versent pas de rançon. Généralement, le Canada paie...

Le président: Merci, madame Quaid.

Monsieur Julian, votre temps de parole est écoulé.

Merci beaucoup aux témoins d'avoir comparu pour discuter d'un sujet très important.

Nous allons suspendre la séance...

M. Glen Motz: Monsieur le président, puis-je poser une question aux témoins?

Si les questions posées aujourd'hui vous font penser à autre chose dont vous voudriez traiter plus à fond, auriez-vous l'obligeance de communiquer vos réponses au Comité pour qu'il en tire parti dans ses délibérations et son rapport?

Merci.

Le président: Merci.

Nous allons suspendre la séance pendant cinq minutes pour nous préparer à accueillir un autre groupe de témoins.

Merci beaucoup d'avoir comparu.

● (0915)

_____(Pause)_____

● (0925)

Le président: Je souhaite la bienvenue à notre deuxième groupe de témoins.

Par vidéoconférence, de la Régie de l'énergie du Canada, nous accueillons Chris Loewen, premier vice-président, Réglementation, et Christopher Finley, directeur, Gestion des urgences et sécurité.

Nous accueillons en personne, du Conseil de la radiodiffusion et des télécommunications canadiennes, Steven Harroun, chef de l'application de la Conformité et enquête, Anthony McIntyre, avocat général et sous-directeur exécutif, Services juridiques; et Leila Wright, directrice exécutive, Télécommunications.

Nous allons accorder jusqu'à cinq minutes pour les déclarations liminaires, après quoi nous passerons aux questions. Bienvenue à tous.

J'invite maintenant M. Loewen à faire sa déclaration liminaire. Je vous en prie.

M. Chris Loewen (premier vice-président, Réglementation, Régie de l'énergie du Canada): Bonjour.

Je m'appelle Chris Loewen. Je suis premier vice-président, Réglementation, à la Régie canadienne de l'énergie. Je suis accompagné de M. Chris Finley, directeur, Gestion des urgences et sécurité.

Je vous remercie d'avoir invité la Régie de l'énergie du Canada à témoigner au sujet du projet de loi C-26.

Nous nous joignons à cette réunion depuis Calgary. Je souhaite profiter de l'occasion pour reconnaître les territoires traditionnels des peuples de la région du Traité n^{o} 7 dans le Sud de l'Alberta.

[*Français*]

J'aimerais d'abord vous présenter un aperçu du mandat de la Régie de l'énergie du Canada.

La Régie travaille à réglementer les infrastructures afin d'assurer l'acheminement sécuritaire et efficace de l'énergie partout au pays et ailleurs dans le monde. Elle réglemente les pipelines, les lignes de transport d'électricité, la mise en valeur des ressources énergétiques et le commerce de l'énergie au nom de la population canadienne de manière à protéger le public et l'environnement tout en favorisant l'efficience des marchés.

[*Traduction*]

La sécurité est au cœur de notre travail qui consiste à réglementer pour prévenir les préjudices sous toutes leurs formes, ce qui s'entend des menaces à la cybersécurité que le projet de loi C-26 vise à contrer. La Régie canadienne de l'énergie prend très au sérieux les menaces à la cybersécurité qui pèsent sur l'approvisionnement énergétique du Canada.

La Régie canadienne de l'énergie, la RCE, supervise quelque 71 000 kilomètres d'oléoducs et de gazoducs au Canada et réglemente les sociétés dont les pipelines traversent les frontières provinciales ou la frontière canado-américaine. Les sociétés pipelinières réglementées par la Régie sont tenues de mettre en place des mesures proactives pour protéger ces infrastructures essentielles contre les cybermenaces.

Les sociétés réglementées doivent disposer d'un programme de gestion de la sûreté visant à prévenir, à gérer et à contrôler les situations qui touchent directement les personnes, les biens et l'environnement. De plus, en ce qui concerne les menaces physiques à l'infrastructure, les entreprises doivent tenir compte de la cybersécurité dans leur programme de gestion de la sécurité et mettre en œuvre des mesures d'atténuation appropriées en fonction des résultats d'un processus d'évaluation des risques pour la sécurité. Ces exigences sont énoncées dans la norme Z246.1 de l'Association canadienne des normes, laquelle est incluse par renvoi dans le Règlement sur les pipelines terrestres découlant de la loi régissant la REC.

Les mesures de cybersécurité doivent refléter le caractère essentiel des actifs cybernétiques, ainsi que les résultats des évaluations régulières, des vulnérabilités et du risque global pour la sécurité.

La réglementation de la production, du transport et de la distribution d'électricité relève de la compétence des provinces et des territoires. Cependant, la Régie réglemente environ 1 500 kilomètres de lignes internationales de transport d'électricité. Les Canadiens s'attendent, à juste titre, à ce que nous tenions les sociétés pipelinières et les compagnies de lignes internationales de transport d'électricité que nous réglementons responsables de l'exploitation en toute sécurité des infrastructures énergétiques réglementées par la Régie.

La Régie canadienne de l'énergie est bien placée pour administrer les obligations énoncées dans le projet de loi C-26, en particulier celles qui s'appliquent aux entreprises qu'elle réglemente et qui rejoignent celles qui figurent déjà dans la Loi sur la Régie canadienne de l'énergie.

Par exemple, le projet de loi donne à la Régie canadienne de l'énergie la capacité d'émettre des ordonnances et de prendre les mesures d'application de la loi nécessaires pour que les entreprises trouvées en défaut renouent avec la conformité, de sorte à assurer la protection des systèmes cybernétiques essentiels.

● (0930)

[*Français*]

La Régie utilise déjà des outils semblables. Par exemple, elle publie des avis de non-conformité, des ordonnances d'inspecteur et des sanctions administratives pécuniaires, au besoin, pour remettre les sociétés en conformité et assurer leur exploitation en toute sécurité.

La Régie vérifie également si les sociétés respectent les exigences au moyen d'inspections, d'audits, de réunions sur la conformité et d'exercices d'intervention en cas d'urgence.

[*Traduction*]

La Régie applique une approche intégrée à l'échelle gouvernementale. Elle collabore avec des organismes fédéraux, territoriaux, provinciaux et internationaux, ainsi qu'avec l'industrie réglementée, pour veiller à ce que des mesures de protection contre les cyberrisques ou les cyberattaques soient prises de façon proactive à l'égard des infrastructures énergétiques sous réglementation fédérale.

Merci beaucoup de m'avoir donné l'occasion de vous parler aujourd'hui de cette question importante. Nous serons heureux de répondre à vos questions.

Le président: Merci, monsieur Loewen.

Madame Wright, allez-y.

Mme Leila Wright (directrice exécutive, Télécommunications, Conseil de la radiodiffusion et des télécommunications canadiennes): Bonjour, et merci de nous avoir invités à comparaître devant vous.

Avant de commencer mon allocution, j'aimerais souligner que nous sommes réunis sur le territoire traditionnel non cédé du peuple algonquin anishinabe.

Je m'appelle Leila Wright, et je suis directrice exécutive, Télécommunications, au CRTC. Je suis accompagnée aujourd'hui par mes collègues, Steven Harroun, Cadre en chef de la conformité et des enquêtes, et Anthony McIntyre, avocat général.

[*Français*]

Le CRTC est un tribunal indépendant et quasi judiciaire qui fonctionne sans lien de dépendance avec le gouvernement. Nous tenons des audiences publiques sur les questions de télécommunication et de radiodiffusion et nous prenons des décisions fondées sur le dossier public.

[*Traduction*]

Dans le secteur des télécommunications, notre travail vise essentiellement à stimuler la concurrence dans les services Internet et de téléphonie mobile. Pour ce faire, nous faisons la promotion d'un plus grand choix et de prix plus abordables pour la population canadienne, nous encourageons les investissements dans des réseaux fiables et de grande qualité, et nous améliorons l'accès aux services de télécommunications dans les communautés autochtones, rurales et éloignées. Nous disposons également d'une équipe qui contribue à protéger les Canadiens contre les messages textes, les appels non désirés, et les arnaques en ligne.

[*Français*]

Le CRTC joue un rôle modeste dans l'effort du gouvernement fédéral en vue de protéger la sécurité du système de télécommunications du Canada.

[*Traduction*]

D'autres organismes contribuent également à cet effort, dont le Centre de la sécurité des télécommunications, le Service canadien du renseignement de sécurité, Innovation, science et développement économique Canada, le Comité consultatif canadien pour la sécurité des télécommunications et plusieurs autres.

Le CRTC n'a pas de rôle à jouer dans la proposition de Loi sur la protection des cybersystèmes essentiels. En outre, bon nombre des modifications proposées à la Loi sur les télécommunications établissent de nouveaux pouvoirs exclusivement pour le gouverneur en conseil et le ministre de l'Industrie, et ne modifient pas le mandat réglementaire du CRTC en vertu de cette loi.

● (0935)

[*Français*]

Toutefois, quelques modifications seraient pertinentes pour les travaux du CRTC, dont trois en particulier, que j'aimerais souligner.

[*Traduction*]

Premièrement, la modification proposée à l'article 7 ajouterait un nouvel objectif stratégique axé sur la promotion de la sécurité du système de télécommunications canadien. Comme pour d'autres objectifs stratégiques énoncés dans la loi, cet ajout permettrait au CRTC d'examiner expressément comment ses décisions pourraient faire avancer ce nouvel objectif.

Deuxièmement, l'ajout de l'article 15.6 faciliterait le partage d'information entre le CRTC et un groupe plus large d'agences et ministères ayant la sécurité comme objectif, dans le but d'assurer la conformité avec les ordonnances et règlements pris par le Gouverneur en conseil et le ministre.

[*Français*]

Troisièmement, l'article 47 exigerait que le CRTC tienne compte, dans sa prise de décision, de toute ordonnance et tout règlement pris par le gouverneur en conseil et le ministre.

[*Traduction*]

Si le Parlement adopte le projet de loi C-26, le CRTC sera prêt à mettre en œuvre toute modification apportée à la Loi sur les télécommunications ayant un effet sur notre travail.

Encore merci de votre invitation, et nous serons maintenant heureux de répondre à vos questions.

Le président: Merci, madame Wright.

Nous allons passer directement aux questions.

M. Shipley sera le premier, pour six minutes.

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

Merci à tous les témoins pour leur présence.

Durant cette première heure, nous avons entendu un chiffre choquant cité par M. de Boer, qui a dit que 5,2 millions de cyberattaques avaient été stoppées. Ce chiffre me choque.

M. Loewen pourrait-il nous préciser combien de ces cyberattaques concernent le secteur qui relève de son organisme de réglementation?

M. Chris Loewen: Merci beaucoup de la question.

Je dois dire que c'est l'une des raisons pour lesquelles la production de rapports prévue dans le projet de loi est fondamentale. Nous nous fions déjà aux rapports des entreprises parce qu'ils nous permettent de comprendre l'ampleur des cybermenaces ou des cyberattaques concernant nos entreprises, mais pas leur nombre précis. L'industrie réglementée est ciblée par des menaces provenant d'acteurs nationaux et étatiques. Celles-ci vont du vol de mots de passe et de documents à l'utilisation de rançongiciels et d'autres types de maliciels.

Je vais céder la parole à mon collègue, Chris Finley. Il pourra peut-être vous donner une meilleure idée de l'ampleur du problème.

M. Christopher Finley (directeur, Gestion des urgences et sécurité, Régie de l'énergie du Canada): Je vous remercie de la question.

À ce jour, la Régie de l'énergie du Canada n'a reçu aucune preuve d'incidents de cybersécurité émanant de sociétés réglementées et ayant eu une incidence sur l'exploitation d'un pipeline — autrement dit, sur le réseau technologique opérationnel. Il est vrai qu'aucun incident lié à la cybersécurité n'a été signalé. Notre réglementation énonce toute une série d'incidents à déclaration obligatoire. Aucun n'a encore été déclaré.

Nos industries réglementées sont bien sûr toujours menacées. Bon nombre des attaques qui les visent ne sont pas conséquentes, et nous n'en entendrions pas parler. De plus, les déclarations au Centre canadien pour la cybersécurité sont volontaires.

M. Doug Shipley: Merci.

Je pense qu'il y avait quelque part de bonnes nouvelles pour nous. Comme je l'ai dit, outre le chiffre de 5,2 millions de cyberattaques mentionnées au début, il y a quelque chose de rassurant dans le fait de savoir que vous subissez considérablement moins de telles agressions.

En quoi le projet de loi C-26 changera-t-il votre façon de faire en général? Cela aidera-t-il vos membres et vous aidera-t-il? Quelles seraient les principales répercussions de l'adoption du projet de loi; que changerait-il?

● (0940)

M. Chris Loewen: Le projet de loi cadre parfaitement avec le mandat de surveillance de la Régie. Nous disposons déjà d'un cadre de réglementation assez solide qui exige que les entreprises constatent et anticipent les menaces et les risques pesant sur leurs systèmes, leurs processus et leurs activités, et qu'elles mettent en place des programmes pour les prévenir et les atténuer. Nous avons aussi des agents d'inspection qui peuvent émettre des ordonnances de non-conformité et, au besoin, imposer des sanctions administratives pécuniaires.

On voit que les éléments du projet de loi reflètent étroitement ce qui est déjà en place. De plus, il améliore les dispositions relatives à la production de rapports et l'échange de renseignements ce qui, à mon avis, ne peut que renforcer la surveillance des cybermenaces au sein de notre industrie.

M. Doug Shipley: Merci.

Je vais m'adresser à nos témoins du CRTC, probablement à Mme Wright, qui a commencé.

Certains se sont dit préoccupés par le fait que les décrets en conseil, les arrêtés ministériels ou la prise de règlements annulant une décision du CRTC ne font pas l'objet d'un avis public ou d'un avis de décision. Seriez-vous d'accord pour dire que ce processus devrait être plus transparent?

Mme Leila Wright: Le CRTC a pour rôle de mettre en œuvre les lois adoptées par le Parlement. Comme il ne s'agit pas pour nous de commenter les projets de loi dont le Parlement est saisi, je ne suis malheureusement pas en mesure de répondre à votre question.

M. Doug Shipley: Merci.

Seriez-vous en faveur de dispositions qui obligeraient le gouvernement à déposer un rapport annuel indiquant le nombre de fois où les décrets ou les règlements gouvernementaux ont eu préséance sur les décisions du CRTC?

Mme Leila Wright: Je dirais respectueusement que cette question s'adresse à ISDE.

M. Doug Shipley: Excusez-moi, je ne vous ai pas entendue.

Mme Leila Wright: C'est une question qu'il faudrait poser à nos collègues d'ISDE.

M. Doug Shipley: D'accord.

Merci, monsieur le président.

Le président: Merci, monsieur Shipley.

Nous passons à M. Schiefke pour six minutes. Allez-y, monsieur.

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

Je tiens à remercier nos témoins de comparaître en personne ou virtuellement.

Je vais commencer par poser mes questions à M. Loewen.

Monsieur Loewen, pourriez-vous nous expliquer en termes simples, pour les Canadiens qui sont touchés par ce sujet et qui s'y intéressent quelles seraient les conséquences d'une cyberattaque réussie contre un exploitant d'infrastructures essentielles dans le secteur de l'énergie?

M. Chris Loewen: Je vous remercie de cette question.

Les conséquences pourraient varier considérablement et dépendre de la nature de l'attaque, évidemment.

D'après l'évaluation de la situation par le cybercentre, la principale menace pesant sur le secteur de l'énergie du Canada émane de cybercriminels motivés par des gains financiers qui utilisent principalement des rançongiciels, comme je l'ai dit plus tôt. Ces attaques touchent généralement les réseaux des technologies de l'information, bien qu'il leur soit possible de cibler la technologie opérationnelle. Bien sûr, les attaques par rançongiciel contre les réseaux de TI coûtent cher aux entreprises visées qui doivent payer la rançon, mais elles sont aussi coûteuses en temps perdu et en remise en état des infrastructures.

Les rançongiciels sur un ancien réseau en T ou un réseau technologique opérationnel comme un système SCADA, bien que rares, pourraient perturber beaucoup plus l'exploitation des pipelines. Bien qu'il soit peu probable que cela crée des conditions d'exploitation dangereuses, comme mon collègue l'a mentionné plus tôt, nous ne savons pas s'il y en a déjà eu ou pas. Nous n'avons pas entendu parler de telles attaques contre des systèmes de technologies opérationnelles dans une industrie réglementée par la Régie.

M. Peter Schiefke: Je vais enchaîner sur le même sujet.

Compte tenu de l'interdépendance du secteur de l'énergie au Canada et de celui de notre principal partenaire commercial et allié, les États-Unis, dans quelle mesure est-il important d'exiger du Canada, dans le projet de loi C-26, qu'il renforce sa cybersécurité?

M. Chris Loewen: Je dirais que le secteur de l'énergie est ciblé par les activités de cyberespionnage des États-nations qui ne reconnaissent pas les frontières. Il s'agit principalement d'une menace à la propriété intellectuelle, comme la recherche et les plans d'affaires. Étant donné que le secteur de l'énergie est une infrastructure essentielle d'une importance stratégique et qu'il est transfrontalier, comme vous l'avez souligné, celui-ci est également susceptible d'être la cible d'États-nations antagonistes cherchant à saboter toute technologie opérationnelle.

Les répercussions seraient considérables.

● (0945)

M. Peter Schiefke: L'un des principaux objectifs de notre comité est d'améliorer le projet de loi et de voir ce que nous pourrions y ajouter à cette fin.

Selon vous, les États-Unis, notre partenaire commercial et allié, ont-ils des choses que nous n'avons pas, mais que nous devrions avoir dans notre projet de loi C-26?

M. Chris Loewen: Vous savez, ce n'est pas nous qui pilotons ce projet de loi particulier, mais nous avons quand même donné notre avis. À mon sens, il est déjà très bien aligné sur ce que nous avons en place à la Régie de l'énergie du Canada.

Je vais céder le micro à mon collègue, M. Chris Finley, qui connaît mieux certaines des activités que mènent les États-Unis.

M. Peter Schiefke: Monsieur Finley, vous pouvez y aller.

M. Christopher Finley: Merci.

Nous travaillons en étroite collaboration avec la Transportation Security Administration et la Pipeline and Hazardous Materials Safety Administration. Essentiellement, au Canada, nous travaillons en étroite collaboration avec le Centre de la sécurité des télécommunications et son centre pour la cybersécurité pour maintenir l'alignement interne.

Nous croyons, comme mon collègue l'a dit, que notre cadre réglementaire est solide. Nous croyons quand même que le signalement qu'exigent les nouveaux articles 17, 18 et 19 constitue un grand avantage. Nous pouvons prendre ces renseignements et les mettre en œuvre dans l'ensemble de notre réseau de pipelines pour le rendre plus sécuritaire.

M. Peter Schiefke: Merci à vous deux.

Je m'adresse maintenant à Mme Wright.

Madame Wright, merci d'être là.

La protection de la vie privée des Canadiens est une priorité pour nous tous ici, quel que soit notre parti politique. Certains témoins prévoient que ce projet de loi pourrait amener le gouvernement à accéder aux renseignements personnels, notamment dans les téléphones cellulaires, à les recueillir et à les utiliser à mauvais escient. Selon votre interprétation du projet de loi et selon votre expérience et votre position, croyez-vous qu'on en viendra là?

Mme Leila Wright: Encore une fois, malheureusement, je ne suis pas en mesure de répondre à votre question.

Notre rôle est de mettre en œuvre les dispositions qui touchent le travail du Conseil de la radiodiffusion et des télécommunications canadiennes, le CRTC. Je les ai décrites. Elles sont très limitées, et je ne suis donc pas en mesure de répondre à votre question.

M. Peter Schiefke: Pourriez-vous nous expliquer quel sera le point d'intersection du projet de loi C-26 avec la Loi sur la protection des renseignements personnels? Le projet de loi touche-t-il de quelque manière l'applicabilité de la loi?

Mme Leila Wright: Malheureusement, je ne suis pas en mesure de répondre à votre question.

M. Peter Schiefke: D'accord.

Dernière question avant que mon temps de parole ne soit écoulé.

Y a-t-il quoi que ce soit d'autre que vous aimeriez voir dans le projet de loi C-26, madame Wright, pour appuyer davantage le travail que vous faites?

Mme Leila Wright: Encore une fois, notre rôle consiste à mettre en œuvre les lois adoptées par le Parlement, et non pas à commenter les projets de loi présentés dont le Comité est saisi.

M. Peter Schiefke: D'accord. Merci, madame Wright.

C'est tout, monsieur le président. Merci.

Le président: Monsieur Julian, vous avez six minutes, je vous prie.

[*Français*]

M. Peter Julian: Monsieur le président, je vais poser une question au nom de Mme Normandin. J'aimerais que vous soyez un peu flexible quant à mon temps de parole. Si cela vous convient, je poserai d'abord sa question, puis je poserai les miennes.

Madame Wright, la question que je vais vous poser concerne la recommandation que le Comité a reçue de Citizen Lab, qui a proposé de prévoir des allégements pour les petites entreprises de télécommunications.

Croyez-vous qu'il est important que la mise en place du cadre réglementaire du projet de loi C-26 se fasse en considérant l'impact que cela va avoir sur de plus petites entités de télécommunications? Croyez-vous que la mise en vigueur de ce cadre réglementaire doit être assez flexible pour permettre aux petites entreprises de se conformer aux éléments du projet de loi sans problème?

[*Traduction*]

Mme Leila Wright: Je vous remercie de la question et vous prie de m'excuser si le Comité trouve ma réponse frustrante.

Notre rôle est de mettre en œuvre les lois adoptées par le Parlement. En ce qui concerne le projet de loi dont le Comité est saisi aujourd'hui, nous pouvons parler des modifications proposées à la Loi sur les télécommunications qui touchent le travail du CRTC, ainsi que de la façon dont le CRTC applique des dispositions semblables actuellement. Cependant, je ne suis pas en mesure de répondre à votre question.

M. Peter Julian: D'accord, merci.

J'aimerais m'adresser à M. Loewen et à M. Finley.

Monsieur Finley, lorsque M. Shipley vous a interrogé au sujet du nombre d'incidents, vous avez dit que rien n'avait été signalé à ce jour, mais qu'il y avait peut-être eu des signalements au centre pour la cybersécurité.

Premièrement, pouvez-vous nous dire si vous êtes au courant d'incidents qui ont été signalés au centre pour la cybersécurité? Cela fait-il partie du rapport de situation que vous recevez? Je trouve un peu surprenant, très franchement, qu'il n'y ait rien à ce jour. Je suppose que cela signifie que seuls les incidents dépassant un certain seuil sont signalés. Si vous pouviez clarifier vos propos à ce sujet, ce serait utile, parce que, comme M. Shipley l'a mentionné, BlackBerry vient de témoigner qu'il a été en mesure de bloquer plus de cinq millions de tentatives de cyberattaques au cours des 90 derniers jours. Il me semble que le secteur de l'énergie serait une cible de choix de ces mauvais joueurs.

● (0950)

M. Christopher Finley: Oui, certainement, je peux clarifier mes propos.

Le secteur de l'énergie est une cible; cela ne fait aucun doute. Pour répondre à la question, en général, rien n'oblige à l'heure actuelle à signaler les incidents de cybersécurité à la Régie de l'énergie du Canada. Nous travaillons en étroite collaboration avec les entreprises réglementées et le centre pour la cybersécurité, et nous encourageons la déclaration volontaire de notre entreprise au centre pour la cybersécurité, et il crée des accords de non-divulgation.

Il recueille des renseignements et les transmet aux industries sous une forme qui ne divulgue pas les détails. Je suppose que c'est ce que ferait ce projet de loi. Il renforcerait la déclaration obligatoire et nous permettrait d'avoir accès à cette information plus librement qu'aujourd'hui.

M. Peter Julian: À l'heure actuelle, vous n'avez pas accès à cette information. Serait-il juste de dire qu'il n'y a pas de partage des pratiques exemplaires? S'il y a une attaque contre une entreprise du secteur de l'énergie, les autres entreprises du secteur de l'énergie n'auraient pas accès aux renseignements sur la façon de la bloquer.

Est-ce que cela décrit bien la situation actuelle?

M. Christopher Finley: Il n'y a pas de déclaration obligatoire en matière de cybersécurité pour les signalements à la Régie de l'énergie du Canada, sauf si l'objet du signalement est défini dans le règlement sur les pipelines terrestres pour un autre type d'incident, comme l'exploitation non conforme à la conception, ou quelque chose de plus grave encore.

Ces renseignements sont déclarés volontairement au centre pour la cybersécurité qui, encore une fois, produit des rapports. Ma question s'adresse peut-être au centre pour la cybersécurité. Il produit des rapports sur les menaces et les risques et les distribue au sein de notre industrie et de façon plus générale, de sorte que les entreprises ont certainement accès à l'information nécessaire pour prendre les mesures d'atténuation appropriées.

M. Peter Julian: D'accord. Je vous remercie de votre honnêteté. Cela me dérange. Cela ne signifierait-il pas, par exemple, que dans le cas de la fermeture du pipeline Colonial, dont d'autres témoins ont parlé, les renseignements sur la façon de bloquer ce type d'attaque ne seraient pas nécessairement accessibles aux sociétés d'énergie canadiennes et à la Régie de l'énergie du Canada? Ou est-ce parce que nous recevons de l'information sur des attaques à l'extérieur du Canada, mais qu'au Canada, cette information n'est pas nécessairement communiquée de quelque façon que ce soit pour permettre aux sociétés d'énergie, en l'occurrence, de se prémunir contre une répétition de ces attaques?

M. Christopher Finley: Je suis convaincu que le projet de loi pourrait être plus structuré et plus formalisé. Ces mécanismes seraient alors en place pour communiquer officiellement cette information. Vous le comprendrez, certains de ces renseignements sont accompagnés de mises en garde sur la mesure dans laquelle ils peuvent être communiqués en raison de la confidentialité.

Encore une fois, nous avons des relations informelles avec le centre pour la cybersécurité et avec d'autres ministères et organismes fédéraux pour obtenir cette information. Dans le cadre de nos activités de vérification de la conformité, nous examinons les programmes et les systèmes des entreprises pour vérifier qu'elles font tout ce qu'elles peuvent, qu'elles sont connectées au centre pour la cybersécurité et reçoivent l'information la plus récente sur les menaces et les risques, et qu'elles prennent les mesures voulues.

● (0955)

M. Peter Julian: Le président est très généreux. J'ai une dernière question, plus précisément sur le gaz Colonial.

Avez-vous eu accès à l'information sur cette attaque et sur la façon de prévenir le même genre d'attaque désormais?

M. Christopher Finley: Il s'agit d'un pipeline qui se trouvait aux États-Unis. Donc, nous avons eu connaissance de l'incident officieusement, mais certainement grâce à divers rapports de travail que nous avons avec notre personnel dans différents ministères. Mais, je ne suis pas prêt à parler des détails de l'affaire.

Le président: Merci, monsieur Finley.

Merci, monsieur Julian.

Nous passons au deuxième tour. Nous tombons pile.

Monsieur Lloyd, vous avez cinq minutes.

M. Dane Lloyd: Merci, monsieur le président.

Merci aux témoins d'être venus.

Mes questions porteront sur la Régie de l'énergie du Canada.

Je pense qu'il y a eu un peu de confusion au sujet de ce projet de loi. Certaines personnes qui nous regardent pourraient croire que si nous n'adoptons pas le projet de loi ou s'il est retardé, les entreprises ne dépenseront pas pour la cybersécurité. Pourtant, il est assez clair que les entreprises dépensent beaucoup pour la cybersécurité. Ainsi, une grande société pétrolière intégrée, Cenovus, a annoncé dans son budget de 2024 qu'elle dépensera plus de 100 millions de dollars en cybersécurité. Il semble certainement que de nombreuses entreprises de nombreux secteurs prennent l'enjeu très au sérieux.

Par contre, nous venons tout juste d'entendre les témoins du dernier groupe — je crois qu'il s'agissait d'Électricité Canada — qui se faisaient du souci à cause de ce projet de loi, craignant qu'il n'entraîne pas nécessairement une augmentation massive des dépenses consacrées au signalement et à la prévention des incidents, mais qu'il n'impose une augmentation considérable des dépenses que devront faire les entreprises pour se conformer à la loi, sans plus.

Pourriez-vous nous livrer votre commentaire. Prévoyez-vous que les coûts de conformité pour les entreprises augmenteront considérablement du fait de ce projet de loi?

M. Chris Loewen: Comme je l'ai mentionné dans ma déclaration préliminaire, le projet de loi est très étroitement aligné sur ce que nous avons déjà en place. À la Régie de l'énergie du Canada, nous avons déjà un cadre de réglementation solide qui comprend des inspecteurs, des ordonnances d'inspecteur, la distribution d'avis de non-conformité, le recours à des sanctions administratives pécuniaires et des inspections. Les entreprises connaissent déjà très bien la nécessité de se doter de programmes de cybersécurité pour détecter et prévenir les menaces.

Pour ce qui est de l'impact financier global sur l'industrie réglementée par la Régie de l'énergie du Canada, je pense qu'une partie de ce détail doit être déterminée par des règlements, qui n'ont pas encore été élaborés ni proposés. Pour ce qui est de l'autre partie, je signale que le projet de loi propose, en grande partie, de formaliser les pouvoirs et le cadre de surveillance que nous avons mis en place, mais en les étendant davantage pour formaliser, comme M. Finley l'a mentionné plus tôt, les rapports hiérarchiques, la collecte d'information et l'échange d'information du côté du gouvernement.

M. Dane Lloyd: Si je vous comprends bien, bon nombre des pratiques de cybersécurité qui figurent dans ce projet de loi ont déjà cours, du moins pour les industries réglementées par la Régie de l'énergie du Canada. Pour résumer vos propos, ce projet de loi ne fait que formaliser ce qui existe déjà. Je pense qu'il ne serait pas exagéré de dire que, dans un certain nombre d'autres secteurs, y compris le CRTC, ces pratiques et, dans certains cas, les règlements existent déjà pour assurer la cybersécurité.

Je déplore que le gouvernement envisage de formaliser cela, tout en se donnant plus de pouvoirs, alors que les Canadiens devraient avoir l'assurance, du moins dans votre industrie, que le secteur privé consacre déjà des sommes importantes.

Électricité Canada a également dit craindre que cette nouvelle loi formalisée n'ait un effet paralysant. Plutôt que d'avoir une très bonne relation entre, par exemple, vous-même et les opérateurs désignés sous vos ordres, où vous avez un dialogue très ouvert au sujet de la cybersécurité et de ce qu'il faut faire, il pourrait y avoir un effet paralysant lorsque les avocats conseilleront aux entreprises de ne fournir au gouvernement que les renseignements nécessaires en vertu de la loi.

Pouvez-vous nous parler de cet effet paralysant? Reconnaissez-vous avec Électricité Canada qu'il y a un certain danger que cet effet paralysant se concrétise?

● (1000)

M. Chris Loewen: Merci encore pour ce suivi.

Pour donner une idée plus précise de nos relations avec l'industrie, je dirais que c'est une mosaïque d'interrelations volontaires en matière de signalement, d'utilisation et de collecte de renseignements.

J'emploie le terme « officialiser » pour dire que c'est un aspect bénéfique de ce projet de loi. Je pense que l'industrie est tout à fait prête à mettre en œuvre les éléments du projet de loi associés à ces activités. Ce projet de loi renforcera la capacité du gouvernement de prévenir les cybermenaces et aidera nos entreprises réglementées à détecter et à atténuer les cybermenaces dans le futur.

Concernant les commentaires d'Électricité Canada quant à l'effet paralysant du projet de loi, notre expérience avec le secteur des pipelines et les menaces pour l'environnement, la sécurité et d'autres domaines nous a appris que la clarté des signalements — et je m'attends à ce que ce soit une exigence du règlement — n'est pas tant une exigence de base, mais elle aide à comprendre les attentes à cet égard.

Le président: Je vous remercie, monsieur Loewen. Votre temps est écoulé.

Monsieur McKinnon, c'est à vous, je vous en prie.

M. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.): Je vous remercie, monsieur le président.

Mes questions s'adressent à la Régie de l'énergie.

Vous avez parlé des exigences en matière de signalement et du reste, ainsi que de la nécessité d'avoir de bonnes données. Cela recoupe l'information que nous ont fournie des témoins précédents au sujet de la nécessité d'énoncer des définitions cohérentes et concises afin que les données puissent être saisies dans des entreprises et des contextes différents et avoir une signification.

Avez-vous des commentaires à ce sujet?

M. Chris Loewen: Je pense que chaque fois qu'on peut favoriser la cohérence et la clarté dans un secteur, tout le monde est gagnant.

À la Régie de l'énergie du Canada, nous avons une longue expérience en matière de mise en œuvre de notre cadre réglementaire, notamment du Règlement sur les pipelines terrestres et d'autres règlements. Les divers outils mis à la disposition de l'industrie pour assurer la clarté des signalements d'incident, comme les lignes directrices sur les rapports d'événement ainsi que d'autres directives et documents d'orientation, sont bien accueillis par les entreprises et leur permettent de mieux comprendre les attentes de l'organisme de réglementation. Dans l'ensemble, je pense que cela renforce les protections au sein d'un secteur. Je vois cela comme un aspect des exigences énoncées dans ce projet de loi.

Comme je l'ai constaté tout à l'heure, le règlement n'a pas encore été élaboré. Si le projet de loi est adopté, je serai ravi de fournir des conseils aux ministères et aux organismes responsables.

M. Ron McKinnon: Pensez-vous que ces définitions devraient être énoncées dans le règlement ou devraient-elles être intégrées au projet de loi lui-même?

M. Chris Loewen: N'étant pas le responsable de leur élaboration, je préfère dire que le règlement permet une certaine souplesse quant à son contenu et aux modifications ultérieures qui pourraient y être apportées. Il ne serait pas nécessaire de modifier la loi.

M. Ron McKinnon: Tout à l'heure, on a également dit que les États-Unis avaient entrepris de créer un ensemble cohérent de définitions pour leurs 52 régimes.

Est-ce que cela pourrait être avantageux pour nous? Est-ce un projet auquel nous participons, d'une manière ou d'une autre?

M. Chris Loewen: Je ne sais pas si je peux parler de ce cas précis, mais je peux vous dire que la coordination et la coopération que nous avons avec nos homologues américains, comme la Pipeline and Hazardous Materials Safety Administration, qui réglemente les pipelines, sont excellentes.

L'uniformité des définitions est certes accueillie favorablement par l'industrie. Je dirais que l'uniformité et la cohérence du cadre réglementaire sont souhaitables lorsqu'un réseau peut être mis en place.

● (1005)

M. Ron McKinnon: La notion de cyberincident semble très générique, très abstraite. J'aimerais que vous nous donniez des précisions sur le genre d'incidents dont nous parlons. De quels types d'attaques s'agit-il? Qui sont les mauvais joueurs? Parle-t-on d'un pirate informatique travaillant dans le sous-sol de la maison familiale ou plutôt d'une entité internationale? Pouvez-vous nous éclairer à ce sujet?

M. Chris Loewen: Je vais dire quelques mots et je céderai ensuite le micro à mon collègue, M. Finley, qui vous donnera plus de détails.

Cela varie entre le pirate qui travaille dans son sous-sol et un acteur étatique.

Tout à l'heure, quand nous parlions des incidents et des signalements, la Régie de l'énergie du Canada a expliqué la différence entre une attaque contre un réseau de technologie de l'information — c'est-à-dire le réseau qui vous fournit des services de messagerie électronique et stocke vos documents et vos mots de passe — et un réseau de technologie opérationnelle, c'est-à-dire les systèmes utilisés pour faire fonctionner les vannes des pipelines et d'autres systèmes. À notre connaissance, aucune attaque n'a encore été menée avec succès au Canada contre un réseau opérationnel dans le secteur réglementé par la Régie. Par contre, dans vos réseaux de technologie de l'information — ceux qui stockent les mots de passe et autres données —, oui, ces attaques sont assez fréquentes.

Monsieur Finley, voulez-vous ajouter quelque chose?

M. Christopher Finley: Oui, comme vient de le mentionner mon collègue, la majorité des attaques visent des réseaux de TI; il s'agit de rançongiciels généralement créés par des cybercriminels et des États nationaux. Nous n'avons pas toute l'information à portée de main, mais c'est le genre d'information sur lequel nous travaillons en étroite collaboration avec le Centre canadien pour la cybersécurité qui recueille ces renseignements.

Le président: Je vous remercie, monsieur Finley.

Merci beaucoup, monsieur McKinnon.

C'est maintenant à vous, monsieur Julian. Vous avez deux minutes et demie.

M. Peter Julian: Merci beaucoup, monsieur le président.

Mme Wright, est-ce que le CRTC fait un suivi quelconque des incidents qui mettent en péril la cybersécurité des entreprises de télécommunications et d'autres entreprises relevant de votre compétence?

Mme Leila Wright: Le CRTC ne joue aucun rôle en matière de cybersécurité.

Je vais demander à mon collègue Steven Harroun s'il peut vous décrire une partie de nos activités d'application de la loi dans ce domaine.

M. Steven Harroun (chef de l'application de la Conformité et enquêtes, Conseil de la radiodiffusion et des télécommunications canadiennes): Pour répondre à votre question, la réponse est non. Je pense que le Centre canadien pour la cybersécurité est votre meilleur témoin à cet égard, comme l'a mentionné mon collègue de la Régie de l'énergie.

M. Peter Julian: Aucune des entreprises ou entités relevant de votre compétence ne vous informe des atteintes à la cybersécurité dont elles sont la cible. Vous n'êtes pas mis au courant.

Mme Leila Wright: Nous travaillons en étroite collaboration avec nos collègues d'ISDE pour réglementer cet espace. Nous pouvons vous faire parvenir une réponse ultérieurement.

M. Peter Julian: Je pense que cela nous serait utile, parce que nous avons été stupéfaits du nombre faramineux d'atteintes ou de tentatives d'atteinte à la cybersécurité. Ce matin, BlackBerry nous a appris qu'il y en avait eu plus de cinq millions au cours des 90 derniers jours. Tout comme le secteur de l'énergie, le secteur des télécommunications joue un rôle essentiel et il me semble évident que les entreprises de ce secteur risquent d'être la cible d'attaques et de tentatives d'attaque. Ce que j'entends, c'est que pour le moment vous ne recueillez pas cette information, ce qui me paraît préoccupant. Tout renseignement que vous pouvez fournir au Comité à cet égard nous serait utile.

Puis-je vous demander dans quelle mesure le CRTC a été consulté au sujet de ce projet de loi avant son dépôt? Y a-t-il eu des consultations? Le gouvernement a-t-il communiqué avec vous, compte tenu de votre rôle de réglementation?

Mme Leila Wright: Je vais laisser mon collègue, M. McIntyre, répondre à cette question.

M. Anthony McIntyre (avocat général et sous-directeur exécutif, Services juridiques, Conseil de la radiodiffusion et des télécommunications canadiennes): Nous avons été consultés avant le dépôt du projet de loi. Étant donné que notre rôle en vertu des amendements est très limité, nous n'avons été consultés que sur les quelques dispositions qui s'appliqueraient à nous. Nous avons donc participé aux discussions stratégiques seulement à l'égard des dispositions qui nous concernent.

● (1010)

M. Peter Julian: À votre avis, le contenu du projet de loi reflète-t-il les opinions exprimées par le CRTC?

M. Anthony McIntyre: Je ne sais pas si je suis en mesure de faire un commentaire à ce sujet.

Le président: Monsieur McIntyre, monsieur Julian, je vous remercie.

Pour les deux dernières questions, chaque intervenant disposera de deux minutes et demie.

Allez-y, monsieur Motz, vous avez deux minutes et demie.

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

Mes questions concernent le CRTC. L'an dernier, la vérificatrice générale a constaté que le CRTC ne faisait pas suffisamment d'efforts pour surveiller l'abordabilité des services Internet et de téléphonie mobile, en particulier dans les régions rurales et éloignées. Le CRTC a-t-il entrepris une analyse de l'impact du projet de loi C-26, dans sa forme actuelle, sur les prix que les Canadiens paient pour les services Internet et de téléphonie mobile?

Mme Leila Wright: Pas à ma connaissance.

M. Glen Motz: Vous ne le savez donc pas. D'accord, c'est intéressant.

Pensez-vous qu'il aura un impact sur les prix des services Internet et de téléphonie mobile?

Mme Leila Wright: Il m'est difficile de répondre à cette question sans données ni détails supplémentaires. Par contre, je peux vous dire que le CRTC travaille très fort pour promouvoir un plus grand choix et des prix abordables pour les Canadiens de tout le pays, notamment dans les collectivités autochtones, rurales et éloignées.

M. Glen Motz: Je vous encourage à réfléchir à la question pour voir s'il y a un impact.

Nous savons aussi que les projets de loi C-11 et C-18 confèrent de vastes pouvoirs au CRTC. Des témoins nous ont dit que le projet de loi C-26, dans sa forme actuelle, accorde également trop de pouvoir, surtout au ministre. Quelles modifications recommandez-vous d'apporter à la loi pour donner aux Canadiens l'assurance qu'une surveillance adéquate, sans être excessive, sera exercée et qu'il y aura un juste équilibre entre la transparence et la reddition de comptes?

Mme Leila Wright: Je ne suis malheureusement pas en mesure de commenter le projet de loi dont le Comité est saisi. Notre rôle est de mettre en œuvre les lois adoptées par le Parlement.

M. Glen Motz: J'ai terminé, monsieur le président.

Le président: Merci, monsieur Motz.

Monsieur McKinnon, c'est à vous. Vous avez deux minutes et demie.

M. Ron McKinnon: Je comprends que vous êtes un organisme quasi judiciaire et que cela vous restreint dans les réponses que vous pouvez nous donner, mais nous sommes ici pour étudier le projet de loi C-26 et le bonifier afin qu'une fois adopté, il fasse son travail. Avez-vous quelque chose à nous offrir pour nous aider à faire notre travail?

Mme Leila Wright: Je peux certes commenter les modifications proposées à la Loi sur les télécommunications qui touchent le travail du CRTC. L'une des modifications proposées vise à permettre au CRTC de partager des renseignements, dans des circonstances particulières, avec d'autres ministères et organismes gouvernementaux à vocation financière.

Dans d'autres domaines, nous avons la capacité de partager de l'information avec des ministères et des organismes, et mon collègue Steven Harroun peut vous décrire de quelle manière nous avons utilisé cette capacité.

M. Steven Harroun: Pour ajouter à ce que Mme Wright a dit, l'un de mes rôles en matière de conformité et d'application porte sur la Loi canadienne anti-pourriel. Cette loi prévoit le partage de renseignements très précis avec mes partenaires du Commissariat à la protection de la vie privée et du Bureau de la concurrence. Nous pouvons échanger des renseignements concernant la Loi canadienne anti-pourriel, ce qui a été très efficace pour nous aider à nous acquitter de nos rôles respectifs d'application de la loi.

M. Ron McKinnon: Merci.

Le président: Je vous remercie.

Cela met fin à notre réunion d'aujourd'hui.

M. Doug Shipley: Désolé, mais j'ai une question à poser. Le ministre de la Sécurité publique devait venir passer deux heures avec nous pour discuter des droits des victimes. Avons-nous une idée de la date à laquelle le ministre participera à cette rencontre de deux heures? La motion a été adoptée il y a déjà un certain temps.

Le président: Nous allons faire un suivi, monsieur Shipley. Nous attendons toujours une réponse.

M. Doug Shipley: Nous aussi.

Merci.

Le président: Merci encore à nos témoins.

Le Comité est-il d'accord pour lever la séance?

Des députés: D'accord.

Le président: Je vous remercie.