## EVIDENCE

OTTAWA, Monday, May 4, 2026

The Standing Senate Committee on National Security, Defence and Veterans Affairs met with videoconference this day at 4 p.m. [ET] to study Bill C-8, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.

**Senator Hassan Yussuff** (*Chair*) in the chair.

[*English*]

**The Chair:** Honourable senators, I call this meeting of the Standing Senate Committee on National Security, Defence and Veterans Affairs, to order.

Before we begin, colleagues, I would like to inform you of my resignation from the chair of this committee. It has been a pleasure serving, of course, the past number of years. I have enjoyed working with each one of you and appreciate your efforts, your leadership and your support for everything we have done on the committee.

I don't want to take too much time because we have the minister and officials here and we want to get on with our business. However, I want to sincerely thank you. I'm sure the new chair will find some time at the end for those who want to intervene so we don't disrupt the committee meeting, but I want to conclude by saying thank you to all of you.

With that in mind, the Independent Senators Group, or ISG, has met as a group and proposed Senator Marty Deacon to replace me as the chair. I would put that as a recommendation that we support Marty Deacon to become the Chair of the Standing Senate Committee on National Security, Defence and Veterans Affairs. All those in favour?

**Hon. Senators:** Agreed.

**The Chair:** I'll ask my colleague Senator Marty Deacon to take the chair.

Senator Marty Deacon (*Chair*) in the chair.

**The Chair:** Colleagues, thank you. It's an honour to take on this role. I look forward to working with you in this new capacity. It's going to challenge my desire to ask a million questions every day, but I will do my best to make that transition.

## TÉMOIGNAGES

OTTAWA, le lundi 4 mai 2026

Le Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants se réunit aujourd'hui, à 16 heures (HE), avec vidéoconférence, afin d'examiner le projet de loi C-8, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois.

**Le sénateur Hassan Yussuff** (*président*) occupe le fauteuil.

[*Traduction*]

**Le président :** Honorables sénateurs, je déclare ouverte cette séance du Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants.

Avant de commencer, chers collègues, je tiens à vous informer de ma démission de la présidence de ce comité. Ce fut bien sûr un plaisir de servir ces dernières années. J'ai beaucoup apprécié travailler avec chacun d'entre vous et je vous suis reconnaissant pour vos efforts, votre leadership et votre soutien dans toutes les actions menées au comité.

Je ne veux pas m'étendre trop longtemps, parce que le ministre et les représentants du gouvernement sont présents et que nous souhaitons passer à l'ordre du jour. Je tiens toutefois à vous remercier sincèrement. Je suis certain que la nouvelle présidente trouvera un moment à la fin de la réunion pour donner la possibilité d'intervenir à celles et ceux qui le souhaiteraient, cela pour ne pas perturber la réunion du comité. Je conclurai en vous remerciant toutes et tous.

Dans cette optique, le GSI, le Groupe des sénateurs indépendants, s'est réuni et a proposé la candidature de la sénatrice Marty Deacon pour me succéder à la présidence. Je propose donc que nous soutenions la candidature de Marty Deacon à la présidence du Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants. Quels sénateurs sont en faveur?

**Des voix :** D'accord.

**Le président :** J'invite ma collègue, la sénatrice Marty Deacon, à prendre le fauteuil.

La sénatrice Marty Deacon (*présidente*) occupe le fauteuil.

**La présidente :** Merci, chers collègues. Je suis honorée d'assumer cette fonction et je me réjouis à l'idée de travailler avec vous dans ce nouveau rôle. Cela va mettre à rude épreuve mon envie régulière de poser un million de questions, mais je ferai de mon mieux pour réussir cette transition.

I know we have the minister here, and we'd like to get to that very important part of our meeting, but I want to thank you for putting your faith in me to chair this important committee at this moment in our history.

Thank you to the outgoing chair for his leadership and example as we move ahead with this task.

Chairing your first meeting with a minister is a bit like driving a Formula 1 car, so I ask you to show grace and patience as we move on.

I would also like to take a moment to acknowledge and thank the minister and folks in the room today who attended the event a few hours ago. When we look at the work we do and why, being there for the beginning of this monument and tribute to our Armed Forces members and civilians we lost in Afghanistan was a very powerful reminder of why we're here on Monday afternoons. Speaking with the families, students and staff was very enlightening and also motivating for the work we do.

Before we get started and get to our witnesses, I'd ask that you please introduce yourselves this afternoon.

[*Translation*]

**Senator Carignan:** I'm Claude Carignan from Quebec.

[*English*]

**Senator Batters:** Denise Batters, from Saskatchewan.

[*Translation*]

**Senator Youance:** I'm Suze Youance from Quebec.

[*English*]

**Senator White:** Judy White, Newfoundland and Labrador.

**Senator Al Zaibak:** Mohammad Al Zaibak, Ontario.

**Senator Patterson:** Rebecca Patterson, Ontario.

**Senator Hay:** Katherine Hay, Ontario.

**Senator Dasko:** Donna Dasko, Ontario.

**Senator McNair:** John McNair, New Brunswick.

**Senator Yussuff:** Hassan Yussuff, Ontario.

**Senator Ince:** Tony Ince, Nova Scotia.

Le ministre est déjà là et je sais que nous voulons aborder ce point crucial de notre réunion, mais je tiens à vous remercier de m'avoir fait confiance pour présider ce comité important à ce moment précis de notre histoire.

Merci au président sortant pour son leadership et l'exemple qu'il nous a donné tandis que nous nous attelons à cette tâche.

Présider sa première réunion avec un ministre en face, c'est un peu comme piloter une Formule 1; je vous demande donc de faire preuve de bienveillance et de patience à mesure que nous avançons.

Je tiens également à prendre un moment pour saluer et remercier le ministre ainsi que les personnes présentes qui ont assisté à la cérémonie d'il y a quelques heures. Au regard de notre travail et de nos motivations, je dirais que cette participation à l'inauguration de ce monument et à l'hommage rendus à nos militaires et aux civils tombés en Afghanistan nous rappelle avec force pourquoi nous nous retrouvons ici tous les lundis après-midi. Les échanges avec les familles, les étudiants et le personnel ont été très enrichissants et ont également renforcé notre motivation dans le travail que nous accomplissons.

Avant d'enchaîner et de passer à l'audition des témoins, je vais demander à mes collègues de bien vouloir se présenter.

[*Français*]

**Le sénateur Carignan :** Claude Carignan, du Québec.

[*Traduction*]

**La sénatrice Batters :** Denise Batters, de la Saskatchewan.

[*Français*]

**La sénatrice Youance :** Suze Youance, du Québec.

[*Traduction*]

**La sénatrice White :** Judy White, de Terre-Neuve-et-Labrador.

**Le sénateur Al Zaibak :** Mohammad Al Zaibak, de l'Ontario.

**La sénatrice Patterson :** Rebecca Patterson, de l'Ontario.

**La sénatrice Hay :** Katherine Hay, de l'Ontario.

**La sénatrice Dasko :** Donna Dasko, de l'Ontario.

**Le sénateur McNair :** John McNair, du Nouveau-Brunswick.

**Le sénateur Yussuff :** Hassan Yussuff, de l'Ontario.

**Le sénateur Ince :** Tony Ince, de la Nouvelle-Écosse.

**Senator Kutcher:** Stan Kutcher, Nova Scotia. This is the East Coast side of the table.

**The Chair:** We're glad that you're here today. Thank you, Senator Kutcher.

Today, we will begin our consideration of Bill C-8, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.

To kick off this work, we have the pleasure of welcoming the Honourable Gary Anandasangaree, Minister of Public Safety. Thank you so much to you and your team for being with us today.

The minister is accompanied by the following officials from Public Safety Canada: Colin MacSween, Director General, National and Cyber Security Branch; and Kelly-Anne Gibson, Director, National Cyber Security Policy, National and Cyber Security Branch.

From Innovation, Science and Economic Development Canada, we have Andre Arbour, Director General, Telecommunications and Internet Policy Branch; and Wen Kwan, Director General, Spectrum and Telecommunications Sector. Thank you for joining us today.

We will begin by inviting the minister to provide opening remarks, followed by questions from our members.

Minister, welcome.

**Hon. Gary Anandasangaree, P.C., M.P., Minister of Public Safety:** Thank you, Senator Deacon. I'm going to ask for your indulgence at the outset, if I may, just to acknowledge, first, your chairship today and going forward of this very important committee. I want to congratulate you. I know that Senator Yussuff has left big shoes to fill, but I have absolute confidence in the work that you will, no doubt, do.

I want to thank Senator Yussuff for his leadership on a range of issues and for being someone I have been able to count on and call on as a friend for advice — often solicited but sometimes unsolicited. It's always a pleasure hearing from him. I want to thank you, sir, for your leadership and your many years of service.

I also want to take a moment to acknowledge Senator Kutcher, whom I have had the pleasure of working with at the previous Special Joint Committee on Medical Assistance in Dying. We have mutual friends, and he is someone who over the years has distinguished himself as a very hard-working, smart, intelligent senator who has always held this government and other governments to account. He comes from decades of service in

**Le sénateur Kutcher :** Stan Kutcher, de la Nouvelle-Écosse, le côté de la table qui donne sur la côte Est.

**La présidente :** Nous sommes heureux de vous compter des nôtres, sénateur Kutcher, et je vous remercie.

Nous allons entamer l'examen du projet de loi C-8, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois.

Pour donner le coup d'envoi de ces travaux, nous avons le plaisir d'accueillir l'honorable Gary Anandasangaree, ministre de la Sécurité publique et de la Protection civile. Merci de vous joindre à nous, monsieur le ministre.

Le ministre est accompagné de fonctionnaires de Sécurité publique Canada, soit : Colin MacSween, directeur général, Direction de la sécurité nationale et de la cybersécurité, et Kelly-Anne Gibson, directrice, Politique cybersécurité nationale, Direction de la sécurité nationale et de la cybersécurité,

D'Innovation, Sciences et Développement économique du Canada, nous accueillons André Arbour, directeur général, Direction générale des politiques des télécommunications et de l'Internet, et Wen Kwan, directeur général, Secteur du spectre et des télécommunications.

Nous commencerons par inviter le ministre à prononcer quelques mots, après quoi nos membres pourront lui poser des questions.

Bienvenue au comité, monsieur le ministre.

**L'honorable Gary Anandasangaree, c.p., député, ministre de la Sécurité publique :** Merci, sénatrice Deacon. Permettez-moi tout d'abord de faire appel à votre indulgence et de commencer par saluer votre prise de fonction pour présider aux destinées de ce comité très important. Je vous en félicite. Je sais que le sénateur Yussuff laisse un vide difficile à combler, mais j'ai une confiance absolue dans le travail que vous accomplirez et ne doute pas de votre succès.

Je tiens à remercier le sénateur Yussuff pour son leadership dans tout un éventail de questions et pour avoir été une personne sur laquelle j'ai pu compter et à qui j'ai pu m'adresser en tant qu'ami pour obtenir des conseils — souvent sollicités, mais parfois spontanés. C'est toujours un plaisir d'avoir de vos nouvelles, sénateur, et je tiens à vous remercier pour votre leadership et vos nombreuses années de service.

Je tiens également à prendre un instant pour rendre hommage au sénateur Kutcher, avec qui j'ai eu le plaisir de travailler au sein de l'ancien Comité mixte spécial sur l'aide médicale à mourir. Nous avons des amis communs, et c'est quelqu'un qui, au fil des ans, s'est distingué comme un gros travailleur, un sénateur avisé et intelligent, qui a toujours demandé des comptes à ce gouvernement et aux gouvernements précédents. Il compte

academia and in medicine. So thank you, Stan, if I may call you Stan at this moment, for your friendship and leadership. I wish you all the best in — "retirement" is probably not the right term, but certainly retirement from the Senate. We look forward to the work that you will continue to do.

With that, Madam Chair, I will start our time. I'd like to get this Formula 1 car on the road.

If I may, I will start by acknowledging that we are gathered and meeting on the traditional, unceded territory of the Algonquin Anishinaabe people.

[*Translation*]

It's my pleasure to speak to you today about Bill C-8, an act respecting cybersecurity.

[*English*]

Many of you are already familiar with this bill, having studied a previous iteration and understand that this piece of legislation is critical to protecting Canada's sovereignty, resilience and critical infrastructure.

According to the Communications Security Establishment Canada, or CSE, cybercrime is now one of the most pressing and dangerous threats to Canadians and their businesses.

[*Translation*]

Canada ranks second in the world for countries most affected by ransomware attacks.

[*English*]

Costly and harmful cyberattacks are increasing in frequency, in parallel with our reliance on the technologies under threat. We have all used the internet, smartphones and other technologies that have become essential to our ways of life.

In addition, emerging technologies, like artificial intelligence, are increasingly becoming integral to the ways we work and communicate.

[*Translation*]

All of this means we're that much more vulnerable to cyberthreats.

[*English*]

This is why Bill C-8 is critical. This iteration of the bill has been shaped by Senate considerations and consultations with stakeholders.

des décennies de service dans le milieu universitaire et dans le domaine médical. Merci donc, sénateur Kutcher, pour votre amitié et votre leadership. Je vous souhaite bonne chance dans votre... « retraite » n'est probablement pas le terme idoine, mais je dirais dans votre vie après le Sénat. Nous avons hâte de savoir à quoi vous allez consacrer votre temps.

Sur ce, madame la présidente, je vous invite à déclencher le chronomètre pour votre départ en Formule 1.

Permettez-moi d'abord de rappeler que nous nous sommes réunis sur le territoire traditionnel et non cédé du peuple algonquin anishinabe.

[*Français*]

Je suis heureux de vous parler aujourd'hui du projet de loi C-8, Loi concernant la cybersécurité.

[*Traduction*]

Beaucoup d'entre vous connaissent déjà ce projet de loi pour l'avoir étudié dans une version antérieure et comprennent que cette mesure législative est essentielle à la protection de la souveraineté, de la résilience et des infrastructures essentielles du Canada.

Selon le Centre de la sécurité des télécommunications, le CST, la cybercriminalité constitue désormais l'une des menaces les plus pressantes et les plus dangereuses pour les Canadiens et leurs entreprises.

[*Français*]

Le Canada se classe au second rang mondial des pays les plus touchés par les attaques de rançongiciels.

[*Traduction*]

Les cyberattaques coûteuses et préjudiciables se multiplient, en même temps que notre dépendance vis-à-vis des technologies qu'elles visent. Nous utilisons tous Internet, les téléphones intelligents et d'autres technologies qui sont désormais indispensables à notre mode de vie.

De plus, les technologies émergentes, comme l'intelligence artificielle, font de plus en plus partie intégrante de nos modes de travail et de communication.

[*Français*]

Cela signifie que nous sommes d'autant plus vulnérables aux cybermenaces.

[*Traduction*]

C'est pourquoi le projet de loi C-8 est fondamental. Cette version du projet de loi découle des délibérations du Sénat et des consultations menées auprès des parties prenantes.

[*Translation*]

Bill C-8 has two main parts.

[*English*]

First, it would amend the Telecommunications Act to strengthen the security of Canada's telecommunications framework by adding "to promote the security of the Canadian telecommunications system" as a policy objective in the act; giving the Governor-in-Council and the Minister of Industry the power to compel telecommunications service providers to take action, when necessary, in the face of threats; and adding measures on monitoring and enforcement, including an administrative monetary penalty scheme.

Second, it would amend the critical cyber systems protection act, or CCSPA, by establishing a regulatory regime to strengthen cybersecurity in the federally regulated finance, telecommunications, energy and transportation sectors; increasing information sharing; providing the Governor-in-Council with the power to issue cyber security directions to protect a critical cyber system; obligate designated operators to establish a cybersecurity program; and establish enforcement powers and consequences such as an administrative monetary penalty regime.

These measures are necessary to protect Canadians, our economy and our critical infrastructure.

We must keep pace with our allies in the Five Eyes and G7, as well as ensure we do not fall further behind those who have already introduced similar cybersecurity legislation.

Madam Chair, the cost of recovering from an incident is far greater than the cost of investing in cybersecurity up front. It is critical that we are proactive in setting our systems for success so that we can continue to keep Canadians safe in all aspects of their lives.

[*Translation*]

Thank you, and I look forward to your questions.

[*English*]

The Honourable Mélanie Joly, Minister of Industry, will also be coming to the committee on a separate occasion, so if there are specific issues with respect to telecommunications — though I'm glad to answer questions — they may also be posed to her, and she will also be able to elaborate.

[*Français*]

Le projet de loi C-8 contient deux principales parties.

[*Traduction*]

Premièrement, il modifie la Loi sur les télécommunications afin de renforcer la sûreté du cadre de télécommunications du Canada en ajoutant la promotion de la sûreté du système de télécommunications canadien en tant qu'objectif stratégique; en conférant au gouverneur en conseil et au ministre de l'Industrie le pouvoir de contraindre les fournisseurs de services de télécommunications à prendre des mesures face aux menaces; et en ajoutant des mesures de surveillance et d'application de la loi, notamment un cadre de réglementation des sanctions administratives pécuniaires.

Deuxièmement, il modifie la LPCE, la Loi sur la protection des cybersystèmes essentiels, en mettant en place un cadre de réglementation qui vise à renforcer la cybersécurité dans les secteurs de la finance, des télécommunications, de l'énergie et des transports, qui relèvent de la compétence fédérale; en renforçant l'échange de renseignements; en conférant au gouverneur en conseil le pouvoir d'émettre des directives en matière de cybersécurité afin de protéger un système cybercritique; en obligeant les exploitants désignés à mettre en place un programme de cybersécurité; et en établissant des pouvoirs d'application et des sanctions, comme un régime de sanctions administratives pécuniaires.

Ces mesures sont nécessaires pour protéger les Canadiens, notre économie et nos infrastructures essentielles.

Nous devons rester en phase avec nos alliés du Groupe des cinq et du G7, et veiller à ne pas prendre plus de retard par rapport à ceux qui disposent déjà d'une législation semblable en matière de cybersécurité.

Madame la présidente, le coût de la reprise après un incident est bien supérieur à celui d'un investissement dans la cybersécurité. Nous devons absolument être proactifs et mettre en place les conditions nécessaires à la réussite de nos systèmes afin de pouvoir continuer à assurer la sécurité des Canadiens dans tous les aspects de leur vie.

[*Français*]

Je vous remercie. Je serai heureux de répondre à vos questions.

[*Traduction*]

L'honorable Mélanie Joly, ministre de l'Industrie, se présentera également devant le comité à une autre occasion; ainsi, si vous avez des questions spécifiques concernant les télécommunications — même si je me ferai un plaisir d'y répondre —, vous pourrez également les lui poser, et elle sera en mesure de vous donner des précisions.

With that, I look forward to your questions and comments.

**The Chair:** Thank you, minister.

Just before we proceed, I'd like to welcome Senator Cardozo, from Ontario, who just joined us.

I'd also like to let the rest of the room know that Senator McNair is the sponsor of this bill. Thank you for the work you're doing.

No pressure, Senator Kutcher. We hope you enjoy this final meeting with us. That is wonderful to hear too.

I have talked about the sponsor of the bill, but I'd also like to thank Senator Batters for being here as the critic of the bill. Thank you for joining us.

We'll now proceed to questions. I'd like to note that the minister will be with us until about five o'clock. We'll do our best to allow all members to ask a question during this first hour. A second round of questions with the officials will take place from 5:00 to 5:55. With this in mind, four minutes will be allotted for each question, including the answer. I'd ask that you keep the question part as succinct as possible so we can have as many interventions as possible.

I'd like to offer the first question to our deputy chair, Senator Al Zaibak.

**Senator Al Zaibak:** Thank you, Madam Chair, and congratulations.

Minister Anandasangaree, welcome back to this committee. Thank you to you and your team for your efforts in advancing Canada's cybersecurity framework at a time of increasing global instability.

As cyber-threats become a central tool of statecraft, how does Bill C-8 position Canada to better deter and respond to state-sponsored cyber activity, particularly from hostile actors?

**Mr. Anandasangaree:** Thank you, Senator Al Zaibak, for that question. Let me also acknowledge Senator Batters and, of course, Senator McNair for being the critic and the sponsor of this bill, respectively. I value both of their perspectives, and I want to thank them for the work they've done.

Sur ce, j'ai maintenant hâte de répondre à vos questions et de recueillir vos commentaires.

**La présidente :** Merci, monsieur le ministre.

Avant de poursuivre, je tiens à souhaiter la bienvenue au sénateur Cardozo, de l'Ontario, qui vient de se joindre à nous.

Je tiens par ailleurs à préciser à notre honorable assemblée que le sénateur McNair est le promoteur de ce projet de loi. Merci pour votre travail, sénateur.

Pas de pression, sénateur Kutcher. Nous espérons que vous apprécierez cette dernière réunion avec nous. C'est également très agréable à entendre.

Après avoir mentionné le promoteur du projet de loi, je veux aussi remercier la sénatrice Batters pour sa présence en tant que critique du projet de loi. Merci de vous être jointe à nous.

Passons aux questions. Je tiens à préciser que le ministre restera parmi nous jusqu'à environ 17 heures. Nous ferons de notre mieux pour permettre à tous les membres de poser une question au cours de cette première heure. Une deuxième série de questions avec les fonctionnaires aura lieu de 17 heures à 17 h 55. Dans cette optique, quatre minutes seront allouées à chaque question, réponse comprise. Je vous demanderais de formuler votre question de la manière la plus concise possible afin que nous puissions avoir le plus grand nombre d'interventions possible.

J'invite notre vice-président, le sénateur Al Zaibak, à poser la première question.

**Le sénateur Al Zaibak :** Merci, madame la présidente, et félicitations.

Monsieur le ministre Anandasangaree, bienvenue à nouveau devant ce comité. Je tiens à vous remercier, vous et votre équipe, pour les efforts que vous déployez afin de faire progresser le cadre de cybersécurité du Canada dans un contexte d'instabilité mondiale croissante.

Alors que les cybermenaces deviennent un outil central de la politique d'État, comment le projet de loi C-8 permet-il au Canada de mieux dissuader et de mieux réagir face aux cyberactivités soutenues par des États, en particulier celles attribuables à des acteurs hostiles?

**M. Anandasangaree :** Merci, sénateur Al Zaibak, pour cette question. Moi aussi, je veux remercier la sénatrice Batters de même, bien sûr, que le sénateur McNair, respectivement critique et promoteur de ce projet de loi. J'apprécie leurs points de vue respectifs et je tiens à les remercier pour le travail qu'ils ont accompli.

Every day, we come across new threats, especially cyber-threats, often using ransomware as a tool. Often, we see corporations — big corporations sometimes — paying out due to ransomware. Much of that is unreported. There's no compulsion to report that right now, but it is increasing at a scale and speed that I don't think any of us anticipated. This is likely to be even more complicated as AI and other tools are developed at speeds that we have not seen.

Whether by state actors or others, the use of cyberattacks has become a very critical tool of other states and parties to not just raise money but also to impact the personal privacy rights of individual Canadians.

Several weeks ago, we saw, for example, an attack on a major Canadian insurance company. I can go through a list of other attacks over the past several months alone. Suffice to say that it is at alarming speeds and a scale that we probably never could have anticipated even a couple of years ago.

**Senator Al Zaibak:** Thank you, minister. How does Bill C-8 ensure interoperability with Five Eyes partners, especially in responding to cross-border cyber-threats targeting shared infrastructure?

**Mr. Anandasangaree:** We were very much part of both the Five Eyes and G7, and I'll combine them both in my answer. I've had the opportunity to be part of both conversations. We hosted the G7 in October, and I can tell you this is one of the most important issues that they're dealing with. There's a great deal of cooperation among both our Five Eyes and G7 partners, but, of course, Canada lags behind with respect to other countries in terms of our regime. I hope that will be corrected with the passage of Bill C-8.

**Senator Al Zaibak:** Thank you.

**The Chair:** Next, we go to other members of our steering committee.

[*Translation*]

**Senator Carignan:** Congratulations on your appointment, Madam Chair.

Minister, by definition, a law is a set of general and impersonal rules. This bill gives the Governor-in-Council the power to establish directions or to order an individual designated operator to comply with specific measures. That means that a direction can target a specific business. The scope of the direction is fairly broad in that the impact on the business is

Nous sommes quotidiennement confrontés à de nouvelles menaces, comme celles reposant sur des rançongiciels. Nous voyons souvent des entreprises — parfois de grandes entreprises — céder et payer les rançons exigées. Ces cas sont rarement signalés. Il n'y a actuellement aucune obligation de signaler ces incidents, mais leur ampleur et leur fréquence augmentent à un rythme qu'aucun de nous n'avait prévu. La situation risque vraisemblablement de se compliquer davantage tandis que l'IA et d'autres outils se développent à une vitesse sans précédent.

Que ce soit de la part d'acteurs étatiques ou d'autres, le recours aux cyberattaques est devenu un outil essentiel pour d'autres États et parties prenantes, non seulement pour extraire de l'argent, mais aussi pour porter atteinte au droit à la vie privée des personnes canadiennes.

Il y a quelques semaines, nous avons par exemple assisté à une cyberattaque contre une grande compagnie d'assurance canadienne. Je pourrais aussi vous citer toute une série d'attaques survenues au cours des derniers mois seulement. Il suffit de dire que ces attaques se multiplient à un rythme alarmant et atteignent une ampleur que nous n'aurions probablement jamais pu imaginer il y a encore quelques années.

**Le sénateur Al Zaibak :** Merci, monsieur le ministre. En quoi le projet de loi C-8 permet-il de garantir l'interopérabilité avec les partenaires du Groupe des cinq, notamment pour faire face aux cybermenaces transfrontalières visant les infrastructures communes?

**M. Anandasangaree :** Nous participons activement aux travaux du Groupe des cinq et du G7, et je vais les grouper dans ma réponse. J'ai eu l'occasion de participer aux discussions dans les deux cas. Nous avons accueilli le G7 en octobre, et je peux vous dire que c'est l'un des enjeux les plus importants pour ses membres. Il y a beaucoup de coopération entre les partenaires du Groupe des cinq et du G7, mais notre système est effectivement en retard par rapport aux autres pays. J'espère que ce sera corrigé avec l'adoption du projet de loi C-8.

**Le sénateur Al Zaibak :** Merci.

**La présidente :** Nous allons maintenant passer aux autres membres de notre comité directeur.

[*Français*]

**Le sénateur Carignan :** Félicitations pour votre nomination, madame la présidente.

Monsieur le ministre, par définition, une loi est un ensemble de normes générales et impersonnelles. Dans ce projet de loi, on donne au gouverneur en conseil le pouvoir d'établir des directives qui peuvent être données ou d'exiger certaines mesures de la part d'un exploitant désigné individuellement. Au moyen de la directive, on peut donc viser une entreprise en

taken into account. However, paragraph 20(3)(e) indicates "any other factor that the Governor in Council considers to be relevant" and subclause 20(3.1) states the following, and I quote:

> The provisions of the direction must, in scope and substance, be reasonable in relation to the purpose of protecting a critical cyber system.

The law already defines what, in your opinion, would be reasonable. How do you think that we can prevent abuses of power? How can the courts fulfill their traditional role of curbing such abuses of power when these parameters are so broad?

[*English*]

**Mr. Anandasangaree:** Thank you, senator, for the question.

The powers bestowed right now by way of order of the Governor-in-Council with respect to each operator are to ensure that there's compliance and capability within the respective areas of regulation within an industry, for example, telecommunications.

The safeguards that are in place are important. When order-making powers are used, there is reference to both the National Security and Intelligence Committee of Parliamentarians, or NSICOP, and the National Security and Intelligence Review Agency, or NSIRA. When issues are of a confidential nature — in some cases, they have to be, for example, to ensure that industry is able to protect certain aspects of a business interest that they may not want to share. However, to ensure they still comply with the act, it is critical to have that specific set of guidelines for that particular industry, with some safeguards.

There is certainly the ability to have the matter go to the Federal Court. It is certainly within the purview. They may not want to, but within the safeguards that are built in, the reasonableness standard is the starting point, which is a legal standard that is fairly well understood. However, coupled with that is the potential for oversight with NSICOP and NSIRA if they choose to respond to a referral based on the act.

There are safeguards in place, and I believe that overreach is something that could be captured by them.

[*Translation*]

**Senator Carignan:** As for the provision regarding the five-year review, many laws contain such a provision, but the review does not happen. At the National Security and Intelligence Committee of Parliamentarians, you indicated that this provision was set out in the legislation that was passed several years ago, but that the review has not yet been

particulier. Le pouvoir ou l'encadrement de la directive est assez général, en ce sens que l'on prend en considération les répercussions sur l'entreprise. Cependant, à l'alinéa 20(3)e), on dit : « tout autre facteur que le gouverneur en conseil considère pertinent [...] » et, au paragraphe 20(3.1), on précise ceci :

> La portée et la teneur des dispositions de la directive sont raisonnables eu égard à l'objectif de protéger un cybersystème essentiel.

Dans la loi, on détermine déjà ce qui, selon vous, sera raisonnable. Comment croyez-vous qu'on pourra éviter les abus de pouvoir? Comment les tribunaux pourront-ils jouer leur rôle traditionnel, qui est de contrôler ces abus de pouvoir, avec un encadrement aussi large?

[*Traduction*]

**M. Anandasangaree :** Merci de la question, sénateur.

Les pouvoirs actuellement conférés par décret à l'égard de chaque exploitant visent à garantir le respect de la réglementation et la capacité opérationnelle dans les domaines réglementaires concernés au sein d'un secteur, par exemple celui des télécommunications.

Les garanties mises en place sont importantes. Les pouvoirs décisionnels renvoient à la fois au CPSNR, le Comité des parlementaires sur la sécurité nationale et le renseignement et à l'OSSNR, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement. Quand les enjeux sont de nature confidentielle... c'est parfois nécessaire, par exemple pour permettre aux entreprises de protéger certains aspects de leurs intérêts commerciaux qu'elles ne souhaitent pas divulguer. Cela dit, pour garantir que les exploitants respectent la loi, il faut absolument que, pour tel ou tel secteur d'activité, des lignes directrices assorties de certaines garanties soient appliquées.

Il est tout à fait possible de saisir la Cour fédérale. Cela relève effectivement de sa compétence. C'est au gré de chacun, mais, dans le cadre des garanties prévues, le critère du caractère raisonnable est le point de départ, et c'est un critère juridique généralement bien compris. Cela s'accompagne cependant d'un éventuel contrôle de la part du CPSNR et de l'OSSNR si ceux-ci décident de donner suite à un renvoi en vertu de la loi.

Des garanties sont donc en place, et je suis convaincu que ces dernières permettent de remédier à tout abus.

[*Français*]

**Le sénateur Carignan :** Pour ce qui est de la disposition portant sur la révision dans cinq ans, plusieurs lois en contiennent une, mais on ne fait pas cette révision. Au Comité des parlementaires sur la sécurité nationale et le renseignement, vous avez affirmé que cette disposition était contenue dans la loi et que la loi a été adoptée depuis plusieurs années, mais que la

conducted. How will you ensure that this legislation will be reviewed in five years?

[*English*]

**Mr. Anandasangaree:** There are a number of acts. Bill C-12 just went through this committee. There's a review period built in there. It's customary with respect to NSICOP itself and NSIRA that there is need for review. Those are reviews that need to happen, and in this case, on a five-year timeline. It is up to parliamentarians and governments to ensure that those reviews take place.

**Senator Cardozo:** First, congratulations, Madam Chair, on your election.

Thank you, minister, for being here. Bill C-26 in the previous Parliament was introduced in June 2022, so four years ago. I wonder if you can talk a little bit about how the threat situation has changed since then and how the bill reflects that.

Specifically, with respect to adding sectors that you could be looking at or the regulations as outlined in clause 15, are those regulations pretty much ready to go or will that take a while? In terms of sectors, you haven't looked at, for example, the education sector, where universities sometimes have a concern or problem. I know that's a provincial jurisdiction, but I wonder if you can talk about whether that can be added to the picture.

**Mr. Anandasangaree:** Thank you. The observation of the passage of time is of critical importance. I can give you the number of incidents in the past couple of years, since 2022, that have had a significant impact on Canadians. I referenced the insurance company. In August 2025, we had Wealthsimple. In July 2025, we had the Colabar Group. In June 2025, we had Pembroke Regional Hospital and WestJet. We had Nova Scotia Power in April 2025. We had Shell in June 2024. Then there was the City of Hamilton, and I could go on. It has escalated in a significant way over the past number of years.

With reference to the four industries that are subject to this act — finance, telecommunications, energy and transport — those are the four that are primarily in the federal domain. When you referenced education, for example, that is very much of a provincial nature.

There's an interplay with respect to telecom because telecom, in a broader sense, will have implications for health systems or education systems, which are run by the provinces. Breaches through the telecom sector will certainly have some implications and are subject to the act.

révision n'a pas encore été faite. Comment vous assurerez-vous que cette loi sera révisée dans cinq ans?

[*Traduction*]

**M. Anandasangaree :** Il y a un certain nombre de lois. Le projet de loi C-12 vient tout juste d'être examiné par ce comité. Une période de révision y est prévue. Il est d'usage, en ce qui concerne le CPSNR et l'OSSNR, de prévoir des révisions. Elles sont nécessaires, et, en l'occurrence, sont prévues dans un délai de cinq ans. Il appartient aux parlementaires et aux gouvernements de veiller à ce que ces révisions soient effectuées.

**Le sénateur Cardozo :** Tout d'abord, félicitations pour votre élection, madame la présidente.

Merci de votre présence, monsieur le ministre. Le projet de loi C-26 a été présenté au cours de la législature précédente, en juin 2022, il y a quatre ans. Pourriez-vous nous dire quelques mots sur l'évolution de la menace depuis et sur la façon dont le projet de loi en tient compte?

Plus précisément, concernant l'ajout de secteurs que vous pourriez envisager ou la réglementation décrite à l'article 15, les règlements sont-ils près d'entrer en vigueur ou cela prendra-t-il encore un certain temps? Au sujet des secteurs, vous n'avez pas encore examiné, par exemple, celui de l'éducation, où les universités sont parfois confrontées à des préoccupations ou à des problèmes. Je sais que cela relève de la compétence des provinces, mais pourriez-vous nous dire si ce secteur pourrait être intégré?

**M. Anandasangaree :** Merci. L'observation de la situation au fil du temps est d'une importance cruciale. Je peux vous fournir le nombre d'incidents qui, depuis quelques années, depuis 2022, ont eu un impact significatif sur les Canadiens. J'ai parlé des compagnies d'assurances. En août 2025, il y a eu l'affaire Wealthsimple. En juillet 2025, il y a eu le groupe Colabar. En juin 2025, il y a eu l'hôpital régional de Pembroke et WestJet. Il y a eu Nova Scotia Power en avril 2025. Il y a eu Shell en juin 2024. Ensuite, il y a eu la municipalité de Hamilton, et je pourrais continuer. La situation s'est considérablement aggravée depuis quelques années.

Les quatre secteurs visés par cette loi — les finances, les télécommunications, l'énergie et les transports — sont ceux qui sont principalement de compétence fédérale. Vous avez évoqué l'éducation, par exemple, mais c'est un secteur qui relève très largement de la compétence des provinces.

Il y a une interaction avec le secteur des télécommunications, puisque celui-ci, au sens large, est lié aux systèmes de santé ou d'éducation, qui relèvent de la compétence des provinces. Les atteintes à la sécurité dans le secteur des télécommunications auront évidemment des conséquences et seront sanctionnées par la loi.

With the evolution with respect to regulation, there is flexibility. On issues of AI, for example, as technology develops, there is an evergreen set of regulations that can be brought in to ensure — and we speak about the actual underlying architecture and not necessarily the content — can be addressed through regulation.

At this point — my colleagues may be able to speak to it in greater detail — this changes the bill. We've had a number of changes from Bill C-26. I don't believe the regulations are quite ready to go, but as soon as this bill passes, we will be able to move on the regulations quite fast. There are also the usual timelines once it's gazetted. There's a 30-day window or a certain time frame to get input before regulations become law.

**Senator Cardozo:** If there are other sectors you need to go to, do you have the ability to add that or are we stuck with these four?

**Mr. Anandasangaree:** Primarily, the focus is on these four because they are in the federal domain. We need to work with the provinces and territories to see if there are replicate bills that can be undertaken there or some reporting mechanisms, but so far, these four have been strictly in the federal domain.

**Senator Cardozo:** Good luck. This is urgent, and I hope it gets moving soon.

**Senator Batters:** Thanks very much. Minister, in your second reading speech, you argued it's urgent to pass Bill C-8 because cyber-threats are becoming more numerous, sophisticated and pervasive. After a decade of consultation and after the Senate's in-depth study of Bill C-26, and despite six months between that previous bill dying on the Order Paper because the government chose to prorogue, why did the government choose to reintroduce a virtually identical bill instead of making important revisions from the start that would have addressed the major flaws identified by key witnesses at this committee and allowed Parliament to move forward more quickly on that? Isn't there a contradiction between the urgency you're invoking and the lack of diligence that your government showed in preparing this bill initially last year?

**Mr. Anandasangaree:** I would beg to differ, senator. There was an urgency to produce the bill. The previous bill, Bill C-26, had gone through all the different stages. It was at Parliament's doorstep for a technical amendment. The work of Senator

L'évolution de la réglementation offre une certaine souplesse. Concernant les enjeux liés à l'IA, par exemple, les progrès technologiques s'accompagnent d'un cadre réglementaire évolutif qui peut être instauré pour garantir que ces enjeux — et on parle ici de l'architecture elle-même, et non pas nécessairement du contenu — puissent être abordés par le biais de règlements.

À ce stade — mes collègues pourront peut-être vous en dire davantage —, cela change le projet de loi. Nous avons apporté un certain nombre de modifications au projet de loi C-26. Je ne crois pas que les règlements soient tout à fait prêts, mais, dès que le projet de loi aura été adopté, nous pourrons progresser très rapidement. Il y a aussi les délais habituels après publication dans la *Gazette*. Il y a une période de 30 jours ou un certain délai pour recueillir des commentaires avant que les règlements n'entrent en vigueur.

**Le sénateur Cardozo :** Si d'autres secteurs doivent être couverts, êtes-vous habilité à les ajouter ou sommes-nous limités à ces quatre-là?

**M. Anandasangaree :** Nous nous concentrons principalement sur ces quatre secteurs, parce qu'ils sont de compétence fédérale. Nous devons travailler avec les provinces et les territoires pour voir s'il est possible d'y proposer des projets de loi semblables ou s'il y existe des mécanismes de reddition des comptes, mais, jusqu'à présent, ces quatre secteurs sont strictement de compétence fédérale.

**Le sénateur Cardozo :** Bonne chance. C'est urgent, et j'espère que les choses vont bientôt avancer.

**La sénatrice Batters :** Merci beaucoup. Monsieur le ministre, dans votre discours en deuxième lecture, vous avez fait valoir qu'il était urgent d'adopter le projet de loi C-8, parce que les cybermenaces sont de plus en plus nombreuses, complexes et omniprésentes. Après une décennie de consultations et après l'étude approfondie du projet de loi C-26 par le Sénat, et malgré les six mois écoulés depuis que ce dernier est mort au Feuilleton en raison de la prorogation, pourquoi le gouvernement a-t-il décidé de présenter à nouveau un projet de loi pratiquement identique au lieu d'y apporter d'emblée les modifications importantes qui auraient corrigé les principales lacunes relevées par d'importants témoins devant ce comité et qui auraient permis au Parlement de faire avancer ce dossier plus rapidement? N'y a-t-il pas contradiction entre l'urgence que vous invoquez et le manque de diligence dont votre gouvernement a fait preuve au moment de la préparation initiale de ce projet de loi l'année dernière?

**M. Anandasangaree :** Je ne suis pas de votre avis, sénatrice. Il était urgent de présenter ce projet de loi. Le projet de loi C-26 qui le précède avait franchi toutes les étapes. Il était sur le point d'être examiné par le Parlement pour un amendement technique.

McNair in that is noteworthy. It was to ensure that the bill was able to get Royal Assent.

Of course, when we introduced that bill, our expectation was that if there were new items that came up, we would work with our opposition. Some 75% of the amendments we accepted were from opposition, which is quite remarkable because we had a sense that working in collaboration was critical. This is not a bill to be politicized. For the most part, we were working with the different parties in the House to ensure that all those valid concerns were taken into account as amendments. We were able to pass those amendments, which are now before you.

**Senator Batters:** Right. The only thing is that many of those concerns had already been brought up in the previous iteration and could have been made before you introduced it. The technical amendment you spoke of could have potentially knocked out half your bill, so, yes, it was important to make it.

However, there were three important amendments made by Conservative MPs at the House committee on Bill C-8, which would have required that judicial authorization before ministerial powers and ministerial orders be allowed in certain instances under this statute. Your Liberal government chose to oppose those key amendments rather than agreeing to have those changes made to Bill C-8. You could have agreed to include those judicial authorization amendments in Bill C-8, but you hadn't learned those lessons that were articulated by many witnesses who testified at our Senate committee during the Bill C-26 hearings. Nearly all the witnesses who testified, other than government witnesses, strongly advocated for more oversight, which would have been accomplished by that type of judicial authorization.

Minister, why didn't your government agree to make those types of key amendments to improve the bill and protect Canadians' rights by putting those important judicial authorization measures into Bill C-8?

**Mr. Anandasangaree:** Senator, I believe those amendments were ruled out of scope.

**Senator Batters:** You could have chosen to put them in.

**Mr. Anandasangaree:** Having a bill go through the different processes is neither an art nor a science. It's a bit of both. This is a bill, for all intents and purposes, passed in its first iteration as Bill C-26. It has been improved, and it improved because all parties worked together, and it is now before this house. I believe that the strengthened bill should pass. There is an urgency and a

Le travail du sénateur McNair à cet égard mérite d'être souligné. L'objectif était de garantir que le projet de loi obtienne la sanction royale.

Quand nous avons présenté ce projet de loi, nous espérions évidemment que, si de nouveaux éléments devaient être examinés, nous pourrions travailler avec l'opposition. Environ 75 % des amendements que nous avons acceptés venaient de l'opposition, ce qui est tout à fait remarquable, car il nous semblait essentiel de travailler en collaboration. Ce projet de loi ne doit pas être politisé. La plupart du temps, nous avons travaillé avec les différents partis représentés à la Chambre pour veiller à ce que toutes les préoccupations légitimes soient prises en compte sous forme d'amendements. Nous avons réussi à faire adopter ces amendements, qui vous sont soumis aujourd'hui.

**La sénatrice Batters :** D'accord. Le seul problème est que beaucoup de ces préoccupations avaient déjà été soulevées auparavant et qu'elles auraient pu être traitées avant que le projet de loi soit présenté. L'amendement technique dont vous parlez aurait pu éliminer la moitié de votre projet de loi. Il était donc effectivement important de le proposer.

Mais les députés conservateurs ont proposé trois amendements importants au comité de la Chambre au sujet du projet de loi C-8, et ces amendements auraient exigé une autorisation judiciaire pour permettre l'exercice des pouvoirs ministériels et des décrets ministériels dans certains cas prévus par cette loi. Votre gouvernement libéral a décidé de s'opposer à ces amendements déterminants plutôt que d'accepter que ces modifications soient apportées au projet de loi C-8. Vous auriez pu accepter d'inclure ces amendements d'autorisation judiciaire dans le projet de loi C-8, mais vous n'aviez pas tiré les leçons des recommandations formulées par de nombreux témoins qui ont comparu devant notre comité sénatorial au cours des audiences concernant le projet de loi C-26. Presque tous les témoins, à l'exception de ceux du gouvernement, ont vigoureusement plaidé en faveur d'un renforcement de la surveillance, et c'est ce qu'aurait permis ce type d'autorisation judiciaire.

Monsieur le ministre, pourquoi votre gouvernement n'a-t-il pas accepté d'apporter ces modifications essentielles pour améliorer le projet de loi et protéger les droits des Canadiens en intégrant des mesures importantes en matière d'autorisation judiciaire dans le projet de loi C-8?

**M. Anandasangaree :** Sénatrice, je crois que ces amendements ont été jugés hors champ.

**La sénatrice Batters :** Vous auriez pu décider de les inclure.

**M. Anandasangaree :** Le processus qui fait passer un projet de loi par différentes étapes n'est ni un art ni une science. C'est un peu des deux. À toutes fins utiles, c'est un projet de loi qui a été adopté dans sa première version sous l'appellation de projet de loi C-26. Il a été amélioré, et ce grâce à la collaboration de tous les partis, et il est maintenant soumis à cette chambre.

need, and we need to work collaboratively to get to the point of passage of this bill.

**Senator Batters:** Do you not think the judicial authorization measures are required?

**Mr. Anandasangaree:** As I have indicated from the outset, the safeguards are there. There are references to NSIRA and NSICOP. There are some matters that are of a confidential nature that require protection, but entities have the ability to go to court if they so desire. Those safeguards are in place.

**Senator McNair:** Chair, congratulations on your election.

Minister and officials, thank you for being here. We appreciate your attendance. You grabbed our attention at the beginning when you talked about how we're now second in the world for ransomware attacks. That is not a list we want to be on — not at that level, at least.

I was also going to ask questions about the three amendments made at the House committee, but Senator Batters covered those. I want to recognize that 37 amendments were made, and the committee should be recognized for the collaborative approach that it took.

I know the Privacy Commissioner in his appearance at the House committee made three recommendations. Two of them — as I understand it — were adopted by the committee in amendment, but the third was voted down. Can you speak to why the third amendment, which deals with the notification of privacy breaches directly to the Privacy Commissioner, was voted down by the committee?

**Mr. Anandasangaree:** Thank you, senator. You're quite right: A number of amendments have been accepted. Over 50% of the amendments were accepted, and 75% of those amendments came from opposition; they were not government amendments.

I had the opportunity to meet with the Privacy Commissioner in October of this year, and I certainly respect the work that they have done. With respect to the input we received, two of the three amendments have been taken into account. The third one, which is part of the Personal Information Protection and Electronic Documents Act, or PIPEDA, already requires an organization to notify the Privacy Commissioner along with affected individuals. It's already law under the Privacy Act for the disclosure to take place. That's the primary reason why it wasn't included in one of the amendments that went through committee.

**Senator McNair:** Is it already covered under PIPEDA?

J'estime que ce projet de loi renforcé devrait être adopté. C'est urgent et nécessaire, et nous devons travailler en collaboration pour parvenir à son adoption.

**La sénatrice Batters :** Ne pensez-vous pas que des mesures d'autorisation judiciaire seraient nécessaires?

**M. Anandasangaree :** Comme je l'ai dit dès le départ, on a prévu des garanties. Il y a des références à l'OSSNR et au CPSNR. Certaines questions sont de nature confidentielle et nécessitent une protection, mais les entités ont la possibilité de saisir la justice si elles le souhaitent. Ces garanties sont prévues.

**Le sénateur McNair :** Madame la présidente, félicitations pour votre élection.

Merci au ministre et aux fonctionnaires de leur présence parmi nous. Nous vous sommes reconnaissants d'être ici. Vous avez retenu notre attention dès le début de la réunion en nous disant que le Canada est aujourd'hui au deuxième rang des pays victimes d'attaques par rançongiciel. Ce n'est pas un classement dans lequel nous souhaitons figurer — pas à ce degré en tout cas.

J'avais également l'intention de poser des questions sur les trois amendements proposés en comité parlementaire, mais la sénatrice Batters vient d'en parler. Je rappelle que 37 amendements ont été adoptés par le comité, dont il faut saluer l'esprit de collaboration.

Je sais que le commissaire à la protection de la vie privée a recommandé trois mesures au comité parlementaire. Si j'ai bien compris, deux d'entre elles ont été adoptées sous forme d'amendements, mais la troisième a été rejetée. Pourriez-vous nous expliquer pourquoi ce troisième amendement, portant sur le signalement direct de violations de confidentialité au commissaire à la protection de la vie privée, a été rejeté par le comité?

**M. Anandasangaree :** Merci, sénateur. Vous avez tout à fait raison : un certain nombre d'amendements ont été adoptés. Plus de 50 % des amendements ont été adoptés, et 75 % d'entre eux venaient de l'opposition, et non du gouvernement.

J'ai eu l'occasion de rencontrer le commissaire à la protection de la vie privée en octobre dernier, et je respecte tout à fait le travail qu'il fait. Quant aux mesures qu'on nous a proposées, je rappelle que deux des trois amendements ont été retenus. Le troisième relève de la Loi sur la protection des renseignements personnels et les documents électroniques, ou LPRPDE, qui impose déjà à une organisation d'informer le commissaire ainsi que les intéressés. La divulgation est déjà prévue par la Loi sur la protection des renseignements personnels. C'est la principale raison pour laquelle cette proposition n'a pas été retenue par le comité.

**Le sénateur McNair :** C'est déjà prévu dans la LPRPDE?

**Mr. Anandasangaree:** That's correct.

**Senator McNair:** Currently, the Social Affairs, Science and Technology Committee of the Senate is studying Bill S-5, the connected care for Canadians act, and that is an act to remove data blocking and make electronic medical records and electronic health records connected and interoperable. At committee, senators are hearing that a system of interconnected records risks creating a larger target for cyberattacks. As we well know, the health sector has been targeted over the past few years.

Subclause 6(1) of the critical cyber systems protection act, or CCSPA, permits the Governor-in-Council to add other federally regulated critical infrastructure sectors to Schedule 1. You talked a little bit about this already. In this committee's report on Bill C-26, we recommended adding health systems within the legislative authority of Parliament to Schedule 1.

Has health security been considered in the context of Bill C-8?

**The Chair:** No, primarily for the reason I outlined previously. We are essentially staying in our lane. As you are aware, federal-provincial relations can often result in lengthy court cases that will ultimately keep the federal government in its lane and the provinces in theirs. Senator McNair, we want to use this as a model and work with the provinces and territories to bring them on board with similar mirrored legislation within their jurisdictions or other forms of regulations that will have an element of disclosure and information sharing within the country, which we desperately need.

I believe the way to do it is through a collaboration. If we were to legislate, I've been assured by counsel that will be challenged, so our primary objective is to have a bill that is in line with our constitutional abilities to make laws in specific areas, which, in this case, are the four that have been outlined.

I believe it is an important starting point. We don't expect this to be the end.

**Senator McNair:** Thank you.

**Senator Kutcher:** Chair, congratulations on your election. You have big shoes to fill.

Thank you very much, minister, for being here and for the kind words you said about Senator Yussuff. I want to continue with the health care issues and draw attention to virtual health care providers, whose regulation is not clear to me. Some of the

**M. Anandasangaree :** En effet.

**Le sénateur McNair :** Le Comité sénatorial permanent des affaires sociales, des sciences et de la technologie est en train d'étudier le projet de loi S-5, Loi visant un système de soins de santé connecté au Canada, qui vise à éliminer le cloisonnement des données et à rendre les dossiers médicaux et les dossiers de santé électroniques connectés et interopérables. Au comité, les sénateurs se font dire qu'un système de dossiers connectés risque de constituer une cible de plus grande ampleur pour les cyberattaques. Personne n'ignore que le secteur de la santé a fait l'objet d'attaques dans les dernières années.

Le paragraphe 6(1) de la LPCSE, la Loi sur la protection des cybersystèmes essentiels, permet au gouverneur en conseil d'ajouter d'autres secteurs d'infrastructures essentielles relevant de la réglementation fédérale à l'annexe 1. Vous en avez déjà un peu parlé. Dans notre rapport sur le projet de loi C-26, nous avons recommandé d'ajouter les systèmes de santé relevant de la compétence du Parlement à l'annexe 1.

Est-ce qu'on a tenu compte de la sécurité du secteur de la santé dans le cadre du projet de loi C-8?

**La présidente :** Non, principalement pour la raison que j'ai exposée antérieurement. Nous restons essentiellement dans notre domaine de compétence. Comme vous le savez, les relations fédérales-provinciales peuvent souvent entraîner de longues procédures judiciaires qui finissent par confirmer le gouvernement fédéral dans son domaine de compétence et les provinces dans le leur. Sénateur McNair, nous voulons nous en servir comme modèle et travailler avec les provinces et territoires pour les amener à adopter des lois semblables dans leurs juridictions ou d'autres formes de réglementation comportant un volet sur la divulgation et le partage de renseignements à l'échelle du pays parce que nous en avons cruellement besoin.

Je crois que la solution passe par la collaboration. Si nous étions tentés de légiférer, nos conseillers juridiques m'ont assurée que ce serait contesté. Notre objectif principal est donc d'avoir un projet de loi conforme aux compétences constitutionnelles nous habilitant à légiférer dans des domaines précis, en l'occurrence les quatre qui ont été définis.

Je crois que c'est un point de départ important. Mais ce n'est pas la fin de l'histoire, à notre avis.

**Le sénateur McNair :** Merci.

**Le sénateur Kutcher :** Madame la présidente, félicitations pour votre élection. C'est une grande responsabilité.

Merci beaucoup d'être parmi nous, monsieur le ministre, et merci de vos aimables paroles au sujet du sénateur Yussuff. Je voudrais poursuivre la conversation sur les enjeux liés à la santé et attirer l'attention sur les fournisseurs de soins de santé

virtual health care providers are non-Canadians. There is a tremendous amount of health information stored in Canada by virtual health care providers, which may use our telecoms, but also by virtual health care providers outside the country. Some of that data is very important personal data, but some of it, particularly in psychotherapy situations, is narrative data.

How does the regulation of that kind of data fit in? It's a very difficult problem. I'm raising it not to criticize the bill but to try to understand how this bill may be a foundation for moving forward on that area.

**Mr. Anandasangaree:** Thank you, senator. If I know a retiring senator who can come up with a plan to address this, I would probably engage that person to do some more work.

You pose a very important question. We are seeing the evolution of virtual care. The interprovincial element is one aspect, and that's probably easier to address than the overseas element.

At the end of the day, health care needs to be in line with the Canada Health Act. With respect to the protection of information, we can regulate information that is within Canada. There are certainly some concerns around data sovereignty. Those are live conversations that are now taking place as AI data centres evolve as well as the imposition of the USA PATRIOT Act on certain types of data that are Canadian but stored in U.S. facilities. Those are live questions to which, I will confess, I don't have the answers. But they are part of the work that needs to be done post facto and part of the ongoing scrutiny that needs to take place in the context of cybersecurity because we know that those vulnerabilities continue to exist.

The challenge we face is that much of this data may not be in line with the Privacy Act. That is a starting limitation, whether it is a federal or provincial privacy act, because most provinces have some sort of privacy act in place.

When information is gathered and held overseas, accessing that information is not subject to Canadian privacy laws. We are already starting off with an uneven playing field.

One of the ways we can address it, apart from trying to regulate that here, is to have partnerships with different governments, depending on which country it is. As we enhance our trade relationships, we may be able to build collaboration with other countries on privacy protection.

virtuels, dont la réglementation ne m'apparaît pas claire. Certains de ces fournisseurs virtuels ne sont pas Canadiens. Une quantité considérable de données médicales est stockée au Canada par des fournisseurs virtuels qui peuvent utiliser nos réseaux de télécommunications, mais aussi par des fournisseurs virtuels installés à l'étranger. Certains de ces renseignements sont des données personnelles très importantes, et, notamment dans le domaine de la psychothérapie, il peut s'agir de données narratives.

Comment la réglementation aborde-t-elle ce type de données? C'est une question très difficile. Je la soulève non pas pour critiquer le projet de loi, mais pour essayer de comprendre en quoi il pourrait servir de socle permettant d'avancer à cet égard.

**M. Anandasangaree :** Merci, sénateur. Si je connaissais un sénateur à la retraite qui puisse proposer un plan pour régler cette question, je lui demanderais probablement de faire du travail supplémentaire.

Vous soulevez une question très importante. Nous sommes attentifs à l'évolution des soins virtuels. Le volet interprovincial en est un aspect, et il est probablement plus facile à gérer que le volet international.

Au final, les soins de santé doivent être conformes à la Loi canadienne sur la santé. Quant à la protection des renseignements, il est possible de réglementer l'accès à ceux qui se trouvent au Canada. La souveraineté des données est évidemment une préoccupation. On en discute actuellement, tandis que des centres de données d'IA s'étendent et que la USA PATRIOT Act s'applique à certains types de données canadiennes stockées dans des installations américaines. Ce sont des questions très actuelles, et j'avoue ne pas avoir de réponses. Mais elles font partie du travail à faire a posteriori et de l'examen permanent qu'exige la cybersécurité, puisqu'on sait bien que ces vulnérabilités persistent.

La difficulté tient au fait que beaucoup de ces données ne sont peut-être pas conformes à la Loi sur la protection des renseignements personnels. C'est déjà une limitation, qu'il s'agisse d'une loi fédérale ou provinciale, étant donné que la plupart des provinces ont une loi sur la protection des renseignements personnels.

Quand les données sont recueillies et conservées à l'étranger, l'accès à ces renseignements n'est pas assujetti aux lois canadiennes sur la protection des renseignements personnels. La situation n'est donc pas la même au départ.

Pour y remédier, on peut, outre les mesures de réglementation ici, essayer de créer des partenariats avec différents gouvernements, selon les pays en question. En même temps qu'on consolide nos relations commerciales, on pourrait instaurer des rapports de collaboration avec d'autres pays en matière de protection des renseignements personnels.

**Senator Ince:** Thank you, Madam Chair, and congratulations.

I have some beautiful insoles for those shoes for you.

**The Chair:** Wonderful. Fill them up.

**Senator Ince:** Thank you, minister and staff, for being here.

Minister, on October 30, 2025, Philip Stupak, Senior Director of Advocacy for ISC2 Inc., told the House Standing Committee on Public Safety and National Security that not all federally regulated critical infrastructure sectors, including water systems, are included in Schedule 1 of the proposed CCSPA. In addition, Canada's 2009 National Strategy for Critical Infrastructure identifies 10 critical infrastructure sectors, including water.

Why does Schedule 1 of the proposed CCSPA not include all 10 critical infrastructure sectors that are identified in the 2009 strategy?

**Mr. Anandasangaree:** We go back to being in the federal lane of regulation. We have authorities in a number of different sectors — finance, telecom, energy and transport being the primary ones — and the powers that would be bestowed through CCSPA are with respect to those four specific industries; it doesn't go beyond them. That said, many provinces and municipalities, for example, have critical infrastructure, so this is both an opportunity and a challenge for us. Once we have a framework in place that works federally, we need to be able to work with the provinces to maybe adopt similar mirror legislation or some other ways for compliance and reporting within areas of provincial jurisdiction.

We were very careful not to overstep. Often, legislation is subject to judicial scrutiny, and one of the dangers we have is that if it goes beyond the scope of a federal mandate, then it can be subject to court intervention, perhaps even disallowing elements of the bill or striking provisions altogether.

That's the primary reason we are sticking to the four areas that are outlined.

**Senator Ince:** Thank you.

Are there situations that could lead to other critical infrastructure sectors being added to Schedule 1?

**Mr. Anandasangaree:** Right now, senator, we don't contemplate anything specific outside of the four sectors. However, the Governor-in-Council has the authority to add other federally regulated vital services and systems to Schedule 1,

**Le sénateur Ince :** Merci, madame la présidente. Félicitations à vous.

J'ai de belles semelles pour vos nouvelles chaussures.

**La présidente :** Excellent. Je les prends.

**Le sénateur Ince :** Merci au ministre et à son équipe d'être parmi nous.

Monsieur le ministre, le 30 octobre 2025, Philip Stupak, directeur principal de la défense des intérêts pour ISC2 Inc., a déclaré au Comité permanent de la sécurité publique et nationale de la Chambre des communes que les secteurs d'infrastructures essentielles sous réglementation fédérale, dont les systèmes d'approvisionnement en eau, ne sont pas tous inscrits à l'annexe 1 de la LPCSE. Par ailleurs, la Stratégie nationale de 2009 sur les infrastructures essentielles du Canada circonscrit 10 secteurs d'infrastructures essentielles, dont celui de l'eau.

Pourquoi l'annexe 1 de la LPCSE ne comprend-elle pas les 10 secteurs circonscrits dans la stratégie de 2009?

**M. Anandasangaree :** Nous restons dans le cadre de la compétence fédérale. Nous sommes habilités à l'égard de plusieurs secteurs distincts — les finances, les télécommunications, l'énergie et les transports étant les principaux —, et les pouvoirs conférés par la LPCSE s'appliquent à ces quatre secteurs, mais pas au-delà. Cela dit, beaucoup de provinces et de municipalités, par exemple, possèdent des infrastructures essentielles, et c'est pour nous à la fois une opportunité et une difficulté. Quand nous aurons instauré un cadre efficace à l'échelle fédérale, nous pourrons collaborer avec les provinces pour les inciter à adopter des lois équivalentes ou trouver d'autres mécanismes permettant de garantir conformité et communications dans les secteurs relevant de la compétence des provinces.

Nous avons pris soin de ne pas outrepasser nos compétences. Les lois sont souvent assujetties à des contrôles judiciaires, et le risque est, entre autres, que, si la loi excède le champ d'application du mandat fédéral, une intervention judiciaire puisse invalider certains éléments du projet de loi ou annuler ses dispositions.

C'est la principale raison pour laquelle nous nous en tenons aux quatre secteurs définis.

**Le sénateur Ince :** Merci.

Certaines situations pourraient-elles conduire à l'ajout d'autres secteurs d'infrastructures essentielles à l'annexe 1?

**M. Anandasangaree :** Pour l'instant, sénateur, rien de précis n'est envisagé en dehors de ces quatre secteurs. Cependant, le gouverneur en conseil a le pouvoir d'y ajouter d'autres services et systèmes essentiels sous réglementation fédérale, les

making them subject to the CCSPA. Those include those portions of water services that you talked about and that are now federally regulated.

So, while these are the four that we were sticking to when we contemplated the legislation, there are scenarios in which we could add others as needs and other opportunities arise for us.

**Senator Ince:** Thank you.

**Senator Yussuff:** Thank you, chair, and congratulations.

Minister, I have a few questions in regard to the gap based upon what we constantly hear in the public domain. Many of the major breaches that have taken place in terms of cybersecurity have been at the provincial level, over which you have no oversight or control.

Given the expectations of Canadians and the importance of this bill in trying to rectify the federal jurisdiction, how can we best collaborate with the provinces? They don't have any of the infrastructure we do at the federal level that could aid and support them. Should there be an interprovincial approach to say, "For some of these things, we may want to defer recognizing what the Constitution says"? We're going to continue to hear the same problems unless we find a way to have some symmetry in which we have broader oversight.

If you ask a Canadian in Ontario versus one in B.C. or Nova Scotia, they will believe that somebody is supposed to protect them. Of course, at the provincial level, we know they don't have the same degree of oversight that is available at the federal level.

How can we accomplish that? I think one of the biggest gaps after this bill is passed will be that we will continue to be frustrated with hearing about these breaches while not knowing why they are happening in the first place.

**Mr. Anandasangaree:** Senator, that's an astute observation. I would say it's a source of frustration.

Our Confederation is complex. On most days, I think, most of us don't fully comprehend the depth of our mandates, whether it is federal or provincial jurisdiction, and it is much harder to explain to Canadians the challenges the federal government would face, and vice versa, because there are also times the provinces are frustrated with the federal government.

I believe that this is an imperfect bill, but it captures what we want to do vis-à-vis federal authorities and jurisdiction. With its passage, one of the things we could do is also include this in our FPT. Between Mr. Fraser, the Minister of Justice, and I, the Minister of Public Safety, we have annual meetings with the provinces and territories. It's an area we can certainly bring to

soumettant de ce fait à la LPCSE. Cela inclut les parties des services d'approvisionnement en eau dont vous avez parlé et qui sont désormais sous réglementation fédérale.

Donc, même si nous nous en sommes tenus à ces quatre secteurs, certaines situations nous permettraient d'en ajouter au fur et à mesure des besoins ou des occasions.

**Le sénateur Ince :** Merci.

**Le sénateur Yussuff :** Merci, madame la présidente, et félicitations à vous.

Monsieur le ministre, j'ai quelques questions au sujet de ce décalage, compte tenu de ce qu'on entend constamment dans l'espace public. Beaucoup d'atteintes majeures à la cybersécurité se produisent à l'échelle provinciale, là où vous n'avez aucun pouvoir de surveillance ou de contrôle.

Compte tenu des attentes des Canadiens et de l'importance du projet de loi pour corriger la législation fédérale, comment mieux collaborer avec les provinces? Elles n'ont pas d'infrastructure semblable à ce que nous avons à l'échelle fédérale pour les aider et les soutenir. Faudrait-il envisager une perspective interprovinciale en partant du principe qu'on pourrait « ignorer ce que dit la Constitution dans certains cas »? On va continuer d'entendre parler des mêmes problèmes à moins d'instaurer une certaine symétrie qui permettrait une surveillance élargie.

Si vous posez la question à des Canadiens de l'Ontario, de la Colombie-Britannique et de la Nouvelle-Écosse, vous constaterez qu'ils estiment tous que quelqu'un est censé les protéger. Or, on sait que, à l'échelle provinciale, le degré de surveillance n'est pas aussi élevé qu'à l'échelle fédérale.

Comment faire? Je crois que, après l'adoption de ce projet de loi, nous allons continuer d'être frustrés d'entendre parler de ces atteintes à la sécurité alors que nous ne comprenons toujours pas pourquoi elles se produisent.

**M. Anandasangaree :** Vous êtes perspicace, sénateur. C'est effectivement une source de frustration.

Notre Confédération est un système complexe. Je crois que, la plupart du temps, nous sommes très nombreux à ne pas comprendre pleinement l'étendue de nos mandats, qu'ils soient fédéraux ou provinciaux, et il est beaucoup plus difficile d'expliquer aux Canadiens les difficultés auxquelles le gouvernement fédéral est confronté, et réciproquement, puisqu'il arrive aussi que les provinces soient frustrées par le gouvernement fédéral.

Ce projet de loi est certainement imparfait, mais il traduit ce que nous souhaitons faire compte tenu de la compétence et des pouvoirs du gouvernement fédéral. Quand il sera adopté, nous pourrons l'intégrer à notre forum FPT. M. Fraser, le ministre de la Justice, et moi-même, ministre de la Sécurité publique, avons des rencontres annuelles avec les provinces et territoires. C'est

the table and ask for collaboration in terms of how this could be mirrored within provincial jurisdictions. There may be slight variations in terms of the types of privacy acts that exist within each province, but it's worth the conversation.

You're right: For the average person, whether it's a provincial water system, a federal water system or a credit union as opposed to a chartered bank, the distinction is moot. There is an impetus for us to ensure, for the sake of protection, that we expand this. It is a federal bill and always will be, but we need to have compliance by way of discussions and negotiations.

**Senator Yussuff:** Criminals don't really care about who will be the benefactor once they are able to succeed in their efforts.

I would plead that the gap that exists here be recognized and not that federal-provincial collaboration is fundamental for Canadian security. It's terrible to tell somebody that their data is now in some criminal's hands and we can't do anything about it because, at the provincial level, where they have jurisdiction, they didn't have the elements the federal government could have offered to help them to better secure their data in the first place.

It would be extremely helpful.

If Canadians are watching this, they might be left scratching their heads when recognizing that the federal government cannot protect them at the provincial level, no matter what the situation might be.

**Mr. Anandasangaree:** In fact, if I may, with your indulgence, Madam Chair, the fact is that if something happens at the provincial level, chances are it will go to other provinces. It's not just one province that would be impacted; it would be multiple provinces.

I acknowledge the need for federal leadership on this for collaborations to take place because, ultimately, it is about protecting Canadians, as you said.

**Senator Dasko:** Congratulations, Madam Chair. It is great to see you in that spot.

Thank you, witnesses and minister. I want to dig a little deeper, especially regarding the state actors or perpetrators of cybercrimes. I want to understand a few things about them. Who are they? What is their motivation? What are they looking for? Are they disruptors, or are they seeking certain kinds of information? Which sectors are they focusing on?

What they are interested in and what sectors they are focusing on would help us understand what their interests are and what they're trying to do. I find it a little bit mysterious — but maybe it's not mysterious and you have all the answers.

un sujet que nous pourrons certainement aborder et au titre duquel nous pourrons demander leur collaboration pour envisager la possibilité de lois provinciales semblables. Il pourrait y avoir de légères variations dans les lois provinciales sur la protection des renseignements personnels, mais cela mérite discussion.

Vous avez raison : pour le Canadien moyen, que le réseau hydrique soit de compétence provinciale ou fédérale ou qu'on parle d'une coopérative de crédit ou d'une banque à charte importe peu. Nous avons tout intérêt, par souci de protection, à élargir le champ d'application. C'est un projet de loi fédéral et il le restera, mais nous devons assurer la conformité au moyen de discussions et de négociations.

**Le sénateur Yussuff :** Les criminels se fichent pas mal de savoir qui profitera une fois leurs objectifs atteints.

Je préférerais que cette lacune soit reconnue et non que la collaboration fédérale-provinciale soit considérée comme indispensable à la sécurité canadienne. Il est terrible de dire à quelqu'un que ses données sont entre les mains d'un criminel et qu'on ne peut rien faire parce que les administrations provinciales compétentes ne disposent pas des moyens que le gouvernement fédéral aurait à offrir pour mieux sécuriser ses données dès le départ.

Ce serait extrêmement utile.

Les Canadiens qui voient cela risquent de s'interroger sur le fait que le gouvernement fédéral ne puisse pas les protéger à l'échelle provinciale quelle que soit la situation.

**M. Anandasangaree :** En fait, si je peux me permettre, madame la présidente, le fait est que, s'il arrive quelque chose à l'échelle provinciale, il y a de fortes chances que cela se propage dans d'autres provinces. Il n'y aura pas qu'une seule province touchée, mais plusieurs.

Il faudrait effectivement que le gouvernement fédéral assume le leadership de ce genre de collaboration, puisque, au final, il s'agit de protéger les Canadiens, comme vous l'avez dit.

**La sénatrice Dasko :** Félicitations, madame la présidente. Quel plaisir de vous voir à ce poste.

Merci aux témoins et au ministre. Je voudrais aller un peu plus loin, notamment au sujet des auteurs étatiques ou autres de cybercrimes. J'aimerais savoir qui ils sont et connaître leurs motivations et leurs objectifs. Est-ce qu'ils cherchent à perturber nos systèmes ou à obtenir certains types de renseignements? À quels secteurs s'intéressent-ils?

Comprendre ce qui les intéresse et savoir quels secteurs ils visent nous aiderait à comprendre leurs objectifs. Je trouve cela un peu mystérieux — mais peut-être que ce ne l'est pas et que vous avez toutes les réponses.

Technologically speaking, do you have the ability to collect information on exactly who they are — the who, what, when, where and why?

**Mr. Anandasangaree:** You always ask questions for which I think there are great answers but ones probably best given in a setting that is secure.

But let me try.

**Senator Dasko:** Let's just turn off —

**Mr. Anandasangaree:** I will try to answer this, but I will also invite this committee to receive a secure briefing on this because it is quite important. I will talk about how there are a number of actors. CSIS's annual report was tabled on Friday, and there are references to some actors there.

There are a number of motivations. One is to pose some instability to Canada —

**Senator Dasko:** Disruption.

**Mr. Anandasangaree:** — disruption to Canada, to Canadian institutions and to Canadian political systems, and that's been a motivation for a number of nefarious actors.

In part, it is also to do with geopolitics and Canada's position on a range of issues, including what are very strong human rights perspectives on a range of issues; Canada's general tenor on human rights violations is consistent across a range of countries.

To be sure, the Foreign Influence Transparency Registry is an additional irritant to some actors. There is a range of motivations that may lead other state actors to be part of it.

Let's also not underestimate private interests and those who are essentially, with ransomware, for example — doing it for money. They are doing it to raise money to add to the criminal networks that already exist, albeit in a much more sophisticated way than we may have seen in the past.

**Senator Dasko:** So, of course, the private actors are looking for information, material gain, commercial interests and so on. With respect to state actors, is it mainly to cause disruption or are they looking for information too?

**Mr. Anandasangaree:** I will go back to my initial point: This warrants, I believe, a closed conversation.

Sur le plan technologique, avez-vous la capacité de recueillir des informations précises sur leur identité — sur qui, quoi, quand, où et pourquoi?

**M. Anandasangaree :** Vous posez toujours des questions auxquelles je pense qu'il existe d'excellentes réponses, mais qu'il vaut sans doute mieux aborder dans un cadre sécurisé.

Je vais néanmoins essayer d'y répondre.

**La sénatrice Dasko :** Fermons simplement...

**M. Anandasangaree :** Je vais essayer d'y répondre, mais j'inviterai également ce comité à recevoir un mémoire sécurisé à ce sujet, car c'est une question assez importante. Je vais vous expliquer qu'il existe plusieurs acteurs en jeu. Le rapport annuel du Service canadien du renseignement de sécurité, le SCRS, a été déposé vendredi, et on y discute de certains de ces acteurs.

Il existe plusieurs motivations. L'une d'elles est de semer une certaine instabilité au Canada...

**La sénatrice Dasko :** Causer des perturbations.

**M. Anandasangaree :** ... des perturbations au Canada, au sein des institutions canadiennes et des systèmes politiques canadiens, ce qui a motivé un certain nombre d'acteurs malveillants.

Cela tient en partie à la géopolitique et à la position du Canada sur toute une série de questions, notamment ses positions très fermes en matière de droits de la personne; la ligne générale adoptée par le Canada face aux violations des droits de la personne est cohérente dans de nombreux pays.

Il est certain que le Registre canadien pour la transparence en matière d'influence étrangère constitue une source de contrariété supplémentaire pour certains acteurs. Diverses motivations peuvent toutefois expliquer pourquoi d'autres acteurs étatiques y sont visés.

Il ne faut pas non plus sous-estimer les intérêts privés et ceux qui, par le biais des rançongiciels par exemple, agissent essentiellement pour l'argent. Ils le font pour récolter des fonds destinés à alimenter les réseaux criminels déjà existants, bien que d'une manière bien plus sophistiquée que ce à quoi nous avons pu être habitués par le passé.

**La sénatrice Dasko :** Il va donc de soi que les acteurs privés recherchent des informations, des gains matériels, des intérêts commerciaux, et ainsi de suite. Quant aux acteurs étatiques, veulent-ils principalement semer la perturbation ou recherchent-ils eux aussi des informations?

**M. Anandasangaree :** Je reviens à mon argument initial : cela justifie, à mon avis, une discussion à huis clos.

The speculation that I will offer is that, yes, it is about disruption. It is about ensuring that Canadian systems that are well developed, grounded by the rule of law and have safeguards in place that ensure privacy protection and human rights protection are challenged in a way that disrupts our way of life. They certainly won't be successful in doing so, but these are attempts to destabilize.

We are a strong democracy with great institutions, such as the RCMP, CSIS, CBSA and CSE, that defend our borders. They are continuously doing the work to protect Canadians.

**Senator Dasko:** Thank you.

**Senator Hay:** Minister, just a few minutes ago, you said this is an imperfect bill, so I have a comment: If we wait for perfect, we will always be waiting. I thought I would throw that out there.

My question is this: How does this bill address or reduce the risk of AI-generated threats, like "deepfake" disinformation that's been talked about, AI-powered phishing and autonomous cyberattacks? As a follow-up, will it be adaptive enough for the Wild West that is the AI world of today?

**Mr. Anandasangaree:** That's a great question. The bill looks at the architecture that is under attack. It doesn't necessarily look at individual breaches but rather more architectural weaknesses. For example, the use of AI is part of the regulation, although the AI itself is not being regulated here. It is the actual outcomes and impacts the architectural vulnerabilities have in the imposition of ransomware or other attacks that are addressed in this bill.

To the evergreen piece, as technologies evolve, as different AI is unleashed to the full extent, there is capability within the act to respond to those evolutions. However, one cannot predict how far we're going to go in the next two, three or five years. Based on what we know now and what is readily and publicly available, we are quite confident that the bill and the regulatory authorities will enable us to keep up. However, the five-year review is critical for this.

We have a number of other bills. Bill C-22 is going to come before the House. We are all working toward bringing things up

Je pense, pour ma part, qu'il s'agit bien d'une tentative de perturbation. L'objectif consiste à remettre en cause les systèmes canadiens, qui sont bien établis, fondés sur la primauté du droit et dotés de mécanismes de protection garantissant le respect de la vie privée et des droits de la personne, d'une manière qui perturbe notre mode de vie. Ils n'y parviendront certainement pas, mais il s'agit là de tentatives visant à déstabiliser le système.

Nous sommes une démocratie solide dotée d'institutions de premier plan, comme la Gendarmerie royale du Canada, la GRC, le SCRS, l'Agence des services frontaliers du Canada, l'ASFC et le Centre de la sécurité des télécommunications, le CST, qui défendent nos frontières. Elles œuvrent sans relâche pour assurer la protection des Canadiens.

**La sénatrice Dasko :** Merci.

**La sénatrice Hay :** Monsieur le ministre, il y a quelques minutes à peine, vous avez dit qu'il s'agissait d'un projet de loi imparfait; j'ai donc une remarque à faire : si nous attendons la perfection, nous attendrons longtemps. Je tenais simplement à le signaler.

Ma question est la suivante : comment ce projet de loi aborde-t-il ou réduit-il le risque lié aux menaces générées par l'IA, telles que la désinformation par hypertrucage, dont on a beaucoup parlé, l'hameçonnage alimenté par l'IA et les cyberattaques autonomes? Par ailleurs, aura-t-il la souplesse nécessaire pour s'adapter à ce Far West qu'est le monde de l'IA aujourd'hui?

**M. Anandasangaree :** C'est une excellente question. Le projet de loi s'intéresse à l'architecture qui fait l'objet d'attaques. Il ne porte pas nécessairement sur les infractions individuelles, mais plutôt sur les failles architecturales. Par exemple, l'utilisation de l'IA fait partie du champ d'application de la réglementation, bien que l'IA elle-même ne soit pas réglementée ici. Ce sont les répercussions et les résultats concrets des vulnérabilités architecturales sur la mise en œuvre de rançongiciels ou d'autres attaques qui sont abordés dans ce projet de loi.

À savoir, si le texte présente un caractère intemporel, à mesure que les technologies évoluent et que différentes formes d'IA sont pleinement mises à contribution, la loi prévoit les moyens de s'adapter à cette évolution. Il est toutefois impossible de prédire jusqu'où cela ira dans les deux, trois ou cinq prochaines années. Sur la base de ce que nous savons aujourd'hui et des informations facilement accessibles au public, nous sommes tout à fait convaincus que le projet de loi et les organismes de réglementation nous permettront de rester à la page. Toutefois, l'examen quinquennal est essentiel à cet égard.

Nous avons plusieurs autres projets de loi. Le projet de loi C-22 va être présenté à la Chambre. Nous nous efforçons tous

to current standards and even looking ahead a little bit, but we have to be vigilant in terms of what is coming down the pipeline.

**Senator Hay:** Just a quick follow-up — you talked about AI not being regulated. Do you see this bill working in line with the unfolding AI strategy and potential legislation that might come down the pipe?

**Mr. Anandasangaree:** Certainly, the regulatory powers will have some impact on AI, bots and other tools. There will certainly be other legislation that looks at AI. I know Minister Solomon was here during Question Period a couple of weeks ago, and he will be well positioned to speak about the vision in terms of where, as a country, we are embracing but also safeguarding AI. It's a strategy that he is working on. The Prime Minister has talked about AI for a while, and I believe we will see more from Minister Solomon over the coming months.

**Senator Hay:** And this bill will plug into that?

**Mr. Anandasangaree:** It will, yes.

**Senator Hay:** Thank you.

[*Translation*]

**Senator Youance:** Welcome and congratulations. Thank you for being here, minister.

My question will focus on one specific example, but I would have liked to have given two or three others. Since the bill gives the government a new tool to require a designated operator to take measures to protect its cyber system "as needed", could you give us an example of the sort of measures that the government could take in the event of a cyberattack, if Bill C-8 were already in place? You mentioned the cyberattack on WestJet earlier.

[*English*]

**Mr. Anandasangaree:** There are two things here. The first is disclosure in a timely manner. Right now, for example, if a company like an airline is attacked, information is leaked or there is some kind of ransomware demand, the ability to share that information with other similarly situated companies in the industry will enable greater vigilance and also proactive steps by others. Our ability to look at the technology that was used for that attack will also be helpful.

d'assurer la conformité avec les normes actuelles et même d'anticiper un peu l'avenir, mais nous devons rester vigilants quant à ce qui nous attend.

**La sénatrice Hay :** Juste une petite question complémentaire : vous avez évoqué le fait que l'IA n'est pas réglementée. Pensez-vous que ce projet de loi s'inscrira dans le cadre de la stratégie en cours sur l'IA et des éventuelles mesures législatives à venir?

**M. Anandasangaree :** Il ne fait aucun doute que les pouvoirs réglementaires auront une incidence sur l'IA, les robots et d'autres outils. D'autres mesures législatives portant sur l'IA verront certainement le jour. Je sais que le ministre Solomon était présent lors de la période des questions il y a quelques semaines, et il sera bien placé pour exposer la vision de notre pays quant à la manière dont nous adoptons l'IA tout en la protégeant par des mesures de sécurité. C'est une stratégie à laquelle il travaille. Le premier ministre parle de l'IA depuis un certain temps déjà, et je pense que le ministre Solomon nous en dira davantage au cours des prochains mois.

**La sénatrice Hay :** Et ce projet de loi s'inscrira-t-il dans ce cadre?

**M. Anandasangaree :** Oui.

**La sénatrice Hay :** Merci.

[*Français*]

**La sénatrice Youance :** Bienvenue et félicitations. Merci d'être ici, monsieur le ministre.

Ma question portera sur un exemple concret, mais j'aurais aimé en avoir deux ou trois autres. Comme le projet de loi donne un nouvel outil au gouvernement afin de contraindre « au besoin » un exploitant désigné à prendre des mesures pour protéger son cybersystème, pouvez-vous nous donner un exemple — vous avez cité tout à l'heure la cyberattaque sur WestJet — du genre de mesures que le gouvernement pourrait prendre dans le cas d'une cyberattaque, si le projet de loi C-8 était déjà en place?

[*Traduction*]

**M. Anandasangaree :** Il y a deux points à retenir ici. Le premier concerne la communication d'informations en temps opportun. À l'heure actuelle, par exemple, si une entreprise comme une compagnie aérienne est victime d'une cyberattaque, que des informations sont divulguées ou qu'une demande de rançongiciel est formulée, la possibilité de partager ces informations avec d'autres entreprises du secteur confrontées à des situations similaires renforcera la vigilance et incitera ces autres acteurs à prendre des mesures proactives. Notre capacité à analyser la technologie utilisée pour cette attaque sera également utile.

It is very much on a proactive basis to ensure that if the attack is on one narrow player, it doesn't have broader implications on the entire industry. It is one way that the bill is designed. That's one concrete example.

The other way is learning from this. There have been a number of examples recently where ransomware was used in one industry and another in a provincial setting. Again, there is greater learning for us as to what kind of an impact it will have on the broader sectors.

It is about CSE, for example, continuously playing its part in defence within the cyberworld, but also for governments to be able to share within the federal system to see how we can best prevent it from happening again.

**The Chair:** We're approaching five o'clock. This brings us to the end of our time with the minister.

Thank you, minister, for taking the time to meet with us today. Thank you also to the front row, the back row and the two side rows of the team that supports you. All this work needs every one of you. We appreciate you being here.

Department officials have graciously agreed to stay behind, so we will carry on with our questions.

This past hour, we've had the opportunity and the pleasure of hearing from the Minister of Public Safety as we open our study of Bill C-8.

We will now carry on with our second panel and continue with our questions to Public Safety Canada and Innovation, Science and Economic Development Canada.

**Senator Al Zaibak:** Thank you all for being here today.

Bill C-8 introduces significant new authorities to issue cybersecurity directions. We received a briefing yesterday that it doesn't add any significant authorities. I'm in need of your clarification in that respect.

What specific thresholds or risk criteria will trigger these interventions? How will consistency be ensured across all sectors?

**Colin MacSween, Director General, National and Cyber Security Branch, Public Safety Canada:** Thank you, senator, for the question. Just so I understand correctly, I think the question was about the new order-making power in Part 2 of the

Il s'agit avant tout d'une approche proactive visant à garantir que, si une attaque vise un seul acteur, elle n'ait pas de répercussions plus larges sur l'ensemble du secteur. C'est l'un des objectifs pour lesquels le projet de loi a été conçu. En voilà un exemple concret.

L'autre approche consiste à tirer des enseignements de ces situations. On a récemment observé plusieurs cas où des rançongiciels ont été utilisés dans un secteur d'activité donné, puis dans un autre, au niveau provincial. Là encore, cela nous permet de mieux comprendre quel type d'incidence cela aura sur l'ensemble des secteurs concernés.

Il s'agit, par exemple, pour le CST de continuer à jouer son rôle de défenseur dans le cyberespace, mais aussi pour que les gouvernements puissent échanger au sein du système fédéral afin de déterminer comment éviter au mieux que cela ne se reproduise.

**La présidente :** Il sera bientôt 17 heures, ce qui marque la fin de notre entretien avec le ministre.

Merci, monsieur le ministre, d'avoir pris le temps de nous rencontrer aujourd'hui. Merci également à l'équipe qui vous soutient, qu'elle soit au premier rang, au dernier rang ou sur les deux rangées latérales. Tout ce travail ne peut se faire sans chacun d'entre vous. Nous vous remercions de votre présence ici.

Puisque les fonctionnaires du ministère ont aimablement accepté de rester, nous allons poursuivre nos questions.

Au cours de la dernière heure, nous avons eu l'occasion et le plaisir d'entendre le ministre de la Sécurité publique et de la Protection civile à l'occasion de l'ouverture de notre examen du projet de loi C-8.

Nous allons maintenant accueillir notre deuxième groupe de témoins et poursuivre nos questions adressées à Sécurité publique Canada et à Innovation, Sciences et Développement économique Canada.

**Le sénateur Al Zaibak :** Merci à tous d'être ici aujourd'hui.

Le projet de loi C-8 prévoit de nouveaux pouvoirs importants en matière de prise de directives de cybersécurité. Nous avons reçu hier un mémoire indiquant qu'aucun nouveau pouvoir significatif n'est ajouté. J'aimerais que vous m'éclairiez à ce sujet.

Quels seuils ou critères de risque précis déclencheront ces interventions? Comment garantira-t-on la cohérence entre tous les secteurs?

**Colin MacSween, directeur général, Direction de la sécurité nationale et de la cybersécurité, Sécurité publique Canada :** Merci, sénateur, pour cette question. Si j'ai bien compris, je crois que la question portait sur le nouveau pouvoir

critical cyber systems protection act, known as cyber security directions.

The power itself is designed to give the Governor-in-Council the ability to order a designated operator to do anything necessary to protect their vital service or system. It was designed as a bit of a measure of last resort. I say that because there are a lot of things in front of that direction-making power.

The way Part 2 of the act works is it sets up a regulatory framework for the federally regulated critical infrastructure sectors that the minister mentioned. It will require them to do four things: have a cybersecurity program, identify and mitigate supply chain risks, perform mandatory incident reporting to the Canadian Centre for Cyber Security and, if necessary, implement a cyber security direction.

The reason I mention that is the cybersecurity program is really just an articulation of what the designated operator is doing to protect its vital service or system.

Within that, that's where we're able — with the help of the technical expertise of the Canadian Centre for Cyber Security — to understand if that particular critical infrastructure, or CI, owner is doing a sufficient amount of work to protect its vital service or system.

The order-making power is there in the event that the government has to order a designated operator to do something. However, there are certain steps along the way. For example, if a designated operator is found to be in non-compliance with the requirements of the legislation, they can enter into a compliance agreement with the regulator to address bringing them back into compliance so we don't have to use any of those powers in the back end. They're really just there as sort of an emergency power to allow the government to issue the direction, if it's necessary, to protect that vital service or system for Canadians.

**Senator Al Zaibak:** From your perspective, how does the bill, as currently articulated, strike the right balance between security imperatives, citizens' and businesses' privacy and maintaining a competitive digital economy for all sectors?

**Mr. MacSween:** Thank you very much for the question.

In terms of the privacy and order-making powers, what the House of Commons committee did was reaffirm the application of the Privacy Act in the legislation to ensure that privacy rights are applied. Generally speaking, there are quite a few amendments around establishing guardrails in the legislation as well. The order-making powers are a good example in that case.

de prise de décrets prévu à la partie 2, Loi sur la protection des cybersystèmes essentiels, connu sous le nom de « directives de cybersécurité ».

Ce pouvoir vise à permettre au gouverneur en conseil d'ordonner à un exploitant désigné de prendre toutes les mesures nécessaires pour protéger son service ou son système essentiel. Il a été conçu comme une mesure de dernier recours. Je dis cela, car de nombreuses autres options précèdent ce pouvoir de prise de décrets.

La partie 2 de la loi établit un cadre réglementaire pour les secteurs d'infrastructures essentielles relevant de la compétence fédérale dont le ministre a parlé. Elle leur impose quatre obligations : mettre en place un programme de cybersécurité, identifier et atténuer les risques liés à la chaîne d'approvisionnement, signaler obligatoirement les incidents au Centre canadien pour la cybersécurité et, si nécessaire, mettre en œuvre une directive en matière de cybersécurité.

Je le précise, car le programme de cybersécurité est en réalité une formalisation de ce que l'exploitant désigné met en œuvre pour protéger son service ou système essentiel.

C'est dans ce cadre que nous sommes en mesure — grâce à l'expertise technique du Centre canadien pour la cybersécurité — de déterminer si le propriétaire de cette infrastructure essentielle met en œuvre suffisamment de mesures pour protéger son service ou système vital.

Le pouvoir de prise de décrets s'exerce lorsque le gouvernement doit ordonner à un exploitant désigné de prendre certaines mesures. Cependant, cette procédure comporte plusieurs étapes. Par exemple, si un exploitant désigné ne respecte pas les exigences législatives, il peut conclure une entente de conformité avec l'organisme de réglementation afin de se conformer sans avoir recours à ces pouvoirs en dernier ressort. Ces pouvoirs ne sont donc qu'un mécanisme d'urgence permettant au gouvernement d'émettre des décrets, si nécessaire, pour protéger ce service ou système essentiel pour les Canadiens.

**Le sénateur Al Zaibak :** Selon vous, dans quelle mesure le projet de loi, tel qu'il est actuellement formulé, parvient-il à trouver le juste équilibre entre les impératifs de sécurité, la protection de la vie privée des citoyens et des entreprises, et le maintien d'une économie numérique concurrentielle pour tous les secteurs?

**M. MacSween :** Merci beaucoup pour votre question.

Concernant la protection de la vie privée et les pouvoirs de prise de décrets, le comité de la Chambre des communes a réaffirmé l'application de la Loi sur la protection des renseignements personnels dans le projet de loi pour assurer le respect des droits à la vie privée. De manière générale, plusieurs amendements visent aussi à établir des garde-fous dans la

There's a non-exhaustive list of criteria that the Governor-in-Council would have to consider if they were to issue a direction.

An example of that could be considering the financial impact on a designated operator or the implications for the vital service or system if they order someone to do something in order to do that.

On the transparency side, as the minister had mentioned, again, if an order were issued, there would be an automatic notification to NSIRA and NSICOP, so they are aware that an order-making power was used, and should they feel it necessary, they would have the authority under their own act to review that.

Those are a few examples of what's changed in the act that's tried to balance the authorities versus the privacy concerns. Is there anything you wanted to add?

**The Chair:** If we can move along there, if you don't mind and have our next question.

**Senator Batters:** Thank you. First, I want to follow up on a couple of things. I was very glad to hear the minister state that the Minister of Industry will come to this committee. That was going to be my first question: Where's the minister? She came to the House of Commons to testify on Bill C-8, so I think both ministers should appear at the Senate committee to afford us the proper respect and enable the committee to ask questions. I look forward to that.

Following up, the minister indicated the regulations were not ready to go yet, but he stated that it would be ". . . quite fast . . ." after the bill passed. Isn't that regulatory process more likely to be a two-year process? After the bill is passed and you go through the necessary consultations and that sort of thing, isn't it likely to be about two years after the bill is passed that the regulations will come into effect?

**Mr. MacSween:** Thank you, senator, for the question.

The regulatory process is incredibly well defined. There are multiple steps that must be taken, which can expand timelines. The objective, though, obviously, as the minister stated, is to do these as quickly as we possibly can within the confines of that process. The regulatory process is established by the Treasury

législation. Les pouvoirs de prise de décrets en sont un exemple. Il existe une liste non exhaustive de critères dont le gouverneur en conseil devra tenir compte s'il doit émettre une directive.

On pourrait par exemple envisager les répercussions financières pour un exploitant désigné ou les conséquences pour le service ou système essentiel si un décret lui ordonne de prendre certaines mesures.

Sur le plan de la transparence, comme l'a dit le ministre, je le répète, si un décret était pris, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, l'OSSNR, et le Comité des parlementaires sur la sécurité nationale et le renseignement, le CPSNR, en seraient automatiquement informés, pour qu'ils sachent qu'un pouvoir de prise de décrets a été exercé; et s'ils le jugeaient nécessaire, ils auraient le pouvoir, en vertu de leur propre loi, de réexaminer cette décision.

Voici quelques exemples des modifications apportées à la loi visant à équilibrer les pouvoirs octroyés et les préoccupations en matière de protection des renseignements personnels. Avez-vous quelque chose à ajouter?

**La présidente :** Si vous le permettez, passons à la question suivante.

**La sénatrice Batters :** Merci. Tout d'abord, je voudrais revenir sur quelques points. J'ai été très heureuse d'entendre le ministre indiquer que la ministre de l'Industrie se présenterait devant ce comité. C'était justement ma première question : où est la ministre? Elle s'est rendue à la Chambre des communes pour témoigner au sujet du projet de loi C-8; je pense donc que les deux ministres devraient comparaître devant le comité sénatorial permanent afin de nous témoigner le respect qui nous est dû et de permettre à ce comité de poser des questions. J'attends leur présence avec impatience.

En réponse, le ministre a indiqué que les règlements n'étaient pas encore prêts, mais il a précisé qu'ils allaient « […] progresser très rapidement […] » une fois le projet de loi adopté. Ce processus réglementaire ne risque-t-il pas plutôt de s'étaler sur deux ans? Une fois le projet de loi adopté et quand les consultations nécessaires auront été menées et tout ce qui s'ensuit, n'est-il pas vraisemblablement le cas que le règlement n'entre en vigueur que deux ans environ après l'adoption du projet de loi?

**M. MacSween :** Merci, madame la sénatrice, pour cette question.

Le processus réglementaire est extrêmement bien défini. Il comporte plusieurs étapes à suivre, ce qui peut allonger les délais. L'objectif, cependant, comme l'a indiqué le ministre, est évidemment de mener ces démarches aussi rapidement que possible, dans le respect de ce processus. Le processus

Board. There are obligations that we have to undertake, including, as you mentioned, public consultations.

**Senator Batters:** Since I have limited time, is it likely to be about a two-year process — yes or no?

**Mr. MacSween:** It could be shorter.

**Senator Batters:** How much shorter?

**Mr. MacSween:** You could easily do it in 12 to 18 months.

**Senator Batters:** All right. Also, the minister said he met with the Privacy Commissioner in October, but that was already months after Bill C-8 was introduced. Why weren't the Privacy Commissioner and the Intelligence Commissioner consulted before Bill C-8 was introduced? Both of them had raised serious concerns about privacy, state powers, oversight and the lack of consultation they received from the government during the study of Bill C-26.

**Kelly-Anne Gibson, Director, National Cyber Security Policy, National and Cyber Security Branch, Public Safety Canada:** Bill C-26 was introduced, I believe, in June 2022. We had working-level consultations with the Privacy Commissioner in June 2019, so that would have technically been before.

**Senator Batters:** That was long before the bill. I'm talking about consultations about the actual bill and the problems they saw with Bill C-26 so it could be fixed with Bill C-8. Why weren't there those kinds of consultations when both those officers raised those concerns throughout the Bill C-26 process?

**Ms. Gibson:** We would have had the bill drafted when we talked with them in 2019. It was drafted, and then it was introduced after that, obviously.

**Senator Batters:** But I'm asking why they weren't consulted after Bill C-26 died on the Order Paper and you were preparing Bill C-8. They had raised serious concerns about going through the process in committees, both in the House of Commons and the Senate. Why weren't they consulted by the government at that point to try to improve the bill before it was reintroduced as Bill C-8?

réglementaire est établi par le Conseil du Trésor. Nous avons certaines obligations à remplir, notamment, comme vous l'avez dit, les consultations publiques.

**La sénatrice Batters :** Comme je dispose de peu de temps, est-ce que cela va vraisemblablement prendre environ deux ans — oui ou non?

**M. MacSween :** Cela pourrait être plus court.

**La sénatrice Batters :** De combien exactement?

**M. MacSween :** On pourrait facilement y parvenir en 12 à 18 mois.

**La sénatrice Batters :** Très bien. Par ailleurs, le ministre a déclaré avoir rencontré le commissaire à la protection de la vie privée en octobre, mais cela s'est produit plusieurs mois après le dépôt du projet de loi C-8. Pourquoi le commissaire à la protection de la vie privée et le commissaire au renseignement n'ont-ils pas été consultés avant le dépôt du projet de loi C-8? Tous deux avaient en effet exprimé de sérieuses préoccupations concernant la protection de la vie privée, les pouvoirs de l'État, la surveillance et l'absence de consultation de la part du gouvernement lors de l'examen du projet de loi C-26.

**Kelly-Anne Gibson, directrice, Politique cybersécurité nationale, Direction de la sécurité nationale et de la cybersécurité, Sécurité publique Canada :** Le projet de loi C-26 a été déposé, si je ne m'abuse, en juin 2022. Nous avions tenu des consultations techniques avec le commissaire à la protection de la vie privée en juin 2019, donc cela remonte techniquement à une date antérieure.

**La sénatrice Batters :** C'était bien avant le dépôt du projet de loi. Je parle des consultations portant sur le projet de loi en soi et des préoccupations qu'ils avaient soulevées dans le projet de loi C-26 afin qu'elles puissent être corrigées dans le projet de loi C-8. Pourquoi n'a-t-on pas mené ce genre de consultations alors que ces deux commissaires ont soulevé ces préoccupations tout au long du processus du projet de loi C-26?

**Mme Gibson :** Le projet de loi avait été rédigé lorsque nous leur avons parlé en 2019. Il avait été rédigé, puis il a été présenté ensuite, bien sûr.

**La sénatrice Batters :** Je me demande toutefois pourquoi ils n'ont pas été consultés après que le projet de loi C-26 est mort au feuilleton, au moment où vous prépariez le projet de loi C-8. Ils avaient soulevé de sérieuses inquiétudes concernant le processus en comité, tant à la Chambre des communes qu'au Sénat. Pourquoi le gouvernement ne les a-t-il pas consultés à ce moment-là pour tenter d'améliorer le projet de loi avant sa réintroduction sous la forme du projet de loi C-8?

**Ms. Gibson:** We didn't consult. We had consulted in other instances, and we had examined their submissions very carefully. We went with the changes that had been made in the House and the Senate.

**Senator Batters:** Not the ones from the Senate. The Privacy Commissioner had specifically requested an amendment. This was the one that Senator McNair was referencing earlier. It was the third out of the three that he had requested, and it was the actual amendment that I brought to the Senate committee. It was not adopted by the Senate, but it was one that the Privacy Commissioner wanted to know about with respect to what specific major cyber incidents would be so he could know whether to investigate and also inform Canadians, if need be.

**Senator McNair:** Mr. MacSween, you talked about the financial impact on designated operators. It ties into a concern some of my colleagues have raised about small- and medium-sized enterprises making up over 99% of businesses in Canada and employing 90% of the private sector workforce. Increasingly, many of these firms, as you are aware, are digital and rely on telecommunications infrastructure.

Given that Bill C-8 introduces new compliance expectations and potential orders affecting telecom systems, how will the government ensure that SMEs are not disproportionately burdened, particularly those without in-house legal or extensive cybersecurity capacity?

**Mr. MacSween:** Thank you for the question, senator.

The bill was designed with that in mind. We obviously don't want to see a negative financial impact, on small- and medium-sized enterprises in particular. I think if you look at Schedule 1, at the moment, the vast majority of designated operators would probably be on the larger side. Maybe it would help if I described that a little bit.

Schedule 1 establishes the sectors, for lack of a better term, to which the law would apply. Schedule 2, which will be developed during the regulatory process, will establish the classes of operators. It's not going to specifically name a particular institution, for example. Instead, it's going to say, "If you're an institution of this size that serves customers across the nation . . ." and so on. That is just by way of an example because that will be developed later. Those institutions that fall into that class would ultimately be subject to the requirements of the legislation.

**Mme Gibson :** Nous n'avons pas consulté à ce moment-là. Nous l'avions fait dans d'autres circonstances, et nous avions examiné leurs observations très attentivement. Nous avons repris les modifications qui avaient été adoptées à la Chambre des communes et au Sénat.

**La sénatrice Batters :** Pas celles du Sénat. Le commissaire à la protection de la vie privée avait expressément demandé une modification. C'est celle dont le sénateur McNair parlait tout à l'heure. C'était la dernière des trois modifications qu'il avait demandées, et c'était précisément celle que j'ai présentée au comité sénatorial permanent. Elle n'a pas été adoptée par le Sénat, mais c'était celle dont le commissaire à la protection de la vie privée voulait être informé, afin de savoir quels cyberincidents majeurs seraient concernés, pour pouvoir décider s'il devait enquêter et, au besoin, en informer les Canadiens.

**Le sénateur McNair :** Monsieur MacSween, vous avez évoqué l'impact financier sur les exploitants désignés. Cela rejoint une préoccupation que certains de mes collègues ont soulevée au sujet des petites et moyennes entreprises, les PME, qui représentent plus de 99 % des entreprises au Canada et emploient 90 % de la main-d'œuvre dans le secteur privé. Comme vous le savez, bon nombre de ces entreprises sont de plus en plus numériques et dépendent des infrastructures de télécommunications.

Étant donné que le projet de loi C-8 introduit de nouvelles exigences de conformité et des décrets potentiels affectant les systèmes de télécommunications, comment le gouvernement veillera-t-il à ce que les PME ne soient pas trop lourdement touchées, particulièrement celles qui ne disposent pas de services juridiques internes ou de capacités étendues en cybersécurité?

**M. MacSween :** Merci pour la question, monsieur le sénateur.

Le projet de loi a été conçu en tenant compte de cet aspect. Nous ne voulons évidemment pas qu'il ait un impact financier négatif, surtout pour les petites et moyennes entreprises. Je pense que si vous consultez l'annexe 1, actuellement, la grande majorité des exploitants désignés seraient probablement des exploitants de grande taille. Peut-être serait-il utile que je vous explique un peu comment cela fonctionnera.

L'annexe 1 établit les secteurs, faute d'un meilleur terme, auxquels la loi s'appliquerait. L'annexe 2, qui sera élaborée dans le cadre du processus réglementaire, définira les catégories d'exploitants. Elle ne désignera pas expressément un organisme en particulier, par exemple. On y visera plutôt les organismes d'une certaine taille qui desservent des clients à l'échelle nationale, et ainsi de suite. Ce n'est qu'un exemple, car cela sera développé ultérieurement. Les organismes qui relèvent de cette catégorie seront en bout de ligne soumis aux exigences de la loi.

Part of the benefit of the regulatory process, even though we will be expediting this as quickly as we can, is it will give us time to determine what those classes of operators will look like.

To help us with that, the way the law works is that the existing regulators are actually the ones who will ultimately be responsible for ensuring compliance with the act. That's helpful for us because those existing regulators know their sectors incredibly well, including the entities that make up those sectors. Aside from hearing from industry directly, we'll also be able to benefit from their knowledge when we set out those classes of operators.

[*Translation*]

**Senator Carignan:** I see that there have been several amendments to the bill compared to Bill C-26. I would imagine that this was necessary to maintain a balance when it comes to the protection of personal information and privacy. It is clear that new information or insights have come to light in that regard. However, subclause 20(1.1) includes the following prohibition: ". . . the Governor in Council must not order the decoding of an encrypted *private communication*". That was not included in Bill C-26. Why did the government include this prohibition, which would prevent the Governor-in-Council from ordering decoding? How might that affect the effectiveness of investigations?

[*English*]

**Mr. MacSween:** Thank you very much for the question, senator.

That provision was an amendment proposed by the government. It was designed to address some concerns, specifically from civil liberties organizations, that this legislation could be used to undermine encryption or otherwise create a back door. The government decided to introduce the amendment to ensure that prohibition was there.

It is a "for greater certainty" that could never have been in the first place. The act is designed to protect the underlying infrastructure; that's the objective of the act. There would be no action that the government could take to undermine that objective in the law. However, for greater certainty, that provision was added to address that concern and ensure the appropriate guardrails were in place.

[*Translation*]

**Senator Carignan:** This refers to section 183 of the Criminal Code, so does that mean it refers only to the communications of people who are in Canada?

L'un des avantages du processus réglementaire, même si nous allons l'accélérer au maximum, est qu'il nous donnera le temps de déterminer à quoi ressembleront ces catégories d'exploitants.

Pour nous aider dans cette tâche, la loi prévoit que les organismes réglementaires existants seront en fin de compte responsables de veiller à la conformité à la loi. Cela nous est utile parce que ces organismes connaissent extrêmement bien leurs secteurs, y compris les entités qui les composent. Outre les informations reçues directement des intervenants de l'industrie, nous pourrons aussi bénéficier de leurs connaissances lors de l'établissement de ces catégories d'exploitants.

[*Français*]

**Le sénateur Carignan :** Je vois qu'il y a eu plusieurs modifications au projet de loi par rapport au projet de loi C-26. J'imagine que c'est nécessaire pour conserver un équilibre en matière de protection des renseignements personnels et de protection de la vie privée. On constate qu'il y a eu de l'information ou un nouvel éclairage à ce niveau. Cependant, le paragraphe 20(1.1) prévoit cette interdiction : « Le gouverneur en conseil ne peut cependant ordonner le décodage d'une *communication privée* [...] » Cela n'existait pas dans le projet de loi C-26. Pourquoi a-t-on inclus cette interdiction d'ordonner le décodage pour le gouverneur en conseil? En quoi cela peut-il affecter l'efficacité des enquêtes?

[*Traduction*]

**M. MacSween :** Merci beaucoup pour la question, monsieur le sénateur.

Cette disposition était une modification proposée par le gouvernement. Elle visait à répondre à certaines préoccupations, notamment celles d'organisations de défense des libertés civiles, selon lesquelles cette législation pourrait être utilisée pour affaiblir le chiffrement ou créer une porte dérobée. Le gouvernement a décidé de présenter cette modification afin d'assurer l'existence de cette interdiction.

Il s'agit d'une disposition de précision qui n'aurait jamais dû être nécessaire. La loi vise à protéger les infrastructures sous-jacentes; tel est son objectif. Aucun acte gouvernemental ne pourrait s'opposer à cet objectif dans la loi. Toutefois, à titre de précision, cette disposition a été ajoutée pour répondre à cette préoccupation et garantir la présence de garde-fous appropriés.

[*Français*]

**Le sénateur Carignan :** On vise l'article 183 du Code criminel, donc seulement les communications pour lesquelles une personne se trouve au Canada?

[*English*]

**Ms. Gibson:** Yes, you're correct. It references section 183 of the Criminal Code. It would use that definition.

**Senator Kutcher:** I want to follow up on the question from Senator McNair with regard to small- and medium-sized enterprises that need to comply with the act.

Have you given any thought to providing assistance to the ones that don't have access to extensive legal support and all that — perhaps non-profit players? Have you given any thought to providing assistance to them to help them come into compliance?

**Mr. MacSween:** Thank you for the question, senator.

Yes, that is contemplated in the bill. When we look at the role of the Canadian Centre for Cyber Security in this piece of legislation, we're leveraging their advice and guidance mandate in the Communications Security Establishment Act. That is to say that they will be obligated to provide technical advice and guidance to the government but also to regulators and designated operators. In that instance, those designated operators, if it were the case that they didn't have the technical sophistication to spell out what they're doing to protect their vital services or systems, they could turn to the Canadian Centre for Cyber Security for assistance.

Reflecting upon that, it's important for us to consider that we are talking about vital services and systems for Canadians. At an initial glance, the impacts on small- and medium-sized enterprises aren't evident right away. For example, we're talking about banking systems by the big four banks; the telecommunications network, which is predominantly owned by three large companies in Canada; and the energy sector. For the energy sector, it's important to consider that the federal government regulates only segments of that, so there are interprovincial and cross-border elements, as well.

The way the act is set up, we're well positioned to support SMEs as well as we can. Again, any consideration of the impacts on SMEs will be taken into account as the regulations are drafted.

**Senator Cardozo:** What would be examples of SMEs that would be under the act? Would there be non-profit organizations?

**Ms. Gibson:** The way we thought about it in terms of small- and medium-sized enterprises, they would have to provide a function that is absolutely vital. The only case where it would be a small enterprise is if it were an entity that provided a very specific type of service or product as part of a broader chain.

We don't think, initially, that any small- and medium-sized enterprise would be designated, necessarily.

[*Traduction*]

**Mme Gibson :** Oui, vous avez raison. Il s'agit d'un renvoi à l'article 183 du Code criminel. C'est cette définition qui serait utilisée.

**Le sénateur Kutcher :** Je voudrais revenir sur la question du sénateur McNair concernant les petites et moyennes entreprises qui doivent se conformer à la loi.

Avez-vous envisagé d'offrir de l'aide à celles qui n'ont pas accès à un soutien juridique étendu, peut-être des organismes sans but lucratif? Avez-vous pensé à leur fournir une assistance pour les aider à se conformer?

**M. MacSween :** Merci pour la question, monsieur le sénateur.

Oui, cela est prévu dans le projet de loi. Quant au rôle du Centre canadien pour la cybersécurité dans ce texte, nous tirons parti de son mandat de conseil et d'orientation prévu dans la Loi sur le Centre de la sécurité des télécommunications. Cela signifie qu'il sera tenu de fournir des conseils et de l'orientation technique au gouvernement, mais aussi aux organismes réglementaires et aux exploitants désignés. Ainsi, lorsque ces exploitants désignés n'auraient pas les ressources techniques nécessaires pour expliquer leurs mesures de protection des services ou systèmes critiques, ils pourraient solliciter l'aide du Centre canadien pour la cybersécurité.

Cela dit, il est important de se rappeler qu'il s'agit de services et systèmes critiques pour les Canadiens. À première vue, les répercussions sur les petites et moyennes entreprises ne sautent pas aux yeux. Par exemple, on parle des systèmes des quatre grandes banques, du réseau de télécommunications, détenu en majorité par trois grandes entreprises au Canada, et du secteur de l'énergie. Pour ce dernier, il convient de signaler que puisque le gouvernement fédéral n'en réglemente que certains segments, il faut aussi tenir compte d'éléments interprovinciaux et transfrontaliers.

La structure de la loi nous place en bonne position pour soutenir au mieux les PME. Encore une fois, toute considération des répercussions sur les PME sera prise en compte lors de l'élaboration des règlements.

**Le sénateur Cardozo :** Quels seraient des exemples de PME relevant de la loi? Les organismes sans but lucratif en feraient-ils partie?

**Mme Gibson :** En termes de petites et moyennes entreprises, elles devraient fournir une fonction absolument critique. Le seul cas où il s'agirait d'une petite entreprise, c'est si elle fournissait un type très spécifique de service ou de produit dans le cadre d'une chaîne plus large.

Nous ne pensons pas, dans un premier temps, qu'une PME serait nécessairement désignée.

A bigger risk to small- and medium-sized enterprises is actually if one of the vital services goes down. For instance, if they lose access to the telecommunications network and can't do a transaction, that's a bigger risk. However, having them actually be designated is relatively unlikely, we believe, unless they have a very specific function within the broader chain of the vital service.

**Senator Cardozo:** On the other issue of foreign interference in Canada, does this deal with that issue? It does, I'm sure, but what's the crossover?

**Mr. MacSween:** As it relates to Part 2 of the bill, it does address the threat of foreign interference insofar as that threat is directed at a vital service or system for Canadians. It's important to consider that's the focus for Part 2 of the legislation. We do not tend to think of it in terms of the actual threat vector; it's more about what it is that we're protecting from an array of threats.

Again, that's why we go back to the fact that the bill is centred upon the idea that ensuring these vital services for Canadians are available and as resilient as possible.

**Senator Cardozo:** Thank you.

**Senator Kutcher:** Thank you all for being here. You're the four horsemen — or four horsepeople — of this bill.

I have the same question for each of you. We can start with Ms. Gibson and go from there. Now that you've listened to the debates in the House and you've heard the comments of witnesses in the House — and I know you would have studied them very carefully — is there one thing you would suggest the Senate think about that would improve the bill?

**Ms. Gibson:** That's a tough question.

**Senator Kutcher:** I thought it was a soft lob.

**Ms. Gibson:** I've been part of this bill since it was Bill C-26, and I've seen the large numbers of improvements that have gone in, both when it was Bill C-26 and now as Bill C-8. I honestly can't think of something in particular that you could put in that would improve it.

Would I like to be able to cover more sectors? Absolutely, but that's not within our current Constitution. I'd like to be able to afford the protections to a greater jurisdiction, but since that's not currently not possible, I don't think there's anything in particular that I would recommend.

**Mr. MacSween:** I am in the same boat, only because Parliament has had two chances at this legislation, and there were amendments from both the House of Commons and the Senate the last time. That made a number of changes, and all for the better, I think.

Le véritable risque pour les PME réside en fait dans la défaillance d'un service critique. Par exemple, si elles perdent l'accès au réseau de télécommunications et ne peuvent plus effectuer de transactions, c'est un risque plus grand. Cependant, nous pensons qu'il est relativement peu probable qu'elles soient effectivement désignées à moins d'avoir une fonction très spécifique dans la chaîne globale du service critique.

**Le sénateur Cardozo :** Concernant la question de l'ingérence étrangère au Canada, est-ce qu'il en est question dans cette loi? Je présume que oui, mais comment le lien avec ce sujet est-il établi?

**M. MacSween :** En ce qui concerne la partie 2 du projet de loi, elle traite effectivement de la menace d'ingérence étrangère dans la mesure où cette menace cible un service ou un système critique pour les Canadiens. Il est important de signaler que c'est le point central de la partie 2 de la loi. Nous ne l'envisageons pas tant sous l'angle du vecteur de la menace, mais plutôt par rapport à ce que nous protégeons contre une gamme de menaces.

C'est pour cela que nous revenons à l'idée que le projet de loi est centré sur la garantie de la disponibilité et de la résilience de ces services critiques pour les Canadiens.

**Le sénateur Cardozo :** Merci.

**Le sénateur Kutcher :** Merci à vous tous d'être ici. Vous êtes les quatre cavaliers — et cavalières — de ce projet de loi.

J'ai la même question pour chacun et chacune d'entre vous. Nous pouvons commencer par Mme Gibson et ainsi de suite. Maintenant que vous avez écouté les débats et entendu les témoignages à la Chambre — que je sais que vous avez étudiés attentivement — y a-t-il une chose que vous suggéreriez au Sénat de prendre en compte pour améliorer ce projet de loi?

**Mme Gibson :** C'est une question difficile.

**Le sénateur Kutcher :** Moi qui pensais qu'elle était facile.

**Mme Gibson :** Je participe à l'élaboration de ce projet de loi depuis qu'il s'appelait C-26, et j'ai vu les nombreuses améliorations apportées, tant à l'époque qu'aujourd'hui avec le projet de loi C-8. Honnêtement, je ne vois rien en particulier à ajouter pour l'améliorer.

Voudrais-je couvrir davantage de secteurs? Absolument, mais cela ne relève pas de la Constitution actuelle. Je souhaiterais étendre ces protections à de plus vastes champs de compétence, mais comme ce n'est pas possible à l'heure actuelle, je ne recommande rien de particulier.

**M. MacSween :** Je suis dans le même cas, simplement parce que le Parlement a eu deux occasions d'examiner ce projet de loi, et d'étudier des modifications proposées tant par la Chambre que par le Sénat. Cela a entraîné plusieurs changements, tous pour le mieux, à mon avis.

I'm at a loss as to how we could improve it more. I think this gets to a bit of an earlier question. The way the bill is constructed, it's designed to work with technology.

There is some criticism that the actual legislation itself could be seen as vague. In a way, that's deliberate, though, because if we start talking about technology or certain types of threats, such as ransomware, I know that came up, the legislation would stale-date really quickly. Having legislation that puts in place the regulator framework where we can start to build out the detail and then have more of the technological detail in the cybersecurity programs is a very sound approach.

**Andre Arbour, Director General, Telecommunications and Internet Policy Branch, Innovation, Science and Economic Development Canada:** Thank you, senator, for the question. Given that there's been quite a bit of study or engagement on the substance of the bill itself, nothing comes to mind in terms of the bill itself. What's keeping me up at night is the lack of authority to take action in this space, and we have just scratched the surface in some of the questions in the first hour on the range of threats that we're seeing. There is a fivefold increase in catastrophic damage from extreme weather events and skyrocketing increases in ransomware due to what we've seen in terms of organized crime and crypto-currency. There are hostile actors, and CSE has publicly talked about the People's Republic of China, or PRC, Russia and Iran specifically, and pre-positioning or linking them to other geopolitical events.

To my colleague's point, a lot of the devil in the details will be worked out through the regulatory process, but we are already pretty substantially behind and are champing at the bit to try to get on with it, frankly. Thank you.

**Wen Kwan, Director General, Spectrum and Telecommunications Sector, Science and Economic Development Canada:** Thank you, senator, for the question. As you might expect, I would say nothing, but I will add a bit more context to it.

This bill has a good balance in terms of the viewpoints from a variety of stakeholders. You name it: We have provincial infrastructure operators; people from civil societies, academia and other associations; the Intelligence Commissioner; and the Privacy Commissioner — and the list goes on.

There's nothing in my mind that would change the bill substantively in a way that is better. We will never be 100% perfect. Cybersecurity is never 100% secure, so the most urgent need in front of us is to get the framework going so we can take real action — because some action is better than nothing.

Je ne vois vraiment pas comment l'améliorer davantage. Cela rejoint en partie une question précédente. Le projet de loi est conçu pour s'adapter à l'évolution de la technologie.

On reproche parfois à la loi d'être vague, ce qui est, en fait, un choix délibéré, car si nous commencions à parler de technologies ou de menaces en particulier comme les rançongiciels — ce qui a été évoqué —, la loi deviendrait rapidement obsolète. Avoir une loi qui établit un cadre réglementaire permettant de développer les détails, puis d'intégrer la technicité dans les programmes de cybersécurité, est une approche très solide.

**Andre Arbour, directeur général, Direction générale des politiques des télécommunications et de l'Internet, Innovation, Sciences et Développement économique Canada :** Merci, monsieur le sénateur, pour cette question. Vu les études et débats déjà menés au sujet du projet de loi, rien ne me vient à l'esprit quant au contenu en soi. Ce qui m'inquiète, c'est le manque de pouvoirs pour intervenir dans ce domaine. Pendant la première heure, nous n'avons fait que survoler les questions liées à l'éventail des menaces observées. On observe une multiplication par cinq des dommages catastrophiques causés par les phénomènes météorologiques extrêmes, et une hausse astronomique des cas de rançongiciels liés au crime organisé et aux cryptomonnaies. Il y a des acteurs hostiles; le Centre de la sécurité des télécommunications a parlé publiquement de la République populaire de Chine, de la Russie et de l'Iran en particulier, les reliant à d'autres événements géopolitiques.

Pour reprendre le commentaire de mon collègue, beaucoup de détails seront réglés dans le cadre du processus réglementaire, mais nous accusons déjà un assez grand retard et, pour être franc, nous sommes impatients de passer à l'action. Merci.

**Wen Kwan, directeur général, Secteur du spectre et des télécommunications, Innovation, Sciences et Développement économique Canada :** Merci, monsieur le sénateur, pour la question. Comme vous devez vous y attendre, je dirais qu'il n'y a rien à ajouter au projet de loi, mais j'aimerais donner un peu plus de contexte.

Ce projet de loi présente un bon équilibre en termes de points de vue de diverses parties prenantes. Il suffit de penser aux exploitants d'infrastructures provinciales, aux membres de la société civile, au milieu universitaire et à d'autres associations, au commissaire au renseignement, au commissaire à la protection de la vie privée, et ainsi de suite.

À mon avis, rien ne viendrait modifier substantiellement le projet de loi de manière avantageuse. Nous n'atteindrons jamais la perfection. La cybersécurité n'est jamais totalement sécurisée, donc le besoin le plus urgent devant nous est de lancer le cadre afin que nous puissions passer à l'action, parce qu'il vaut mieux bouger que de ne rien faire du tout.

**Senator Ince:** Mr. MacSween, this committee received a letter earlier today from an industry player who seems to think that you've overlooked an area in cybersecurity protection, and that is discarded electronic devices and properly wiping equipment and devices. Can you give us an idea of whether that is something you have thought about? Is it something that we should be concerned with?

**Mr. MacSween:** Thank you, senator, for the question. I don't know if we thought about that one very specific issue. If that is of concern — and this kind of goes back to my previous point about how the legislation is set up — when designated operators will be required to lay out their cybersecurity programs, we will have the opportunity in the regulations to build in what will be required in those programs. If the disposition of older devices is determined to be of concern, that can absolutely be built in as a requirement in the regulations for cybersecurity programs.

The honest answer to the question of whether we thought specifically about that is no. But can we address it under the legislation? Yes, that can be done. Absolutely.

**Senator Ince:** Let me try to get an understanding. When we talk about scanning equipment, confidential records, information, storage, media vaulting, digital and so on, you're saying that it's something that could be addressed?

**Mr. MacSween:** Yes. The caveat I have to put on that, though, is it's insofar as it impacts a vital service or system. It always comes back to the protection of the vital service or system. As I mentioned, if any of those are considerations in the protection of that vital service or system, then yes, they can be considered.

**Senator Ince:** Thank you.

**Senator Yussuff:** I have a series of questions. I will put them to you in rapid fire.

Given it's been quite some time since the last bill we were studying — here we are again on Bill C-8 — how would you describe the urgency around getting this passed?

**Mr. Arbour:** Thank you, senator, for the question.

The one mitigating factor is that in the interim we maintain some good, cooperative, voluntary activities with the private sector. It's not to say that we're not doing anything while waiting for the bill to pass.

Frankly, however, we're falling further and further behind in terms of our ability to stand up the core architecture. There are many unknowns. When we start getting incident reports and

**Le sénateur Ince :** Monsieur MacSween, ce comité a reçu plus tôt dans la journée une lettre d'un intervenant de l'industrie qui semble penser que vous avez omis un aspect de la protection en cybersécurité, à savoir les appareils électroniques mis au rebut et l'effacement sécurisé des équipements et appareils. Pouvez-vous nous dire si vous avez réfléchi à cette question? Est-ce un sujet qui devrait nous préoccuper?

**M. MacSween :** Merci, monsieur le sénateur, pour la question. Je ne sais pas si nous avons réfléchi à cette question en particulier. Si cela suscite une préoccupation — ce qui renvoie un peu à mon point précédent sur la structure de la législation —, lorsque les exploitants désignés devront présenter leurs programmes de cybersécurité, nous aurons la possibilité dans la réglementation d'intégrer ce qui sera requis dans ces programmes. Si la mise aux rebuts des appareils plus anciens est jugée préoccupante, cela pourra absolument être intégré comme exigence dans la réglementation des programmes de cybersécurité.

Pour répondre honnêtement à la question de savoir si nous y avons pensé expressément, la réponse est non. Mais pouvons-nous y répondre dans le cadre de la législation? Oui, cela peut se faire. Absolument.

**Le sénateur Ince :** Laissez-moi essayer de comprendre. Quand on parle d'équipement de numérisation, de documents confidentiels, d'informations, de stockage, d'archivage sur support physique, de données numériques, et ainsi de suite, vous dites que c'est un sujet auquel vous pourriez réfléchir?

**M. MacSween :** Oui. La réserve que je dois faire, toutefois, est que cela s'applique dans la mesure où cela touche un service ou un système critique. Tout revient toujours à la protection du service ou du système critique. Comme je l'ai dit, si ces éléments doivent être pris en compte dans la protection de ce service ou système critique, alors oui, ils pourront être considérés.

**Le sénateur Ince :** Merci.

**Le sénateur Yussuff :** J'ai une série de questions. Je vais vous les poser à un rythme rapide.

Puisqu'il s'est écoulé un certain temps depuis le dernier projet de loi que nous avons étudié — nous réexaminons maintenant le projet de loi C-8 —, comment décririez-vous l'urgence de le faire adopter?

**M. Arbour :** Merci, monsieur le sénateur, pour la question.

Le facteur atténuant est que, dans l'intervalle, nous poursuivons des activités volontaires, coopératives et efficaces avec le secteur privé. Cela ne veut pas dire que nous ne faisons rien en attendant l'adoption du projet de loi.

Pour être franc, cependant, nous prenons un retard de plus en plus important dans notre capacité à mettre en place l'architecture de base. Beaucoup de choses restent inconnues.

more granular information, we will be in a better position to truly understand the nature of the challenges we are dealing with.

Sequencing the regulatory program will be a real challenge because there is a lot we will need to be prepared to tackle.

As it stands, first out of the gate — at least in the telecom space — will be high-risk vendor equipment. Then there is a slate of other considerations as we look at the security and resiliency of our networks. We will need to think hard about how best to sequence that because industry can only absorb so much in any given period, and we will do our best to design those rules so it is factored into their natural provisioning cycles so that it can be implemented in a sane way.

However, that will involve consultation and ensuring that we're rolling it out in a staggered way so that it can best be implemented by our partners in the private sector.

**Senator Yussuff:** I have a follow-up on the question Senator Batters asked you, specifically on the time frame for the regulatory regime to happen. Given the urgency of this bill, because we are way behind on the needs of the country's security, if we were to make an observation that we expect the government to move as quickly as possible within the next 12 months on the regulatory regime — because this legislation would be ineffective unless you have the regulatory regime — would that give you some strength, to be able to say, "We have direction that we need to act on in terms of the time frame"? We know regulation could take forever, and we can't compel you once this bill is adopted by the Senate and then the House.

**Mr. Arbour:** Thank you, senator, for the question. Certainly, on the telecom space, the architecture is different such that we're probably looking more within a 6-to-12-month time frame. It will depend on the decisions of cabinet, and it will also depend, to a certain degree, on what stakeholder comments we get. If we get a lot of unexpected things, then we will need to take more time to ensure that we get it right.

Certainly, we are seized with it. Ultimately, decisions are made by cabinet, but there's an appreciation of the need to move quickly. Certainly, we have heard from the Prime Minister about his emphasis on that, and we are gearing up to try to hit the ground running post-Royal Assent, should that be received.

Lorsque nous commencerons à recevoir des rapports d'incident et des informations plus détaillées, nous serons mieux placés pour comprendre véritablement la nature des défis auxquels nous faisons face.

La séquence du programme réglementaire sera un vrai défi parce qu'il y a beaucoup de choses que nous devrons être prêts à affronter.

Pour l'instant, les premiers concernés — du moins dans le domaine des télécommunications — seront les équipements des fournisseurs à haut risque. Ensuite, il y aura toute une série d'autres considérations lorsque nous examinerons la sécurité et la résilience de nos réseaux. Nous devrons réfléchir sérieusement à la meilleure manière de séquencer cette démarche parce que l'industrie ne peut absorber qu'une certaine charge à un moment donné, et nous ferons de notre mieux pour concevoir ces règles de manière à ce qu'elles s'intègrent naturellement dans leurs cycles de provisionnement afin d'être mises en œuvre de façon raisonnable.

Il faudra toutefois pour cela mener des consultations et assurer un déploiement échelonné afin que nos partenaires du secteur privé puissent procéder à la mise en œuvre de la meilleure façon possible.

**Le sénateur Yussuff :** Je reviens à la question que vous a posée la sénatrice Batters, plus précisément sur le calendrier de la mise en place du régime réglementaire. Étant donné l'urgence de ce projet de loi, puisque nous accusons beaucoup de retard face aux besoins en sécurité du pays, si nous faisions observer que nous attendons du gouvernement qu'il agisse le plus rapidement possible dans les 12 prochains mois pour établir le régime réglementaire — car cette législation serait inefficace sans ce régime —, cela vous permettrait-il d'affirmer avec une plus grande autorité : « Nous avons une directive selon laquelle nous devons agir dans un délai précis »? Nous savons que la réglementation peut prendre beaucoup de temps, et nous ne pouvons pas vous contraindre une fois que ce projet de loi aura été adopté par le Sénat puis la Chambre des communes.

**M. Arbour :** Merci, monsieur le sénateur, pour cette question. Assurément, dans le secteur des télécommunications, l'architecture est différente, de sorte que nous envisageons plutôt un horizon de 6 à 12 mois. Cela dépendra des décisions du Cabinet, et aussi, dans une certaine mesure, des observations que nous recevrons des intervenants. Si nous recevons beaucoup d'observations inattendues, nous devrons prendre plus de temps pour faire en sorte d'agir comme il se doit.

Nous en sommes assurément saisis. En fin de compte, les décisions sont prises par le Cabinet, mais il y a une reconnaissance de la nécessité d'agir vite. Le premier ministre a d'ailleurs fait part de son insistance à ce sujet, et nous nous préparons à être opérationnels dès la sanction royale, si celle-ci est accordée.

**Senator Yussuff:** Thank you.

**Senator Hay:** Thank you, all. I was triggered, probably literally through PTSD, by something that Senator McNair and then Senator Cardozo spoke about around SMEs and not-for-profits. This may be out of scope, but I want to share an experience I had.

Perhaps the definition of "vital service or system" needs to be refined.

In an organization I worked in before as the CEO, we were attacked with malware, ransomware, in a bad-actor environment quite significantly. They had been in our system for quite a while, hovering through our emails as well as on the financial side. Luckily, our organization had great friends in the banking system. We are talking hundreds of thousands of dollars, which is a lot to a small not-for-profit, for sure, but we were able to trace it and engage the RCMP and other police.

I would say law enforcement was not particularly responsive; we were small folks. Yet an organization that's a 24-7 e-mental health solution is a vital service. So is 9-8-8 suicide prevention.

This may be totally out of scope, but it's a real-life example that we stickhandled, and it took us months to harden our system and figure it out. I'm curious how this bill would help an SME or a not-for-profit in a similar regard? Luckily, it didn't hit our data for the services we provided.

**Mr. MacSween:** As the minister pointed out, we can only legislate in the area of federal jurisdiction, hence the focus on federally regulated critical infrastructure. That being said, though, there are probably indirect benefits for small- or medium-sized organizations. Both Parts 1 and 2 are, obviously, heavily reliant on Canada's telecommunications network — in order to run your own systems and whatnot.

The powers in the bill that allow us to ensure that those things are being managed properly will absolutely have an indirect positive impact on those smaller areas.

As well, I would highlight that, though not related to the legislation, the Canadian Centre for Cyber Security does put out quite a bit of advice and guidance that anyone can benefit from. That's part of the reason that mandatory incident reporting is included in this bill: If we learn about a significant cybersecurity

**Le sénateur Yussuff :** Merci.

**La sénatrice Hay :** Merci à tous. J'ai été piquée au vif, probablement littéralement par un genre de trouble de stress post-traumatique, par ce qu'ont évoqué les sénateurs McNair et Cardozo à propos des PME et des organismes sans but lucratif. Cela peut être hors sujet, mais j'aimerais vous faire part d'une expérience que j'ai vécue.

Peut-être faudrait-il préciser la définition de « service ou système critique ».

Dans un organisme dont j'étais la PDG auparavant, nous avions été attaqués de manière assez importante par des logiciels malveillants, notamment des rançongiciels, par des acteurs mal intentionnés. Ils étaient dans notre système depuis un bon moment, circulant à travers nos courriels ainsi que dans nos données financières. Heureusement, notre organisation bénéficiait de précieux appuis dans le système bancaire. Nous parlons ici de centaines de milliers de dollars, ce qui est beaucoup pour un petit organisme sans but lucratif, certes, mais nous avons pu retracer les malfaiteurs et faire intervenir la GRC ainsi que d'autres forces policières.

Je dirais que les forces de l'ordre n'ont pas été particulièrement réactives; nous étions de petits joueurs. Pourtant, un organisme qui offre une solution en santé mentale en ligne accessible 24 heures par jour, sept jours sur sept, est un service critique. Il en est de même pour la ligne de prévention du suicide 9-8-8.

Cela peut être complètement hors sujet, mais c'est un exemple concret que nous avons dû gérer, et il nous a fallu des mois pour renforcer notre système et comprendre la situation. Je me demande comment ce projet de loi pourrait aider une PME ou un organisme sans but lucratif dans une situation similaire? Heureusement, cela n'a pas affecté les données relatives aux services que nous offrions.

**M. MacSween :** Comme le ministre l'a souligné, nous ne pouvons légiférer que dans des domaines relevant de la compétence fédérale, d'où l'accent mis sur les infrastructures essentielles sous réglementation fédérale. Cela dit, il y aura probablement des effets indirects bénéfiques pour les petites et moyennes entreprises. Les parties 1 et 2 reposent évidemment largement sur le réseau canadien de télécommunications, pour faire fonctionner vos propres systèmes et ainsi de suite.

Les pouvoirs conférés par le projet de loi visant à assurer une bonne gestion de ces éléments auront assurément un impact positif indirect sur ces plus petites entités.

Je souligne aussi que, même si ce n'est pas lié à la loi, le Centre canadien pour la cybersécurité publie beaucoup de conseils et d'orientations dont tout le monde peut bénéficier. C'est aussi pourquoi la déclaration obligatoire des incidents est prévue dans ce projet de loi. Si nous sommes informés

incident, the Canadian Centre for Cyber Security can take that in, anonymize the information and push out technical advice and guidance — whether it's to a small not-for-profit or a hospital or a large corporation — on how to address it and then how to fix it.

As my colleague often says, we want to create that virtuous circle whereby one incident becomes a defence for all the others.

**Senator Hay:** That's great. In the moment, though, that's not particularly helpful. At some point, I'm sure it will be. I don't mean to discount your advice.

The fact that it came in and out of the banking system, though, does that help a national not-for-profit because it's in that finance pillar?

**Mr. MacSween:** If it did come in and out of the banking system, then this should assist. Again, we have to stress that, at the end of the day, the bill is about ensuring that the designated operators are doing what they need to do to protect that vital service or system. If through that we're able to catch these types of threats, then ultimately it would have an impact —

**Senator Hay:** Thank you. I think it's slightly out of scope, but it's very helpful.

**Senator Dasko:** My question is about technology. We know how quickly technology changes. On the National Defence Committee, for example, we know a lot about drones and how drone technology changes almost every couple of weeks.

When it comes to the technology here, what's called defence technology — that is my terminology, not yours — the technology that companies will be using, how does the fact of change intersect with your regulatory framework?

You're requiring industries to take on various activities and technology. Do you also require them to keep up with changes? Is that part of the framework that you're putting into place?

**Mr. MacSween:** Thank you for the question. Yes, it can be. I will step back a little bit, as I mentioned this before.

The legislation itself, if you read it, is fairly technology agnostic. You don't see those terms in there. That's obviously deliberate because, to your point, it evolves and changes quickly. We don't want that legislation to stale-date.

d'un incident majeur de cybersécurité, le Centre canadien pour la cybersécurité peut recueillir les informations pertinentes, les anonymiser et diffuser des conseils techniques et recommandations — que ce soit à un petit organisme sans but lucratif, un hôpital ou une grande entreprise — sur la manière de gérer l'incident, puis de le corriger.

Comme le dit souvent mon collègue, nous voulons créer un cercle vertueux où un incident sert de moyen de défense pour tous les autres.

**La sénatrice Hay :** C'est très bien, mais pour le moment, ce n'est pas particulièrement utile. À un moment donné, j'en suis sûre, cela le sera. Je ne veux pas dévaluer vos conseils.

Le fait que cela soit passé par le système bancaire, cela aide-t-il un organisme national sans but lucratif, étant donné qu'il relève de ce pilier financier?

**M. MacSween :** Si cela transitait effectivement par le système bancaire, alors cela devrait aider. Encore une fois, je rappelle que, au fond, ce projet de loi vise à faire en sorte que les exploitants désignés font ce qu'il faut pour protéger ce service ou système critique. Si, grâce à cela, nous pouvons déceler ce genre de menaces, cela aura donc en bout de ligne une incidence...

**La sénatrice Hay :** Merci. Je pense que c'est un peu hors sujet, mais c'est très utile.

**La sénatrice Dasko :** Ma question porte sur la technologie. Nous savons à quelle vitesse la technologie évolue. Au Comité permanent de la défense nationale, par exemple, nous connaissons bien les drones et la rapidité avec laquelle la technologie des drones évolue, pratiquement toutes les deux semaines.

En ce qui concerne la technologie dont il est question ici, ce que j'appelle technologie de défense — c'est ma terminologie, pas la vôtre —, la technologie que les entreprises utiliseront, comment cette évolution s'inscrit-elle dans votre cadre réglementaire?

Vous exigez des industries qu'elles adoptent diverses activités et technologies. Leur demandez-vous aussi de suivre l'évolution de la technologie? Cela fait-il partie du cadre que vous mettez en place?

**M. MacSween :** Merci pour cette question. Oui, cela peut en faire partie. Je vais revenir un peu en arrière, puisque j'en ai déjà parlé.

Si vous lisez le texte de loi en soi, il est plutôt neutre sur le plan technologique. Vous n'y trouverez pas ces précisions. C'est bien sûr délibéré, car, comme vous le soulignez, la technologie évolue et change rapidement. Nous ne voulons pas que cette loi devienne tout de suite obsolète.

In terms of the type of technology that a designated operator would be using, we would see that articulated in their cybersecurity program, for one, but the other key point in this bill is that they will be required to identify and mitigate risks in their supply chain.

If they are using a certain piece of technology that presents security risks, then the designated operators themselves will have to identify that and either describe how they are mitigating that risk or changing the technology. If there were a significant enough concern with that technology, there are obviously order-making powers in legislation that could be used to have them remove that piece of technology and so on.

That is the long way around saying that's how we intend to get to that question in the bill: through the identification in the programs and risk identification and mitigation.

**Senator Dasko:** You're saying directly you have to change the technology but through the responsibilities they have going through it.

**Mr. MacSween:** Yes. I should note as well that the cybersecurity programs have to be refreshed. Perhaps my colleague can remind me how.

**Ms. Gibson:** It's on an annual basis. I would add that, through incident reporting, we will also get smarter in terms of understanding what's coming at us so that we can refine those cybersecurity programs and adjust our defences. It's really meant to be an ongoing iterative process.

**Senator Dasko:** Thank you.

**The Chair:** In round two, Senator Batters and Senator Yussuff, if you wouldn't mind both presenting your questions, we will have an opportunity for our panel to answer them.

**Senator Batters:** The government's own Gender-based Analysis Plus for Bill C-8, except for three paragraphs found in the former Bill C-26 document that are missing from the new Bill C-8 document, is identical. In their place is the word "redacted." Even so, the entire two-page Gender-based Analysis Plus document only refers to "women and girls" once.

Why did the government redact those three paragraphs in the Bill C-8 GBA Plus? It was a rare passage that actually specifically noted possible negative effects on certain Canadians. Was it to avoid drawing attention to the bill's adverse consequences in hopes that parliamentarians wouldn't notice it and wouldn't notice what had been removed? Why are women and girls treated almost as an aside in a Gender-based Analysis Plus document?

En ce qui concerne le type de technologie qu'un exploitant désigné utilisera, cela sera précisé dans son programme de cybersécurité, mais un autre point clé de ce projet de loi est qu'il devra identifier et atténuer les risques dans sa chaîne d'approvisionnement.

S'ils utilisent une certaine technologie présentant des risques de sécurité, les exploitants désignés devront identifier ces risques eux-mêmes et soit expliquer comment ils les atténuent, soit changer de technologie. S'il y avait une préoccupation suffisamment importante vis-à-vis de cette technologie, la loi prévoit évidemment des pouvoirs réglementaires pouvant les contraindre à retirer cette technologie, et ainsi de suite.

Autrement dit, c'est ainsi que nous envisageons de répondre à cette question dans le projet de loi : par l'identification dans les programmes, ainsi que par l'identification et l'atténuation des risques.

**La sénatrice Dasko :** Vous dites donc qu'il faut changer la technologie, mais indirectement, dans le cadre des responsabilités qui incombent à ceux qui la gèrent.

**M. MacSween :** Oui. Je précise aussi que les programmes de cybersécurité doivent être actualisés. Ma collègue pourra peut-être me rappeler comment.

**Mme Gibson :** C'est sur une base annuelle. J'ajouterais qu'avec le signalement des incidents, nous deviendrons aussi mieux informés par rapport aux menaces, ce qui nous permettra d'affiner ces programmes et d'ajuster nos moyens de défense. Il s'agit véritablement d'un processus itératif continu.

**La sénatrice Dasko :** Merci.

**La présidente :** Lors de la deuxième partie, madame Batters et monsieur Yussuff, pourriez-vous présenter vos questions tous les deux? Notre groupe de témoins aura alors l'occasion d'y répondre.

**La sénatrice Batters :** L'analyse comparative entre les sexes plus du gouvernement pour le projet de loi C-8 est identique, sauf pour trois paragraphes qui figuraient dans l'ancien document du projet de loi C-26 et qui manquent dans le nouveau projet de loi C-8. À leur place, on trouve le mot « caviardé ». Pourtant, dans ce document de deux pages sur l'analyse comparative entre les sexes plus, il n'est question des « femmes et des filles » qu'une seule fois.

Pourquoi le gouvernement a-t-il censuré ces trois paragraphes dans l'analyse comparative entre les sexes plus du projet de loi C-8? C'était un passage rare qui notait expressément des effets négatifs possibles sur un certain groupe de Canadiens. Était-ce pour éviter d'attirer l'attention sur les conséquences défavorables du projet de loi, en espérant que les parlementaires ne le remarqueraient pas et ne verraient pas ce qui avait été caviardé? Pourquoi les femmes et les filles sont-elles traitées

**Senator Yussuff:** The two big concerns whether this bill meets the test or not have always been, first, whether there is a reasonable balance regarding privacy; and, second, whether there is a reasonable balance in terms of civil rights? The intrusion could always be the creep.

From the amendments that have been made at the House and what you have heard through Bill C-26, do you think we strike the right balance here?

The last question I would raise has to do with telecom data that is offshored for use by other operators that we have no control over because they are in another territory. How do we hold them accountable when they offshore that data outside the country?

**Mr. MacSween:** On the GBA Plus question, we'll have to undertake to follow up with the committee, just so we can review the missing language. I'm not familiar with it off the top of my ahead.

In terms of striking the right balance, I believe we have. A lot of the amendments that were made obviously reaffirm the application of the Privacy Act and put significant guardrails around the order-making powers.

With Part 2, the act itself doesn't contemplate the collection of personal information. It's really focused on either confidential information — and we see that defined in the act and the protections around that — and technical information. That means technical information that would be required to assess a cybersecurity incident and determine what the technical response will be. The risk of that materializing would come through the mandatory incident reporting by the designated operator to the Canadian Centre for Cyber Security.

We have to acknowledge, though, that even though we will spell out in regulations the information a designated operator is to provide, which wouldn't include personal information, its inclusion is always a possibility. The Intelligence Commissioner himself was on record as saying that in his reviews he has seen cases where information came in personally identifiable information, or PII, so that's the real importance of striking that balance. We rely on the existing safeguards: the application of the Privacy Act in order to protect personal information as well as all the safeguards built into the Communications Security Establishment Act.

de façon presque cavalière dans un document d'analyse comparative entre les sexes plus?

**Le sénateur Yussuff :** Les deux grandes questions qui se posent pour savoir si ce projet de loi tient la route sont toujours les mêmes. Premièrement, existe-t-il un juste équilibre en matière de vie privée et, deuxièmement, existe-t-il un juste équilibre en matière de droits civils? Le soupçon porte sur l'intrus.

Au vu des modifications apportées à la Chambre et de ce que vous avez entendu à propos du projet de loi C-26, pensez-vous que nous ayons trouvé le juste équilibre dans ce dossier?

Ma dernière question concerne les données de télécommunications qui sont transférées à l'étranger pour être utilisées par d'autres opérateurs sur lesquels nous n'avons aucun contrôle, parce qu'ils sont dans un autre territoire. Comment pouvons-nous les tenir responsables lorsqu'ils transfèrent ces données hors du pays?

**M. MacSween :** En ce qui concerne la question relative à l'analyse comparative entre les sexes plus, ou ACS+, nous devrons vous revenir, car nous allons devoir examiner les passages manquants. Je n'ai pas cela en tête.

En ce qui concerne la recherche d'un juste équilibre, je pense que nous y sommes parvenus. Bon nombre des modifications apportées réaffirment clairement l'application de la Loi sur la protection des renseignements personnels et établissent de véritables garde-fous autour des pouvoirs réglementaires.

Dans la partie 2, la loi elle-même ne vise pas la collecte de renseignements personnels. Elle porte en réalité soit sur les renseignements confidentiels — dont la définition et les mesures de protection sont précisées dans la loi —, soit sur les renseignements techniques. Il s'agit des renseignements techniques nécessaires pour évaluer un incident de cybersécurité et pour déterminer la réponse technique à apporter. Le risque que cela se concrétise découle de l'obligation faite à l'opérateur désigné de signaler les incidents au Centre canadien pour la cybersécurité.

Nous devons toutefois reconnaître que, même si nous préciserons dans le Règlement le genre d'informations qu'un opérateur désigné devra fournir, lesquelles n'incluraient pas de renseignements personnels, leur inclusion reste toujours possible. Le commissaire au renseignement lui-même a déclaré publiquement que, lors de ses examens, il avait constaté des cas où les informations fournies comprenaient des renseignements personnels identifiables, des RPI; c'est là toute l'importance de trouver ce juste équilibre. Nous nous appuyons sur les mesures de sécurité existantes, soit l'application de la Loi sur la protection des renseignements personnels destinée à protéger les renseignements personnels, ainsi que la mise en œuvre de toutes les mesures de sécurité prévues dans la Loi sur le Centre de la sécurité des télécommunications.

For this reason as well, there is the notification to review agencies so that they are aware of when orders are issued, have the ability to review and so on.

**Mr. Arbour:** I'll just speak to the balance and then the offshore question.

I agree with my colleague that a very strong balance has been struck. I will actually step outside of the balance construct because, in my opinion, the threats we're seeing are by far the biggest risk to Canadian privacy. The ShinyHunters ransomware attack on AT&T resulted in the information of 105 million of their customers being accessed. BPFDoor, an attack in SK Telecom in Korea, affected the data of 27 million customers.

The attacks that we are dealing with here are, in my opinion, by far the biggest risk to Canadians' privacy. That said, I appreciate the questions about guardrails and ensuring that Canadian civil liberties are respected in this context. As a result of that feedback, a set of guardrails has been built into Bill C-8. It starts with the initial scoping. We're not talking about national security writ large, so this doesn't engage with law enforcement or investigations. It's about the protection of the critical infrastructure specifically.

For greater certainty language, that order-making power cannot be used to intercept personal communications and cannot be used to disrupt encryption. There has been a lot of commentary about whether this could be a lawful access bill. That was not the intent, and that further language underscores that lawful access is a separate bill and is not within the scope here. Then, on the handling of personal information, should it be accidentally or inadvertently submitted to us, there's an extra set of considerations and extra controls, over and above commercial information, to ensure that it is protected.

**The Chair:** Thank you.

**Senator Batters:** I have a point of clarification. I would like to let the officials know that I quoted the missing three paragraphs in their entirety in the second reading speech I gave in the Senate Chamber, so you can find them there.

**The Chair:** That brings us to the end of our time with you here today. Thanks for doing a double shift with our witnesses. We really appreciate that and appreciate you taking the time to meet with us.

C'est également pour cette raison qu'une notification est envoyée aux organismes chargés de l'examen, afin de les aviser de la production des ordonnances et qu'ils puissent les examiner, etc.

**M. Arbour :** Je vais simplement aborder la question de l'équilibre, puis celle du transfert de données à l'étranger.

Je partage l'avis de mon collègue selon lequel un équilibre très solide a été trouvé. Je vais toutefois m'écarter quelque peu de cette notion d'équilibre, car, à mon sens, les menaces auxquelles nous sommes confrontés constituent de loin le plus grand risque pour la vie privée des Canadiens. L'attaque par rançongiciel menée par ShinyHunters contre AT&T a permis à des pirates d'accéder aux données personnelles de 105 millions de clients de l'entreprise. Une attaque lancée contre SK Telecom en Corée à l'aide du logiciel malveillant BPFDoor a porté sur les données de 27 millions de clients.

J'estime que les attaques dont il est question ici constituent de loin le plus grand risque pour la vie privée des Canadiens. Cela dit, j'apprécie les questions concernant les garde-fous et la garantie du respect des libertés civiles des Canadiens dans ce contexte. À la suite de ces commentaires, une série de balises a été intégrée au projet de loi C-8. Cela commence dès la phase initiale de définition de la portée de la loi. Il ne s'agit pas ici de sécurité nationale au sens large, ce qui exclut donc les forces de l'ordre et les enquêtes menées. Il s'agit spécifiquement de la protection des infrastructures essentielles.

Je précise que ce pouvoir de prendre des ordonnances ne peut servir à intercepter des communications personnelles ni à contourner le chiffrement. Beaucoup se sont demandé si ce projet de loi pourrait porter sur l'accès légal. Or, ce n'était pas là l'intention visée, et cette précision souligne que l'accès légal fait l'objet d'un projet de loi distinct et ne correspond pas à la portée de cette mesure. Ensuite, en ce qui concerne le cas des données personnelles, si celles-ci devaient nous être transmises accidentellement ou par inadvertance, des considérations et des contrôles supplémentaires s'appliqueraient au-delà de ce qui est prévu pour les données commerciales, cela afin de garantir leur protection.

**La présidente :** Merci.

**La sénatrice Batters :** Je tiens à apporter une précision à nos fonctionnaires et leur signaler que j'ai cité intégralement les trois paragraphes manquants dans l'allocution que j'ai prononcée en deuxième lecture à la chambre du Sénat; vous pourrez donc les retrouver.

**La présidente :** Voilà qui met un terme à cette partie de la séance. Merci d'avoir contribué à ces deux passes de questions. Nous vous en sommes très reconnaissants et vous remercions d'avoir pris le temps de nous rencontrer.

For the next panel, we're very pleased to welcome the Honourable Simon Noël, K.C., Intelligence Commissioner, Office of the Intelligence Commissioner, who is accompanied by Justin Dubois, Executive Director and General Counsel. We also welcome Brendan Carley, Managing Director, Legislative Affairs and Strategic Relations Division, Office of the Superintendent of Financial Institutions. Also joining us, by video conference, are our friends from Canada Energy Regulator, Chris Finley, Director, Emergency Management & Security; and Robert Shepherd, Technical Specialist.

Thank you all for joining us here today. This work is very important. You can see we've had a variety of testimony today.

We will begin by inviting you to provide your opening remarks, to be followed by questions from our members. I remind you that you each have five minutes for your opening remarks.

[*Translation*]

**The Honourable Simon Noël, K.C., Intelligence Commissioner, Office of the Intelligence Commissioner:** Thank you, Madam Chair and honourable members, for the invitation. I am accompanied today by Justin Dubois, Executive Director and General Counsel at the Office of the Intelligence Commissioner.

As some of you may know, I appeared before this committee to discuss Bill C-26, the previous version of this bill. I remain of the view that Canada must have the necessary tools to protect our critical electronic systems, but that these tools must be accompanied by the appropriate safeguards and independent oversight. Bill C-8 is a useful tool, and I support its objectives. However, I am of the view that independent oversight would strengthen the bill.

[*English*]

One of my duties as Intelligence Commissioner, or IC, is to approve ministerial authorizations for cybersecurity activities. These authorizations grant CSE permission to access and collect information from IT systems belonging to non-federal entities that have been designated as being of importance to the federal government. An example in the public domain are the IT systems of the governments of Nunavut, the Northwest Territories and the Yukon.

The reason why my approval is necessary is that for CSE to be effective in carrying out cybersecurity activities on those systems, it will inevitably have to collect information around which Canadians have a reasonable expectation of privacy.

Nous avons maintenant le plaisir d'accueillir l'honorable Simon Noël, conseiller du Roi, commissaire au renseignement, qui est accompagné de Me Justin Dubois, directeur exécutif et avocat général. Nous accueillons aussi Brendan Carley, directeur général, Division des affaires législatives et des relations stratégiques, Bureau du surintendant des institutions financières et, par vidéoconférence, nos amis de la Régie de l'énergie du Canada, Chris Finley, directeur, Direction de la gestion des urgences et de la sécurité et Robert Shepherd, spécialiste technique.

Merci à vous tous de vous joindre à nous. Cette étude est très importante et vous aurez pu constater que nous avons déjà entendu toute une diversité de points de vue aujourd'hui.

Nous commencerons par vos propos liminaires avant de passer aux questions des sénateurs. Je vous rappelle que vous disposez chacun de 5 minutes pour vos remarques.

[*Français*]

**L'honorable Simon Noël, c.r., commissaire au renseignement, Bureau du commissaire au renseignement :** Madame la présidente et honorables sénateurs et sénatrices, je vous remercie de l'invitation à comparaître devant le comité. Je suis accompagné aujourd'hui de Me Justin Dubois, directeur exécutif et avocat général au Bureau du commissaire au renseignement.

Comme plusieurs d'entre vous le savent, j'ai comparu devant ce comité pour discuter du projet de loi C-26, la version précédente de ce projet de loi. Je demeure d'avis que le Canada doit disposer des outils nécessaires pour protéger nos systèmes électroniques essentiels, mais que ces outils doivent être accompagnés de mesures de protection appropriées et d'une surveillance indépendante. Le projet de loi C-8 est un outil utile et j'appuie ses objectifs. Cependant, je suis d'avis qu'une surveillance indépendante renforcerait le projet de loi.

[*Traduction*]

L'une de mes attributions de commissaire au renseignement, ou CR, consiste à approuver les autorisations ministérielles pour les activités de cybersécurité. Ces autorisations accordent au CST, le Centre de la sécurité des télécommunications, la permission d'accéder aux systèmes informatiques d'entités non fédérales désignées comme étant importantes pour le gouvernement fédéral et d'y puiser de l'information. Les systèmes informatiques des gouvernements du Nunavut, des Territoires du Nord-Ouest et du Yukon en sont un exemple dans le domaine public.

Mon approbation est nécessaire parce que, pour que le CST soit efficace dans l'exécution d'activités de cybersécurité sur ces systèmes, il doit inévitablement recueillir de l'information à l'égard de laquelle les Canadiens ont une attente raisonnable

Parliament was therefore of the view that oversight was required. Before approving cybersecurity activities, I must determine that they are reasonable and proportionate and that CSE has taken all appropriate measures to protect information in which Canadians may have a privacy interest.

[*Translation*]

Under this bill, regulations will set out what information designated operators will have to provide to the Communications Security Establishment, or CSE, if they are a victim of a cybersecurity incident. CSE is our cybersecurity expert. It is in our national interest for CSE to have a more complete understanding of cyber-incidents to respond more effectively. The information shared will have to be sufficient to provide CSE with a robust understanding of the incident.

[*English*]

In my experience as IC, even if CSE is only interested in receiving technical information to understand incidents, there may be cases where it must receive more than technical information. There may also be cases where technical information will touch on the privacy interests of Canadians. Indeed, CSE's recent written submissions to this committee confirm that data on cyber incidents can include information with a Canadian privacy interest.

For example, IP addresses can be indicators of compromise shared to better understand cybersecurity incidents, and the Supreme Court of Canada has confirmed that there can be privacy interests in IP addresses.

It's also important to remember that, under this proposed legislation, the reporting of cyber incidents will be mandatory.

Through CSE, the government would be collecting this information.

I think it is necessary to collect information relating to cybersecurity incidents. CSE should receive the information it needs to be effective. However, I remain unconvinced that regulation will guarantee that information shared following a cybersecurity incident will absolutely never engage the privacy interests of Canadians. If that's the case, the question for this committee is whether additional oversight is warranted.

You heard the answer of the Public Safety representative a few moments ago when he was talking about the regulations at the end.

en matière de vie privée. Le Parlement a donc estimé qu'une surveillance s'imposait. Avant d'approuver des activités de cybersécurité, je m'assure qu'elles sont raisonnables et proportionnelles, et que le CST dispose de mesures de protection appropriées pour protéger l'information dans laquelle les Canadiens peuvent avoir un intérêt en matière de vie privée.

[*Français*]

En vertu de ce projet de loi, des règlements préciseront quels renseignements les exploitants désignés devront fournir au Centre de la sécurité des télécommunications, le CST, s'ils sont victimes d'un incident de cybersécurité. Le CST est notre expert en cybersécurité. Il est dans l'intérêt national que le CST ait une compréhension plus complète des cyberincidents afin d'y répondre efficacement. Les renseignements partagés devront être suffisants pour lui donner cette compréhension.

[*Traduction*]

D'après mon expérience en tant que CR, même si le CST ne s'intéresse qu'aux renseignements techniques, il peut arriver qu'il doive recueillir plus que des renseignements techniques pour comprendre un incident de cybersécurité. Il peut également arriver que les renseignements techniques eux-mêmes touchent aux intérêts des Canadiens en matière de vie privée. En effet, dans ses observations écrites présentées à ce comité, le CST confirme que les données relatives aux cyberincidents peuvent inclure des renseignements comportant un intérêt pour la vie privée de Canadiens.

Par exemple, les adresses IP peuvent être des indicateurs de compromission partagés pour mieux comprendre les incidents de cybersécurité, et la Cour suprême du Canada a confirmé qu'il peut exister des intérêts en matière de vie privée à l'égard des adresses IP.

Il importe également de rappeler qu'en vertu du projet de loi proposé, la déclaration des cyberincidents sera obligatoire.

Par l'intermédiaire du CST, le gouvernement recueillerait ces renseignements.

Je considère qu'il est nécessaire de recueillir des renseignements relatifs aux incidents de cybersécurité. Le CST devrait recevoir les renseignements dont il a besoin pour être efficace. Cependant, je ne suis toujours pas convaincu qu'un règlement garantira que les renseignements communiqués à la suite d'un incident de cybersécurité ne toucheront absolument jamais aux intérêts en matière de vie privée. Si c'est le cas, la question pour ce comité est de savoir si une surveillance supplémentaire est justifiée.

Vous avez entendu la réponse du représentant de la Sécurité publique il y a quelques instants, quand il a évoqué la réglementation à la fin.

[*Translation*]

I would be happy to answer any questions.

[*English*]

**The Chair:** Thank you very much.

[*Translation*]

**Brendan Carley, Managing Director, Legislative Affairs and Strategic Relations Division, Office of the Superintendent of Financial Institutions:** Good evening, Madam Chair and honourable senators. Thank you for the opportunity to appear before you today as part of your study of Bill C-8.

[*English*]

I am pleased to provide the perspective of the Office of the Superintendent of Financial Institutions, or OSFI, the regulator of federally regulated financial institutions, including banks, which, as we have heard, comprise one of the vital services or systems contemplated under the proposed critical cyber systems protection act.

From OSFI's perspective, cyber risk is a prudential risk. More broadly, cyber-threats form part of a growing set of integrity and security risks that can affect operational resilience, erode public confidence and, if not well managed, have broader implications for an institution's financial resilience.

These risks are evolving quickly. They are increasingly sophisticated, often originate outside the financial system and can spread through third-party service providers, supply chains and interconnected digital infrastructure. This is why OSFI has steadily strengthened its supervisory focus in this area.

Cyber risk, integrity and security are prominent areas of focus in OSFI's Annual Risk Outlook publication, which we publish on our website. We have also established clear supervisory expectations through a number of important policy instruments.

This includes Guideline B-13 on technology and cyber risk management, which sets expectations for governance, technology resilience, cyber preparedness and incident recovery. It also includes Guideline B-10 on third-party risk management, which addresses risks arising from external service providers, including technology dependencies that may introduce operational vulnerabilities. In addition, OSFI's Integrity and Security Guideline reinforces expectations around safeguarding institutions against a broad range of evolving threats.

[*Français*]

Je serai heureux de répondre à vos questions.

[*Traduction*]

**La présidente :** Merci beaucoup.

[*Français*]

**Brendan Carley, directeur général, Division des affaires législatives et des relations stratégiques, Bureau du surintendant des institutions financières :** Bonsoir, madame la présidente et honorables sénatrices et sénateurs. Je vous remercie de votre invitation à comparaître aujourd'hui dans le cadre de votre étude du projet de loi C-8.

[*Traduction*]

Je suis heureux de vous présenter le point de vue du Bureau du surintendant des institutions financières, le BSIF, qui est l'organisme de réglementation des institutions financières fédérales, dont les banques font partie, qui forment l'un des secteurs des infrastructures essentielles visés par la Loi sur la protection des cybersystèmes essentiels proposée.

Le BSIF considère que le cyberrisque est de nature prudentielle. De façon plus générale, les cybermenaces font partie d'un ensemble croissant de risques liés à l'intégrité et à la sécurité qui peuvent miner la résilience opérationnelle, éroder la confiance du public et, s'ils ne sont pas gérés adéquatement, entraîner des conséquences plus vastes sur la résilience financière.

Ces risques évoluent rapidement. Ils gagnent en complexité, émanent souvent de l'extérieur du système financier et peuvent se propager par l'intermédiaire de tiers fournisseur de services, des chaînes d'approvisionnement et de l'infrastructure numérique interconnectée. C'est d'ailleurs pourquoi le BSIF a resserré sa surveillance à cet égard.

Le cyberrisque et les risques liés à l'intégrité et à la sécurité sont des axes importants dans notre Regard annuel sur le risque, qui est publié sur notre site Web. Nous avons également établi des attentes claires sur le plan de la surveillance, qui sont énoncées dans un certain nombre d'instruments de politique importants.

Il s'agit notamment de la ligne directrice B-13, Gestion du risque lié aux technologies et au cyberrisque, dans laquelle nous exposons nos attentes en matière de gouvernance, de résilience technologique, de préparation face aux cyberrisques et de reprise après un incident. Cela inclut également la ligne directrice B-10, Gestion du risque lié aux tiers, qui porte notamment sur les risques découlant du recours à des fournisseurs de services externes, y compris les dépendances technologiques qui peuvent introduire des vulnérabilités opérationnelles. Par ailleurs, la ligne directrice Intégrité et sécurité du BSIF renforce les attentes

[*Translation*]

OSFI also requires timely reporting of material cyber-incidents and works closely with federally regulated institutions to assess preparedness, strengthen resilience, and improve awareness of emerging threats. We actively collaborate with federal partners to strengthen collective situational awareness and support a coordinated approach to emerging cyber and other risks.

[*English*]

From OSFI's perspective, Bill C-8 would complement our existing regulatory and supervisory framework. In particular, its emphasis on cybersecurity programs, incident reporting, supply chain and third-party risk mitigation and coordination among regulators is broadly aligned with the direction OSFI has already taken in our supervisory and policy work.

Importantly, Bill C-8 maintains a sector-based approach that recognizes the role of existing regulators and supports proportionate, risk-based oversight. From OSFI's perspective, that alignment is important in reducing unnecessary duplication while reinforcing resilience across critical sectors.

Cybersecurity is not a static challenge, as we've discussed tonight. It requires ongoing vigilance, adaptation and close collaboration between regulated institutions, regulators and national security partners.

OSFI remains committed to doing its part to support a strong and resilient financial system in Canada.

[*Translation*]

Thank you. I would be pleased to answer your questions.

[*English*]

**The Chair:** Thank you.

**Chris Finley, Director, Emergency Management & Security, Canada Energy Regulator:** Good evening. My name is Chris Finley. I am the Director of Emergency Management & Security at the Canada Energy Regulator, or CER. I am joined today by Mr. Robert Shepherd, Technical Specialist, Security.

entourant la protection des institutions contre une vaste gamme de menaces qui ne cessent d'évoluer.

[*Français*]

De même, nous exigeons que les cyberincidents de taille soient signalés en temps opportun et nous travaillons en étroite collaboration avec les institutions financières fédérales pour évaluer leur état de préparation, accroître leur résilience et améliorer leurs connaissances sur les menaces émergentes. Nous collaborons aussi activement avec des partenaires fédéraux pour renforcer la conscience situationnelle collective et favoriser une approche coordonnée face aux cyberrisques et autres risques émergents.

[*Traduction*]

À nos yeux, le projet de loi C-8 serait complémentaire à notre cadre de réglementation et de surveillance. Plus particulièrement, son accent sur les programmes de cybersécurité, le signalement des incidents, l'atténuation des risques liés à la chaîne d'approvisionnement et aux tiers, et la coordination entre organismes de réglementation concorde, dans l'ensemble, à l'orientation que nous avons adoptée dans nos travaux de surveillance et d'élaboration de politiques.

Fait important, le projet de loi C-8 maintient une approche fondée sur le secteur qui tient compte du rôle des organismes de réglementation existants et qui favorise un encadrement fondé sur le risque et proportionnel. Selon nous, cet alignement est important pour réduire les chevauchements inutiles tout en renforçant la résilience dans l'ensemble des secteurs essentiels.

En matière de cybersécurité, on ne peut jamais se reposer sur ses lauriers. La cybersécurité requiert une vigilance constante, une adaptation et une collaboration étroite entre les institutions réglementées, les organismes de réglementation et les partenaires du milieu de la sécurité nationale.

Le BSIF est déterminé à participer aux efforts pour favoriser la résilience financière et la solidité du système financier canadien.

[*Français*]

Merci. Je serai maintenant heureux de répondre à vos questions.

[*Traduction*]

**La présidente :** Merci.

**Chris Finley, directeur, Gestion des urgences et sécurité, Régie de l'énergie du Canada :** Bonsoir, je m'appelle Chris Finley. Je suis le directeur de la gestion des urgences et de la sûreté à la Régie de l'énergie du Canada, plus simplement la Régie. Je suis accompagné de Robert Shepherd, spécialiste technique de la sûreté.

Thank you for inviting the Canada Energy Regulator to appear before the committee today to discuss Bill C-8.

Before going further, I want to acknowledge that I am appearing before you today from Calgary, Alberta, located within Treaty 7 territory, the traditional territories of the Blackfoot Confederacy, which includes the Siksika, Piikani and Kainai First Nations. Treaty 7 is also home to the Tsuut'ina First Nation and the Stoney Nakoda, including the Chiniki, Bearspaw and Goodstoney Nations. I would also like to recognize the Métis who have settled in Southern Alberta and call this place home.

I would like to give you an overview of the CER's mandate. We work to regulate infrastructure to ensure the safe and efficient delivery of energy across the country.

The CER regulates pipelines, power lines, energy resource development and energy trade on behalf of Canadians, with a view to protecting the public and the environment while promoting market efficiency.

Safety is at the core of our work. We regulate to prevent harm in all forms, and this includes cybersecurity threats. The CER takes the matter of cybersecurity threats to Canada's energy infrastructure seriously.

The CER oversees roughly 71,000 kilometres of oil and gas pipelines in Canada. We regulate pipelines that cross provincial boundaries or the Canada-U.S. border. CER-regulated companies are required to have proactive measures in place to protect this critical infrastructure from cybersecurity threats.

Under the CER's Onshore Pipeline Regulations, regulated companies must have a security management program that anticipates, prevents, manages and mitigates conditions that could adversely affect people, property or the environment. In addition to physical threats to infrastructure, companies must consider cybersecurity threats in their security management program and implement appropriate mitigation based on the results of a security risk assessment process. These requirements are laid out in the Canadian Standards Association's Z246.1 standard, which is included in the Onshore Pipeline Regulations by reference. Cybersecurity measures must reflect the criticality of cyber assets, as well as the results of regular assessments of threats, vulnerabilities and overall security risk.

Je vous remercie d'avoir invité la Régie de l'énergie du Canada à comparaître devant votre comité pour discuter du projet de loi C-8.

Je tiens d'abord à souligner que je me trouve à Calgary, en Alberta, ville située sur des terres visées par le Traité nº 7 qui font partie du territoire traditionnel de la Confédération des Pieds-Noirs comprenant les Premières Nations Siksika, Piikani et Kainai. Ce traité concerne aussi les Premières Nations Tsuu T'ina et Stoney Nakoda, regroupant les Premières Nations Chiniki, Bearspaw et Goodstoney. Je tiens également à rendre hommage aux Métis qui se sont établis dans le sud de l'Alberta et y ont élu domicile.

Je commencerai par vous donner un aperçu du mandat de la Régie qui est de réglementer les infrastructures énergétiques pour assurer l'acheminement sécuritaire et efficace de l'énergie au Canada.

La Régie réglemente les pipelines, les lignes de transport d'électricité, le développement des ressources énergétiques et le commerce de l'énergie au nom des Canadiens, afin de protéger le public et l'environnement tout en favorisant l'efficience des marchés énergétiques.

La sécurité est au cœur de notre mandat qui consiste à réglementer pour prévenir toutes sortes de dommages, notamment les menaces à la cybersécurité. La Régie prend au sérieux les menaces à la cybersécurité des infrastructures énergétiques du Canada.

Nous supervisons quelque 71 000 kilomètres d'oléoducs et de gazoducs. Nous réglementons les pipelines transprovinciaux ou qui franchissent la frontière canado-américaine. Les sociétés pipelinières que nous réglementons doivent se doter de mesures proactives pour protéger ces infrastructures essentielles contre les menaces à la cybersécurité.

En vertu du Règlement de la Régie sur les pipelines terrestres, les sociétés réglementées doivent disposer d'un programme de gestion de la sûreté apte à prévoir, prévenir, gérer et atténuer les conditions susceptibles d'avoir une incidence sur les personnes, les biens ou l'environnement. Dans ce programme, les sociétés doivent tenir compte des menaces physiques aux infrastructures et à la cybersécurité, et mettre en œuvre des mesures d'atténuation appropriées en fonction des résultats d'un processus d'évaluation des risques. Ces exigences sont énoncées dans la norme de l'Association canadienne de normalisation Z246.1, laquelle est incorporée par renvoi dans le Règlement sur les pipelines terrestres. Les mesures en matière de cybersécurité doivent tenir compte de la criticité des actifs informatiques, ainsi que des résultats des évaluations périodiques des menaces, des vulnérabilités et du risque global pour la sécurité.

The regulation of electricity generation, transmission and distribution rests primarily within the jurisdiction of provinces and territories. However, the CER regulates approximately 1,500 kilometres of international power lines.

The Canadian public rightfully expects us to hold the pipeline and international power line companies we regulate accountable for the safe operation of CER-regulated energy infrastructure.

The CER is well positioned to administer the obligations of Bill C-8 that apply to the companies we regulate, particularly given how these obligations complement those already found in the Canadian Energy Regulator Act. For example, the bill provides the CER with the ability to issue orders and to take necessary enforcement actions to bring a company back into compliance so that critical cyber systems are protected.

The CER already uses similar tools. For example, the CER issues notices of non-compliance, inspector orders and administrative monetary penalties, as necessary, to bring companies into compliance and ensure their safe operation.

The CER also verifies that companies are complying with requirements through inspections, audits, compliance meetings and emergency response and security exercises.

We work with federal, territorial, provincial and international agencies, as well as regulated industry, to ensure that proactive measures are taken to protect federally regulated energy infrastructure from cyber-related risks or attacks.

In closing, thank you for the opportunity to speak with you today about this important issue. We look forward to your questions.

**The Chair:** Thank you. We will now proceed to our questions this evening. Our guests will be with us until about seven o'clock. As always, we will do our best to allow each member to ask their questions. Also, four minutes will continue to be allotted for each question.

I ask that you keep questions as succinct and tight as possible. I'm going to offer the first question to our deputy chair.

**Senator Al Zaibak:** I thank you all for being here today.

La réglementation de la production, du transport et de la distribution d'électricité relève principalement des provinces et des territoires, mais la Régie réglemente environ 1 500 kilomètres de lignes internationales de transport d'électricité.

La population canadienne s'attend à juste titre à ce que la Régie tienne les sociétés pipelinières et les sociétés exploitant des lignes internationales de transport d'électricité responsables de la réglementation responsable de l'exploitation sécuritaire des infrastructures énergétiques relevant de son ressort.

La Régie est bien placée pour veiller à l'application des obligations prévues dans le projet de loi C-8 qui visent les sociétés qu'elle réglemente, d'autant plus que ces obligations viennent compléter celles déjà prévues dans la Loi sur la Régie canadienne de l'énergie. Par exemple, le projet de loi donne à la Régie la capacité de rendre des ordonnances et de prendre les mesures d'exécution nécessaires pour obliger les sociétés à se conformer, afin d'assurer la protection des cybersystèmes essentiels.

La Régie utilise déjà des outils similaires. Par exemple, elle délivre des avis de non-conformité et des ordonnances d'inspecteur et impose des sanctions administratives pécuniaires, au besoin, pour amener les sociétés à se conformer et assurer l'exploitation sécuritaire de leurs installations.

La Régie vérifie également que les sociétés se conforment aux exigences au moyen d'inspections, d'audits, de réunions sur la conformité et d'exercices d'intervention d'urgence et de sécurité.

Nous travaillons avec des organismes fédéraux, territoriaux, provinciaux et internationaux, ainsi qu'avec l'industrie réglementée, pour nous assurer que des mesures proactives sont prises pour protéger les infrastructures énergétiques de ressort fédéral contre les cyberrisques ou les cyberattaques.

Pour conclure, nous tenons à vous remercier de nous avoir donné l'occasion de vous parler de cet enjeu important et c'est avec plaisir que nous répondrons à vos questions.

**La présidente :** Merci. Nous allons maintenant passer aux questions. Nos invités resteront parmi nous jusqu'à environ 19 heures. Comme toujours, nous ferons de notre mieux pour permettre à chacun de poser ses questions. Par ailleurs, quatre minutes continueront d'être allouées pour chaque question.

Veuillez formuler vos questions de la manière la plus concise et la plus précise possible. Je vais donner la parole à notre vice-président pour la première question.

**Le sénateur Al Zaibak :** Je vous remercie tous d'être ici aujourd'hui.

Commissioner Noël, thank you for your opening remarks. From your opening statement, I'm wondering whether you are counting on this committee to make amendments to further improve the bill. If so, do you have any recommendations or submissions for us to consider?

**Mr. Noël:** Yes. Thank you for your kind comments.

My jurisdiction triggers when a minister makes a decision to permit CSE to, for instance, assume certain activities in order to protect Canadians. Then, my duty is to ensure that the activities occurring will not negatively impact Canadian data and information on Canadians.

The recommendation I have to this committee is simple: The Minister of Public Safety should annually grant authorization to CSE to do its work under this bill, which would become law, and that authorization the minister would grant would list whatever has to be done and related concerns. My duty, then, would be to review that decision once it is signed.

So, it's twofold: Is it in line with what the legislation wanted? Second, and most importantly, are the policies of CSE sufficient to protect the Canadian data that will be collected? If they do collect information, how long are they going to keep it and for what purpose? It would also be my part to make sure that if that information is not useful, then it should be destroyed.

It would be like in other legislation — like the CSE Act. The minister should grant an authorization, which will be reviewed by the Intelligence Commissioner on a yearly basis. It's not a big burden; it's on a yearly basis. Then I would issue a decision that would explain whatever has to be done or, if an error has been committed, to flag it out. That what would be my suggestion.

**Senator Al Zaibak:** Thank you so much.

Are you also considering or suggesting more parliamentary oversight?

**Mr. Noël:** NSICOP already provides oversight from members of Parliament. That exists already.

The difference with the position of the Intelligence Commissioner is the following: NSICOP, the parliamentary committee, reviews things once the activities have occurred, and I come in before the activities begin. It's an assurance that is given to the Canadian public that a third party has looked into the situation and has given its blessing or decided that the activity should be done differently.

Monsieur le commissaire Noël, merci pour vos observations liminaires. À la lumière de celles-ci, je me demande si vous comptez sur ce comité pour proposer des amendements visant à améliorer davantage le projet de loi. Si tel est le cas, auriez-vous des recommandations ou des propositions à nous soumettre?

**M. Noël :** Oui. Merci pour vos aimables commentaires.

L'entité que je représente intervient lorsque, par exemple, un ministre prend la décision d'autoriser le Centre de la sécurité des télécommunications à mener certaines activités dans le but de protéger les Canadiens. Il m'incombe alors de veiller à ce que ces activités n'aient pas d'incidence négative sur les données canadiennes ni sur les informations concernant les Canadiens.

Ma recommandation à ce comité est simple : le ministre de la Sécurité publique devrait accorder chaque année au CST l'autorisation de bien faire son travail dans le cadre de ce projet de loi, s'il est adopté, et cette autorisation énoncerait les mesures à prendre ainsi que les préoccupations qui s'y rapportent. Il m'incomberait alors d'examiner cette décision une fois qu'elle aurait été prise.

Il y aurait donc deux aspects à examiner. Tout d'abord, l'esprit de la loi est-il respecté? Deuxièmement, et surtout, les politiques du CST sont-elles suffisantes pour protéger les données qui seront recueillies? Si de l'information est effectivement recueillie, combien de temps sera-t-elle conservée et dans quel but? Il m'incomberait également de veiller à ce que cette information soit détruite si elle ne s'avère pas utile.

Ce serait comme dans d'autres textes législatifs — par exemple la Loi sur le Centre de la sécurité des télécommunications. Le ministre devrait délivrer une autorisation, qui serait évaluée chaque année par le commissaire au renseignement. Étant donné que cela se ferait une fois par an, ce ne serait pas un fardeau important. Je rendrais ensuite une décision pour expliquer les mesures à prendre ou, dans le cas où une erreur aurait été commise, pour la signaler. Voilà ce que je proposerais.

**Le sénateur Al Zaibak :** Merci beaucoup.

Envisagez-vous ou proposez-vous également de renforcer la surveillance parlementaire?

**M. Noël :** Le Comité des parlementaires sur la sécurité nationale et le renseignement prévoit déjà une surveillance assurée par les députés. Ce contrôle existe déjà.

La différence par rapport au rôle du commissaire au renseignement est la suivante : le CPSNR, le comité parlementaire, évalue les faits une fois que les activités ont eu lieu, tandis que j'interviens avant même qu'elles ne commencent. C'est une garantie donnée au public canadien qu'un tiers a évalué la situation et a donné son aval ou a décidé que l'activité devrait être menée différemment.

**Senator Al Zaibak:** Thank you so much.

**Senator Cardozo:** First, to carry on with that conversation, Mr. Noël, your role is to oversee national security and intelligence activities that are planned by the Communications Security Establishment and CSIS. Does this bill help or otherwise affect your mandate?

**Mr. Noël:** I'm completely absent; I'm not involved. If you compare that to the cyber activity that the Canadian Centre for Cyber Security is authorized to do, it follows the decision of the Minister of National Defence, which I have reviewed. In this case, if you look at the documents of CSE that were filed — just for reference purposes, I'm looking at page 7, the top paragraph — it's only a review that will be done. The type of job that I'm doing is not at all part of that process under this bill.

**Senator Cardozo:** Okay, thank you.

Mr. Carley, I'm paraphrasing, but you said something to the effect of this bill adding to a security framework that you currently have; correct me if I have quoted you wrong. What are the other acts that define your security framework?

**Mr. Carley:** Thank you for the question.

We are founded through legislation called the Office of the Superintendent of Financial Institutions Act that sets out the superintendent, the mandate of the office and our powers. We also administer financial institution statutes, like the Bank Act, the Insurance Companies Act, the Trust and Loan Companies Act — a number of statutes under the responsibility of the Minister of Finance. We would be added under this bill as one of the regulators for the designated operators in the banking sector.

**Senator Cardozo:** Are there other existing cybersecurity policies that affect your mandate?

**Mr. Carley:** In terms of our risk mandate around looking to assess and help improve the prudential health, security and integrity of federal financial institutions in Canada, we have broad authority to develop risk-management guidance that we, then, expect our regulating institutions to follow. That includes things like cyber and operational resilience and third-party risk management that then comes back to how they effectively manage the risks of operating as financial institutions and maintaining the trust of Canadians.

**Le sénateur Al Zaibak :** Merci beaucoup.

**Le sénateur Cardozo :** Tout d'abord, pour poursuivre cette discussion, monsieur Noël, votre rôle consiste à superviser les activités liées à la sécurité nationale et au renseignement qui sont planifiées par le Centre de la sécurité des télécommunications et le SCRS. Ce projet de loi facilite-t-il l'exercice de votre mandat ou a-t-il une incidence sur celui-ci?

**M. Noël :** Cela ne me touche pas du tout; je ne suis pas impliqué. En comparaison avec les cyberactivités que le Centre canadien pour la cybersécurité est autorisé à mener, elles relèvent d'une décision du ministre de la Défense nationale, que j'ai examinée. Dans ce cas précis, si vous consultez les documents du CST qui ont été déposés — à titre de référence, je me réfère à la page 7, premier paragraphe, du document anglais —, il s'agit uniquement d'un examen qui serait effectué. Mon travail ne fait absolument pas partie de ce processus prévu dans le projet de loi.

**Le sénateur Cardozo :** D'accord, merci.

Monsieur Carley, je paraphrase, mais vous avez dit en substance que ce projet de loi venait compléter le cadre de sécurité dont vous disposez actuellement. Corrigez-moi si je me trompe. Quelles sont les autres lois qui définissent votre cadre de sécurité?

**M. Carley :** Merci pour votre question.

Notre organisme a été créé en vertu de la Loi sur le Bureau du surintendant des institutions financières, qui définit le poste de surintendant, le mandat du bureau et nos pouvoirs. Nous assurons également l'application des lois régissant les institutions financières, comme la Loi sur les banques, la Loi sur les sociétés d'assurances et la Loi sur les sociétés de fiducie et de prêt — plusieurs textes législatifs qui relèvent de la compétence du ministre des Finances. En vertu de ce projet de loi, nous serions désignés comme l'un des responsables de la réglementation des exploitants désignés du secteur bancaire.

**Le sénateur Cardozo :** Existe-t-il d'autres politiques en matière de cybersécurité qui ont une incidence sur votre mandat?

**M. Carley :** Dans le cadre de notre mandat en matière de risques, qui consiste à évaluer et à contribuer à améliorer l'efficacité prudentielle, la sécurité et l'intégrité des institutions financières fédérales au Canada, nous disposons de larges pouvoirs pour élaborer des lignes directrices en matière de gestion des risques. Nous nous attendons ensuite de nos institutions réglementées qu'elles les respectent. Cela inclut notamment la résilience cybernétique et opérationnelle ainsi que la gestion des risques liés aux tiers, ce qui revient en fin de compte à déterminer comment elles gèrent efficacement les risques liés à leurs activités en tant qu'institutions financières et comment elles préservent la confiance des Canadiens.

We look at some international best practices, and there are a number of regulatory colleges in which OSFI participates globally, that will inform some of our risk-management expectations and approaches, but we don't have specific legislative cyber frameworks that we follow.

**Senator Cardozo:** Okay, thank you.

**Senator Batters:** Thanks very much to all of you for being here. My questions will focus on the Intelligence Commissioner, Mr. Noël.

While Bill C-8 has been improved somewhat, mainly by House of Commons amendments, as compared to Bill C-26, one area remains a glaring omission, which is oversight — pre-authorization for the kinds of orders the law allows. There is virtually none in this bill. In fact, Bill C-8 specifically bypasses, as you indicated, the Intelligence Commissioner, even though your oversight is required in similar order-making contexts.

I understand that the government's decision to bypass the Intelligence Commissioner is also at odds with a recent update report on developments in data protection in which Canada specifically trumpeted your office as a vital oversight actor, which it obviously is, but it's shocking that it's not being used here.

Please tell us more. You certainly got into this with Senator Al Zaibak in the opening exchange, but please tell us a little bit more why you think oversight and pre-authorization are so critical for this act.

**Mr. Noël:** The position I'm in is the following: I view the decision of the minister and the activities that he grants or permits the agencies to actualize.

I've been doing this for the past four years. I can tell you that my experience is such that two or three times I decided that some of the activities that the minister wanted to grant were not to be. Why did I do that? I had viewed the jurisdiction as it was granted, Senator Batters, and came to the conclusion that what the agency wanted to do was not in conformity with the jurisdiction. Therefore, this activity did not occur.

Let me go a little bit further. What did it do? They came back. They tried to improve, and they did in some cases. As recently as this year, they did. That's justice one example. That's for the cybersecurity aspect.

Nous nous inspirons de certaines pratiques internationales éprouvées, et le BSIF participe à plusieurs forums de réglementation à l'échelle mondiale, qui nous aident à définir certaines de nos attentes et approches en matière de gestion des risques. Toutefois, nous ne disposons pas de cadres législatifs spécifiques en matière de cybersécurité auxquels nous sommes assujettis.

**Le sénateur Cardozo :** D'accord, merci.

**La sénatrice Batters :** Je vous remercie tous infiniment d'être ici. Mes questions s'adressent au commissaire au renseignement, M. Noël.

Si le projet de loi C-8 a été quelque peu amélioré par rapport au projet de loi C-26, principalement grâce aux amendements apportés par la Chambre des communes, il subsiste toutefois une lacune flagrante en matière de surveillance : l'autorisation préalable pour les types de décrets autorisés par la loi. Ce projet de loi n'en prévoit pratiquement aucune. En effet, comme vous l'avez souligné, le projet de loi C-8 laisse totalement de côté le commissaire au renseignement, alors même que votre surveillance est requise dans des contextes similaires de délivrance de décrets.

Sauf erreur, la décision du gouvernement de passer outre au commissaire au renseignement va également à l'encontre d'un récent rapport faisant le point sur les développements en matière de protection des données, dans lequel le Canada présentait précisément votre bureau comme un acteur essentiel de la surveillance, ce qu'il est manifestement, mais il est choquant de constater qu'il n'est pas mis à contribution dans ce cas précis.

Pourriez-vous nous en dire davantage à ce sujet? Vous avez déjà abordé la question avec le sénateur Al Zaibak au début de la séance, mais pourriez-vous nous expliquer un peu plus en détail pourquoi vous estimez que la supervision et l'autorisation préalable sont si essentielles pour cette loi?

**M. Noël :** Ma position est la suivante : j'examine la décision du ministre ainsi que les mesures qu'il autorise ou permet aux agences de mettre en œuvre.

Je m'occupe de cela depuis quatre ans. Je peux vous dire que, dans le cadre de mes fonctions, il m'est arrivé à deux ou trois reprises de décider que certaines des activités que le ministre souhaitait autoriser ne devaient pas avoir lieu. Pourquoi ai-je agi ainsi? J'avais examiné les pouvoirs qui avaient été définis, sénatrice Batters, et j'étais arrivé à la conclusion que ce que l'organisme souhaitait faire n'était pas conforme à ces pouvoirs. Les activités en question n'ont donc pas eu lieu.

Permettez-moi d'aller un peu plus loin. Qu'est-ce que cela a donné? Ils sont revenus à la charge. Ils ont essayé de s'améliorer, et ils y sont parvenus dans certains cas. C'est encore ce qui se produit cette année. Voilà pour l'aspect de la cybersécurité.

If I look at CSIS now, we're not talking about cybersecurity, but it will provide a good example. CSIS operates in the field with human sources, and the human sources get their direction from their handler. My position is to follow up on the Minister of Public Safety's decision, which is to permit the activities, and I look at whether there are categories of activities that can be actualized. Again, Senator Batters, on two occasions, I denied some of the activities. They would have been illegal and gone against the legislation.

Let me go further. The big concern for all Canadians is our information, be it our data, our bank information or our medical information. We are misers of our information. When I approach a decision in which I'm involved, I'm a miser in my decision, but by being so, I'm a miser for all Canadians. If you want to impact the personal information of Canadians, you must justify doing so. It compels the decision maker or the agency to really ask, "Can we do this? Are we doing it in accordance with the law?"

**Senator Batters:** Thank you.

**Senator McNair:** Commissioner Noël, thank you for the work that you have done over the past four years and for your testimony on Bill C-26 and again on Bill C-8. You mentioned in your comments it's not onerous, what you're suggesting, and is only on a yearly basis. Can you expand on that and explain that for me? I thought we were talking about prior to the order.

**Mr. Noël:** Yes, the decisions that I review are decisions that regard cybersecurity and are good for a period of one year. They have to come back a year later and ask the minister to continue. I review the decisions then.

**Justin Dubois, Executive Director and General Counsel, Office of the Intelligence Commissioner:** What the Intelligence Commissioner is proposing would be in the sense of a yearly authorization regarding how information from a cyber incident is handled by CSE. It wouldn't be every single cyber incident getting pre-approval. It would be a framework for how that information is handled, and then that framework would be reviewed on an annual basis by the Intelligence Commissioner after being authorized by the minister.

**Senator McNair:** In accordance with the act at the time or the bill right now.

Si je prends l'exemple du SCRS, il ne s'agit pas ici de cybersécurité, mais cela illustre bien mon propos. Le SCRS mène des opérations sur le terrain en s'appuyant sur des sources humaines, et ces dernières reçoivent leurs instructions de leur gestionnaire de sources. Mon rôle consiste à donner suite à la décision du ministre de la Sécurité publique, qui est d'autoriser ces activités, et j'examine s'il existe des catégories d'activités qui peuvent être mises en œuvre. Encore une fois, sénatrice Batters, à deux reprises, j'ai refusé certaines de ces activités. Elles auraient été illégales et contraires à la loi.

Permettez-moi d'aller plus loin. La grande préoccupation de tous les Canadiens concerne nos informations, qu'il s'agisse de nos données, de nos informations bancaires ou de nos dossiers médicaux. Nous protégeons avec rigueur nos informations. Lorsque je dois prendre une décision dans ma sphère d'activité, je fais preuve de prudence, mais ce faisant, j'agis dans l'intérêt de tous les Canadiens. Ceux qui souhaitent accéder aux informations personnelles des Canadiens doivent être justifiés de le faire. Cela oblige le décideur ou l'organisme à se demander sérieusement : « Pouvons-nous faire cela? Agissons-nous conformément à la loi? »

**La sénatrice Batters :** Merci.

**Le sénateur McNair :** Monsieur le commissaire Noël, je vous remercie pour le travail que vous avez accompli au cours des quatre dernières années et pour votre témoignage concernant le projet de loi C-26, puis le projet de loi C-8. Vous avez indiqué dans vos observations que ce que vous proposez n'impose pas un trop grand fardeau et ne s'applique qu'à une fréquence annuelle. Pourriez-vous développer ce point et m'expliquer cela plus en détail? Je croyais que nous parlions de la période antérieure au décret.

**M. Noël :** Oui, les décisions que j'examine concernent la cybersécurité et sont valables pour une durée d'un an. Les demandeurs doivent revenir un an plus tard et demander au ministre de prolonger cette autorisation. C'est à ce moment-là que j'examine à nouveau ces décisions.

**Justin Dubois, directeur exécutif et avocat général, Bureau du commissaire au renseignement :** Ce que propose le commissaire au renseignement s'apparenterait à une autorisation annuelle concernant la manière dont le CST traite les informations issues d'un cyberincident. Il ne s'agirait pas d'obtenir une autorisation préalable pour chacun de ces incidents. Il s'agirait plutôt d'un cadre régissant le traitement de cette information, lequel serait ensuite examiné chaque année par le commissaire au renseignement, après avoir été autorisé par le ministre.

**Le sénateur McNair :** Conformément à la loi en vigueur à ce moment-là ou au projet de loi actuel.

I'm sure Commissioner Noël is aware, and the other panellists probably are as well, that there were a number of amendments to the bill at the House of Commons committee that I think strengthened the bill. They were primarily around privacy safeguards and the applicability of the Privacy Act. Safeguards in the CSE Act continue to apply, regardless, and also put guardrails around the order-making power of the minister and cabinet.

We heard one of the officials from the second panel say that what keeps him up at night is the lack of authority to take action against cybersecurity threats currently without the legislation in place. He also said that the biggest threats to Canadian privacy are the cybersecurity incidents occurring on an ongoing basis.

In light of the changes that have been made, do you think the bill strikes the right balance at this stage? Mr. Carley, I'm curious to know if you would pass the legislation now or continue to work on improving it.

**Mr. Carley:** Thank you for the question. From OSFI's perspective, we will be a responsible regulator under the act. We think that there are benefits to the legislation moving forward, and we support it. It will provide additional last-resort powers, as Public Safety officials have spoken about, in terms of our ability to compel reporting and administer penalties if the legislation isn't respected.

These are next steps beyond what we already do and the general approaches that we take as the federal financial institutions regulator. We do, though, see some additional benefits in terms of the required reporting to the Cyber Centre under CSE. We think the information flowing more broadly — coming across from different critical sectors, enabling a better identification of risks and a better view of the threat landscape — will then assist critical service providers in different industries to then, as we talked about, harden their attack surfaces and be more resilient to the risks. We can't control those risks. It's about how you prepare and mitigate the risk threats to institutions.

So, we support the legislation and remain ready to administer our responsibilities under it.

**Senator McNair:** Thank you.

Je suis certain que le commissaire Noël est conscient, tout comme les autres intervenants sans doute, qu'un certain nombre d'amendements ont été apportés au projet de loi au sein du comité de la Chambre des communes, amendements qui, à mon sens, l'ont renforcé. Ils portaient principalement sur les garanties en matière de protection de la vie privée et sur la pertinence d'appliquer la Loi sur la protection des renseignements personnels. Les garanties prévues par la Loi sur le CST continuent de s'appliquer dans tous les cas, et elles encadrent également le pouvoir du ministre et du Cabinet de prendre des décrets.

Nous avons entendu un des représentants du deuxième groupe de témoins déclarer que ce qui l'empêchait de dormir, c'était le manque de pouvoirs pour agir contre les cybermenaces en l'absence de dispositions législatives. Il a également indiqué que les principales menaces pesant sur la vie privée des Canadiens étaient les cyberincidents courants.

Compte tenu des modifications qui ont été apportées, pensez-vous que le projet de loi comporte un juste équilibre à ce stade? Monsieur Carley, je serais curieux de savoir si vous adopteriez le texte tel quel ou si vous continueriez à travailler à son amélioration.

**M. Carley :** Merci pour cette question. Pour ce qui est du BSIF, nous assurerons la réglementation de façon responsable conformément à la loi. Nous estimons que ces dispositions législatives présentent des avantages pour l'avenir et nous les soutenons. Cela nous conférera des pouvoirs supplémentaires de dernier recours, comme l'ont mentionné les responsables de la Sécurité publique, notamment en ce qui concerne notre capacité à exiger la déclaration d'information et à infliger des sanctions en cas de non-respect de la loi.

Ce sont des mesures qui vont au-delà de ce que nous faisons déjà et des approches générales que nous adoptons en tant que responsable fédéral de la réglementation des institutions financières. Nous voyons toutefois certains avantages supplémentaires en ce qui concerne les obligations de déclaration auprès du Centre pour la cybersécurité relevant du CST. Nous pensons que la diffusion plus large de l'information provenant de différents secteurs critiques et permettant une meilleure identification des risques, ainsi qu'une meilleure vision du contexte des menaces, aidera les fournisseurs de services essentiels dans différents secteurs à renforcer leur surface d'attaque et à être plus résilients face aux risques. Nous ne pouvons pas contrôler ces risques. Il s'agit de savoir comment se préparer et atténuer les menaces qui pèsent sur les institutions.

Nous soutenons donc cette législation et restons prêts à assumer les responsabilités qui nous incombent en vertu de celle-ci.

**Le sénateur McNair :** Merci.

**Senator Ince:** My question is for Mr. Noël. Do the limits in Bill C-8 clearly prevent information collected for cybersecurity from later being used for intelligence purposes beyond what Parliament intended?

**Mr. Noël:** It all depends on how the Cyber Centre deals with that information. The Cyber Centre has its own policies and timetable as to how long they can keep information. I can assure you that I've been following that very closely. The policies are the best they can be at this time.

What the future can tell — cyberattacks change drastically. The modes of operation change. They can capture medical information. They can capture bank data. They can capture a list of electors in a province and decide to do something with it.

It's hard for me to answer this question. I'm doing my best. The tools are there, but what is really missing is having somebody that looks over the shoulder and says, "Have you done your job correctly?" In fairness, I should say that NSIRA, the national security agency that reviews, comes post facto. They may see something, but that will be one, two or three years down the road.

**Senator Kutcher:** Thank you very much to my colleagues for ceding me their time.

My questions are to Mr. Finley and then to Commissioner Noël.

First, Mr. Finley, are there areas in this bill that you would improve or you suggest we look at improving?

And then, Commissioner Noël, is there legislation in other states and other jurisdictions that you think captures the issue that you are raising? If so, which jurisdictions what types of legislation is it?

**Mr. Finley:** Thank you for the question. Under the Canada Energy Regulator, we have fairly robust oversight currently with the Canadian Energy Regulator Act, the Onshore Pipeline Regulations and CSA standard Z246.1. We anticipate that Bill C-8 will increase and enhance what we already have in terms of the requirements for the cybersecurity program, supply chain considerations and especially on the incident reporting side, to inform the Cyber Centre of what's happening in our industry and also be able to receive that information ourselves — to determine how we would implement the information that comes back in terms of our compliance oversight.

**Le sénateur Ince :** Ma question s'adresse à M. Noël. Les limites prévues dans le projet de loi C-8 empêchent-elles clairement que l'information recueillie à des fins de cybersécurité soit par la suite utilisée à des fins de renseignement, au-delà de ce que le Parlement a prévu?

**M. Noël :** Tout dépend de la manière dont le Centre pour la cybersécurité traite cette information. Il dispose de ses propres politiques et d'un calendrier précisant la durée pendant laquelle il peut conserver l'information. Je peux vous assurer que je suis cette question de très près. Ces politiques sont les meilleures possible à l'heure actuelle.

Ce que l'avenir peut nous apprendre, c'est que les cyberattaques évoluent radicalement. Les modes d'opération changent. Ils peuvent permettre de s'emparer d'informations médicales. Ils peuvent permettre de mettre la main sur des données bancaires ou de s'emparer d'une liste d'électeurs d'une province et de décider de l'utiliser à une fin quelconque.

Il m'est difficile de répondre à cette question. Je fais de mon mieux. Les outils sont là, mais ce qui manque vraiment, c'est une deuxième instance qui vérifie si le travail a été fait correctement. Pour être juste, je dois dire que l'Office de surveillance des activités en matière de sécurité nationale et de renseignement intervient a posteriori. Il se peut qu'il remarque quelque chose, mais ce sera un, deux ou trois ans plus tard.

**Le sénateur Kutcher :** Je remercie sincèrement mes collègues de m'avoir cédé leur temps de parole.

Mes questions s'adressent à M. Finley, puis au commissaire Noël.

Tout d'abord, M. Finley, y a-t-il des aspects de ce projet de loi que vous amélioreriez ou sur lesquels nous devrions nous pencher, selon vous?

Ensuite, monsieur le commissaire Noël, existe-t-il dans d'autres États ou secteurs de compétence des lois que vous considérez pertinentes dans le contexte de ce que vous soulevez? Si oui, de quels secteurs de compétence et de quel type de dispositions législatives s'agit-il?

**M. Finley :** Merci pour la question. Sous l'égide de la Régie de l'énergie du Canada, nous disposons présentement d'une surveillance assez robuste, grâce à la Loi sur la Régie de l'énergie du Canada, au Règlement sur les pipelines terrestres et à la norme CSA Z246.1. Nous prévoyons que le projet de loi C-8 augmentera et améliorera nos exigences concernant le programme de cybersécurité, les considérations liées à la chaîne d'approvisionnement et, surtout, le signalement des incidents, pour que le Centre pour la cybersécurité soit informé de ce qui se passe dans notre industrie, et pour que nous recevions cette information nous-mêmes, afin de déterminer comment nous la mettrons en œuvre dans le cadre de notre surveillance de la conformité.

At this point, there is nothing that would be lacking from our perspective. We think that it's fairly comprehensive and should supplement what we already have in place as a regulator. Thank you.

**Mr. Noël:** The position of the Intelligence Commissioner is really a Canadian product, and it's hard to see what other countries would be doing under circumstances like this.

Let me add another point here: We have a Charter in Canada. Not too many countries have a Charter, so it's hard to see if somebody else could do it. However, in my case, the Charter and the rights contained in it are top of mind when I deal with the issues that I have to on a daily basis.

[*Translation*]

**Senator Youance:** My question is for the Canada Energy Regulator. If we consider the example of the major blackout that occurred in Spain, what substantive safeguards does Bill C-8 provide to prevent or contain a cyberattack that could cause a widespread power grid failure in Canada?

[*English*]

**Mr. Finley:** Thank you for the question. I may turn it over to my colleague after responding.

Existing regulations on the international power line side are complex, no question.

The companies operating within Canada and crossing interprovincial and international borders generally follow strict North American Electric Reliability Corporation standards, so critical infrastructure standards and protection standards exist now, and they are fairly robust, and through the Canada Energy Regulator's general order, companies that we regulate must also follow those standards.

The addition of the CCSPA would certainly enhance that protection and ability to understand the threat landscape and to work with federal departments, such as the Cyber Centre, CSE, CSIS and RCMP, as we look at our own infrastructure and how we regulate.

Mr. Shepherd, would you have anything to add?

**Robert Shepherd, Technical Specialist, Canada Energy Regulator:** I don't have much to add. I will simply that we already require, as my colleague pointed out, that regulated companies have robust security management programs, which

À ce stade, il ne manque rien de notre point de vue. Nous jugeons que les mesures sont assez complètes et devraient s'ajouter à ce que nous avons déjà comme responsables de la réglementation.

**M. Noël :** La fonction de commissaire au renseignement est véritablement un produit canadien, et il est difficile d'imaginer ce que feraient d'autres pays dans de telles circonstances.

Permettez-moi d'ajouter un autre point. Nous avons une Charte au Canada. Rares sont les pays qui en ont une, donc il est difficile de savoir si d'autres pourraient faire la même chose. Cependant, pour ma part, la Charte et les droits qu'elle contient sont toujours en tête de mes préoccupations lorsque je traite des questions au quotidien.

[*Français*]

**La sénatrice Youance :** Ma question s'adresse à la Régie de l'énergie du Canada. Si nous pensons à l'exemple de la panne majeure survenue en Espagne, quelle garantie concrète le projet de loi C-8 offre-t-il pour prévenir ou contenir une cyberattaque susceptible de provoquer une panne étendue du réseau électrique au Canada?

[*Traduction*]

**M. Finley :** Merci pour votre question. Je vais répondre et laisser la parole à mon collègue.

Il ne fait aucun doute que la réglementation existante sur les lignes internationales de transport d'électricité est complexe.

Les entreprises qui ont des activités au Canada et qui doivent franchir des frontières interprovinciales et internationales respectent généralement les normes strictes de la North American Electric Reliability Corporation. Il existe donc des normes pour les infrastructures essentielles et des normes de protection, et elles sont assez robustes. De plus, en vertu des ordonnances générales de la Régie de l'énergie du Canada, les entreprises que nous réglementons doivent aussi suivre ces normes.

Le recours additionnel à la Loi sur la protection des cybersystèmes essentiels renforcerait certainement cette protection et permettrait une meilleure compréhension du contexte des menaces, ainsi que la collaboration avec les instances fédérales, comme le Centre pour la cybersécurité, le CST, le SCRS et la GRC, dans le cadre de l'examen de notre propre infrastructure et de la façon dont nous appliquons la réglementation.

Monsieur Shepherd, avez-vous quelque chose à ajouter?

**Robert Shepherd, spécialiste technique, Régie de l'énergie du Canada :** Je n'ai pas grand-chose à ajouter. Je dirai seulement que, comme mon collègue l'a souligné, nous exigeons déjà que les entreprises assujetties à la réglementation disposent

identify the assets and the threats and vulnerabilities associated with those assets and come up with and deploy countermeasures commensurate with the risks posed to those assets.

That would not change under the CCSPA. The addition of cybersecurity plans would complement what we already have.

The mandatory incident reporting requirement of the act will, as several of my colleagues pointed out, improve our situational awareness for the types of attacks or efforts that threat actors are implementing at any given time and improve our ability to react nimbly to that in terms of how we structure our compliance oversight of regulated companies to ensure that we are leaning forward and ensuring that they are mitigating those threats as well as they can. Thank you.

[*Translation*]

**Senator Youance:** With regard to the cybersecurity expertise required to address all of these challenges, would there be a disproportionate impact on small producers operating at a national level compared to larger companies?

[*English*]

**Mr. Finley:** Thank you for that question. I would say that the Canada Energy Regulator has a significant amount of experience in terms of how we regulate large and small operators through the Onshore Pipeline Regulations and the CSA standard we were referring to earlier. They are quite scalable to the type of operation that we regulate.

Most definitely, the opportunity is there, and through CCSPA and the regulations that will be developed to support it, we understand that there will be an opportunity to continue that kind of proactive and flexible performance-based oversight.

**Senator Yussuff:** Thank you, witnesses, for being here. I have a couple of questions. I will start with Mr. Carley. OSFI does an incredible job, obviously, in trying to provide oversight to what the banks can do, but let me dig down a little.

In Quebec, the largest financial institution is not a bank, but it has federal reach and operates outside of Quebec. How would you assist them in that regard? More importantly, a lot of our credit unions are not as large as banks but provide an incredible financial service to their consumers.

How do you assist them, granted that the province doesn't have a robust system to help our credit union meet cybersecurity threats they may be faced with on a regular basis?

de programmes de gestion de la sécurité robustes, permettant d'identifier les actifs, ainsi que les menaces et vulnérabilités qui leur sont associées, et proposant ainsi que déployant des contre-mesures proportionnées aux risques pour ces actifs.

Cela ne changera pas en vertu de la Loi sur la protection des cybersystèmes essentiels. L'ajout de plans de cybersécurité viendrait compléter ce que nous avons déjà.

L'exigence obligatoire de signalement des incidents prévue par la loi permettra, comme l'ont souligné plusieurs de mes collègues, d'améliorer notre connaissance de la situation concernant les types d'attaques ou de tentatives déployées par les acteurs malveillants et renforcera notre capacité à réagir rapidement, en structurant notre contrôle de conformité des entreprises assujetties à la réglementation, afin de nous assurer que nous sommes proactifs et que ces entreprises atténuent ces menaces du mieux possible.

[*Français*]

**La sénatrice Youance :** En ce qui a trait à la compétence requise en matière de cybersécurité pour faire face à tous ces enjeux, y aurait-il un impact disproportionné sur les petits producteurs qui œuvrent à l'échelle nationale, comparativement à de plus grandes entreprises?

[*Traduction*]

**M. Finley :** Merci pour cette question. Je dirais que la Régie de l'énergie du Canada possède une solide expérience en matière de réglementation des exploitants, petits ou grands, grâce au Règlement sur les pipelines terrestres et à la norme CSA mentionnée plus tôt. Ces outils peuvent être assez bien adaptés au type d'opérations que nous réglementons.

Il ne fait aucun doute que cette possibilité existe, et grâce à la loi et à la réglementation qui sera élaborée pour l'appuyer, nous prévoyons pouvoir poursuivre une surveillance proactive, souple et axée sur la performance.

**Le sénateur Yussuff :** Merci aux témoins d'être présents. J'ai quelques questions. Je vais commencer avec M. Carley. Le BSIF fait un travail remarquable, évidemment, en ce qui a trait à la surveillance des banques, mais permettez-moi d'aller un peu plus loin.

Au Québec, la plus grande institution financière n'est pas une banque, mais elle a une portée fédérale et a également des activités à l'extérieur du Québec. Quelle aide pourriez-vous lui apporter? Qui plus est, plusieurs de nos coopératives d'épargne et de crédit ne sont pas aussi grandes que les banques, mais offrent d'excellents services financiers à leurs membres.

Comment les aidez-vous, sachant que la province n'a pas de système robuste pour aider les coopératives d'épargne et de crédit à faire face aux cybermenaces auxquelles elles peuvent être confrontées régulièrement?

**Mr. Carley:** First, in terms of Quebec, the institution that you mentioned does have some federally regulated subsidiaries that are under the oversight of OSFI. Between OSFI and some of the prudential regulators — actually, all the provinces — we have a national association that is there for sharing information and best practices.

As a matter of course, when we come out with new regulatory guidance and expectations, we'll share that in advance of publication and have ongoing conversations with a number of the provincial regulators about the evolution of our policy suite. That goes from things like capital liquidity standards for banks right through to these non-financial risks, as we often call them, so operational cyber-resilience and third-party risk management.

Further, the regulator in Quebec also has its own representation at the international level alongside OSFI and certain groups, so I wouldn't underestimate the resources or capacity of some of the regulators.

**Senator Yussuff:** Commissioner Noël, thanks again for being here, and thank you for your insistence on your responsibility being acknowledged but equally being observed. We don't need your office if your office is not being treated with respect and honoured for its responsibilities.

Given this enormous responsibility, I want to restate something you have said. I want to make sure I understand it correctly. You're simply saying that you want the opportunity, for any order the minister would issue to CSE, to review that order to ensure they are in compliance in keeping with your responsibility as the oversight officer for that jurisdiction.

Maybe you could simplify for me what you see as missing in the legislation and how this could be corrected.

**Mr. Noël:** The fact that the Intelligence Commissioner is not part of the system means that, at the beginning of any decision, there will not be any involvement of a third party that will look into the situation and make sure that it's in accordance with their legislation.

Second, when they do collect information on Canadians, they do it in accordance with their own internal policies. They will be left on their own, except after the fact.

Then NSIRA, the civilian review agency, will have an opportunity. It's been shown that 50 decisions of our office have produced on the part of the agencies an attitude of being very meticulous and very concerned about information on Canadians and with ensuring that they don't go overboard when they have to deal with it for the purposes of solving, for instance, a cybersecurity incident.

**M. Carley :** Tout d'abord, concernant le Québec, l'institution que vous avez mentionnée possède bien des filiales régies par le fédéral, qui relèvent de la surveillance du BSIF. Le BSIF et plusieurs responsables de la réglementation prudentielle — en fait, toutes les provinces —, font partie d'une association nationale qui facilite l'échange d'informations et de pratiques exemplaires.

En général, lorsque nous dévoilons de nouvelles orientations et attentes en matière de réglementation, nous les partageons avant publication et nous entretenons des dialogues continus avec plusieurs responsables provinciaux de la réglementation sur l'évolution de notre cadre politique. Cela va des normes de liquidité des banques aux risques dits non financiers, c'est-à-dire la cyberrésilience opérationnelle et la gestion du risque à l'égard des tiers.

Par ailleurs, l'organisme de réglementation québécois est aussi représenté à l'international aux côtés du BSIF et d'autres groupes. Je ne sous-estimerais donc pas les ressources ni les capacités de certains responsables de la réglementation.

**Le sénateur Yussuff :** Monsieur le commissaire Noël, merci encore d'être parmi nous et merci d'avoir insisté pour que vos responsabilités soient non seulement reconnues, mais aussi respectées. Votre bureau n'a pas lieu d'être s'il n'est pas traité avec respect et si ses responsabilités ne sont pas honorées.

Compte tenu de cette énorme responsabilité, je veux revenir sur quelque chose que vous avez dit, pour être sûr de bien comprendre. Vous dites simplement que vous souhaitez avoir la possibilité, pour toute ordonnance que le ministre adresserait au CST, d'en faire l'examen, afin de confirmer qu'elle est conforme à votre responsabilité de surveillance dans ce domaine.

Pouvez-vous m'expliquer simplement quelles sont les lacunes dans la loi et la façon d'y remédier?

**M. Noël :** Le fait que le commissaire au renseignement ne fasse pas partie du système signifie qu'avant toute décision, il n'y aura pas d'intervention d'un tiers pour examiner la situation et s'assurer que la loi est respectée.

Ensuite, lorsque des renseignements sont recueillis sur des Canadiens, ils le sont en fonction de politiques internes. Les responsables sont laissés à eux-mêmes, et s'il y a intervention, c'est après le fait.

C'est là qu'entrera en jeu l'OSSNR, l'organisme civil de surveillance. Il a été démontré que les 50 décisions rendues par notre bureau ont incité les organismes à être très méticuleux et attentifs concernant les informations touchant les Canadiens, et à veiller à ne pas dépasser les bornes lorsqu'elles gèrent ces renseignements pour, par exemple, résoudre un incident de cybersécurité.

**Senator Dasko:** My questions are to Mr. Finley and Mr. Carley. We are talking about legislation that is supposed to protect the infrastructure in these two industries. I want to ask a question about prevention.

Will this help prevent anything? Are you just expecting to face a barrage of cyberattacks into the future? Are there any preventative expectations in this legislation or is it just protecting and cyberattacks will continue without letting up? I want your sense of the future with the legislation.

**Mr. Carley:** I will start on that question and some of the requirements under the legislation in terms of operators needing to have strategies in place to deal with cyber-threats. I can speak to OSFI's experience in terms of similar requirements that we have through our guidance, but they don't have the same power of law as what will be in this legislation.

With the operators needing to put in place a strategy to mitigate the risks, they need to understand what the risks are. They need to understand where their vulnerabilities are as operators, and then they need to have the resources and expertise and the mitigants put in place.

These types of general requirements in the legislation can drive very specific risk outcomes for operators over time. I don't want you to go away with the expectation that, at least in the banking sector, we don't have expectations in place like that already. We do. However, this bill's reach across a number of industries and, as I mentioned, the reporting on incidents and the ability of the Cyber Centre to pull in that information and look across sectors, then provide that intelligence back to operators, can, over time, have an impact on the ability to mitigate and deter threats.

**Senator Dasko:** Mr. Finley, do you have any comment on that?

**Mr. Finley:** Yes, and thank you for the question. It is slightly different under the Canada Energy Regulator. We have the existing Onshore Pipeline Regulations, and there is a legal requirement for companies to develop a security management program already, so it does have prevention aspects to it. It is to anticipate, prevent, manage and mitigate conditions that could adversely affect people, property and the environment.

With Bill C-8, we would see the enhanced reporting fed back to us or given to us directly so we can look more on a preventative basis at our companies through our compliance oversight and get ahead of the game.

**La sénatrice Dasko :** Mes questions s'adressent à M. Finley et à M. Carley. Nous parlons de dispositions législatives censées protéger les infrastructures dans ces deux secteurs. J'aimerais vous poser une question sur la prévention.

Cela va-t-il vraiment permettre de prévenir quoi que ce soit? Vous attendez-vous à devoir faire face à une vague continue de cyberattaques à l'avenir? Ces dispositions législatives comportent-elles des mesures préventives ou se limitent-elles à assurer une protection, alors que les cyberattaques se poursuivent sans relâche? J'aimerais avoir votre point de vue sur l'avenir dans le contexte de ces dispositions législatives.

**M. Carley :** Je vais commencer en mentionnant certaines exigences de la loi, notamment concernant les exploitants qui doivent avoir des stratégies en place pour répondre aux cybermenaces. Je peux parler de l'expérience du BSIF concernant des exigences semblables dans nos lignes directrices, même si celles-ci n'ont pas la même force exécutoire que ce qui sera dans ce texte.

Pour mettre en place une stratégie d'atténuation de risques, les exploitants doivent comprendre ces risques. Ils doivent identifier leurs vulnérabilités, disposer des ressources et de l'expertise nécessaires et mettre en place des mesures d'atténuation.

Ces types d'exigences générales dans la loi peuvent, avec le temps, provoquer des résultats concrets en matière de gestion des risques pour les exploitants. Je ne veux pas que vous partiez du principe que, dans le secteur bancaire du moins, nous n'avons pas déjà ce genre d'attentes. C'est le cas. Toutefois, la portée de ce projet de loi, qui couvre plusieurs secteurs, ainsi que le signalement des incidents et la capacité du Centre pour la cybersécurité à recueillir et à analyser ces informations intersectorielles et à fournir ce renseignement aux exploitants peuvent, à terme, avoir un impact sur la capacité à atténuer et contrer les menaces.

**La sénatrice Dasko :** Monsieur Finley, souhaitez-vous ajouter quelque chose à ce propos?

**M. Finley :** Oui, merci pour la question. C'est un peu différent sous la Régie de l'énergie du Canada. Nous avons déjà le Règlement sur les pipelines terrestres, et il y a une obligation légale pour les entreprises de développer un programme de gestion de la sécurité. Des aspects de prévention sont donc déjà là. On vise aussi à anticiper, à prévenir, à gérer et à atténuer les situations pouvant nuire aux personnes, aux biens et à l'environnement.

Avec le projet de loi C-8, nous recevrions des rapports améliorés, soit par rétroaction, soit directement, ce qui nous permettrait d'adopter une approche plus préventive lors de notre surveillance de conformité, ainsi que d'être proactifs.

If we know something has happened in terms of an incident, we can look across our industry and either issue safety advisories or do compliance activities that focus on that specific issue. Thank you.

**Senator Dasko:** Thank you.

**The Chair:** In the interests of time and efficiency, we do have round two, Senator Cardozo. I would like to propose we have the three questions stated on the record, and then I would encourage you to respond to us in writing.

I want to get the three questions on the record, and responses would be greatly appreciated.

**Senator Batters:** My question is again to the Intelligence Commissioner, Mr. Noël. When you testified at the House of Commons committee six months ago, you said that Bill C-8 still lacks protection against warrantless searches. There were some amendments made after that, but a warrant is still not required generally for entry into and the search of an office or other non-residential premises. I'm wondering if that hole — warrantless searches — in Bill C-8 continues to concern you. Today, you also reiterated your position that technical information could touch on the private information of Canadians. You also said you ". . . remain unconvinced that regulation . . ." will adequately protect Canadians' rights on this.

That is contrary to the stance voiced by government officials on technical information. I would like you to tell us a bit more about that and how you believe those problems in Bill C-8 can be fixed if you think they need to be.

**Senator McNair:** I was just going to give Mr. Finley an opportunity to indicate whether they support the bill as is, as amended. Two things came from your comments: first, from Mr. Shepherd, that mandatory reporting will improve situational awareness; and, second, that one party's breach becomes another party's defence because you have the knowledge that it's taken place.

That's what is lacking now. That's one of the things that one of the officials was concerned about earlier.

**The Chair:** This brings us to the end of our time this evening. Thank you, Commissioner Noël, Mr. Carley, Mr. Finley and Mr. Shepherd. We greatly appreciate your contributions and, frankly, your candour tonight related to this bill.

Si nous savons qu'un incident s'est produit, nous pouvons analyser le secteur et publier des avis de sécurité ou entreprendre des activités de conformité ciblées.

**La sénatrice Dasko :** Merci.

**La présidente :** Pour économiser du temps et par souci d'efficacité, passons à la deuxième série de questions, sénateur Cardozo. Je suggère que les trois questions soient consignées dans le compte rendu des délibérations, et je vous invite à nous répondre par écrit.

Je souhaite que ces trois questions figurent dans le compte rendu des délibérations et que vous y répondiez.

**La sénatrice Batters :** Ma question s'adresse de nouveau au commissaire au renseignement, M. Noël. Lorsque vous avez témoigné devant le comité de la Chambre des communes, il y a six mois, vous avez affirmé que le projet de loi C-8 ne prévoyait toujours pas de protection contre les perquisitions sans mandat. Certains amendements ont été apportés depuis, mais un mandat n'est toujours pas requis en général pour entrer dans un bureau ou tout autre local non résidentiel et y effectuer une perquisition. Je me demande si ce vide — les perquisitions sans mandat — dans le projet de loi C-8 continue de vous préoccuper. Aujourd'hui, vous avez également réitéré votre position selon laquelle l'information technique pourrait porter atteinte aux renseignements personnels des Canadiens. Vous avez également déclaré que vous n'étiez toujours pas convaincu qu'un règlement protégera adéquatement les droits des Canadiens à cet égard.

Cela va à l'encontre de la position exprimée par les représentants du gouvernement concernant les informations techniques. J'aimerais que vous nous en disiez davantage à ce sujet et que vous nous expliquiez comment, selon vous, ces lacunes dans le projet de loi C-8 pourraient être corrigées, s'il y a lieu.

**Le sénateur McNair :** J'allais justement donner à M. Finley l'occasion d'indiquer si son organisme soutient le projet de loi tel quel, dans sa version modifiée. Deux points ressortent de vos commentaires : premièrement, selon M. Shepherd, l'obligation de signalement améliorera la connaissance de la situation; et, deuxièmement, l'infraction commise par une partie deviendra un moyen de défense pour une autre partie, car il sera connu qu'elle a eu lieu.

C'est précisément ce qui fait défaut actuellement. C'est l'une des préoccupations soulevées par l'un des responsables tout à l'heure.

**La présidente :** Cela nous amène à la dernière partie de notre séance de ce soir. Merci, commissaire Noël, monsieur Carley, monsieur Finley et monsieur Shepherd. Nous apprécions grandement votre contribution et, sincèrement, votre franchise ce soir à l'égard de ce projet de loi.

For this final panel of the evening, we are very pleased to welcome Michael Powell, Vice President, Government Relations, Electricity Canada; Todd Warnell, Chief Information Security Officer and Enterprise Resilience, Bruce Power; and Eric Smith, Senior Vice-President, Canadian Telecommunications Association. Thank you for joining us today.

We are going to begin with your opening remarks, to be followed by questions from senators. I remind you that you each have five minutes for opening remarks.

**Michael Powell, Vice President, Government Relations, Electricity Canada:** Good evening, and thank you, Madam Chair.

My name is Mike Powell, and I am the Vice President of Government Relations at Electricity Canada. I lead our security work and am also, among other things, the staff lead on our board committee on energy security.

Electricity Canada is the national voice of the electricity sector. Our members generate, transmit and distribute electrical energy across Canada to homes and businesses in every province and territory.

Critical infrastructure, like electricity, is constantly targeted by cyber-threat actors. We see this in the National Cyber Threat Assessment, which is consistently underlining the risks to our sector, be it from cybercriminals seeking financial gain through ransomware or hostile nation-state actors aiming to pre-position within our systems with the aim of potentially disrupting service delivery.

Electricity companies understand these threats and the importance of protecting their assets against them. Reliable electricity is essential to Canadians' safety, and critical services depend on it. For these reasons, reliability, resiliency and safety have always been the main priorities for our sector. Our job is to keep the lights on for Canadians, and this includes protecting the grid from physical and cyber-threats.

Our sector has robust and well-developed cybersecurity programs. We are governed — as was mentioned in the last panels — by the North American Electric Reliability Corporation's Critical Infrastructure Protection standards, or NERC CIP, which provinces adopt and enforce through our members. These standards ensure strong and comprehensive measures to secure the grid.

Dans le dernier groupe de témoins de la soirée, nous sommes très heureux d'accueillir Michael Powell, vice-président, Relations gouvernementales, chez Électricité Canada; Todd Warnell, directeur de la sécurité de l'information et de la résilience de l'entreprise, chez Bruce Power; et Eric Smith, vice-président principal de l'Association canadienne des télécommunications. Merci de vous joindre à nous aujourd'hui.

Nous allons commencer par vos observations liminaires, qui seront suivies des questions des sénateurs et sénatrices. Je vous rappelle que vous disposez chacun de cinq minutes pour vos observations liminaires.

**Michael Powell, vice-président, Relations gouvernementales, Électricité Canada :** Bonsoir, et merci, madame la présidente.

Je m'appelle Mike Powell et je suis vice-président, Relations gouvernementales, chez Électricité Canada. Je dirige nos activités en matière de sécurité et je suis également, entre autres, responsable d'équipe au sein du comité du conseil d'administration chargé de la sécurité énergétique.

Électricité Canada est la voix nationale du secteur de l'électricité. Nos membres produisent, transmettent et distribuent de l'énergie électrique à travers le Canada, au service des ménages et des entreprises dans toutes les provinces et tous les territoires.

Les infrastructures essentielles, comme l'électricité, sont constamment ciblées par des auteurs de cybermenaces. C'est ce que souligne l'Évaluation des cybermenaces nationales, qui met régulièrement en évidence les risques pesant sur notre secteur, qu'il s'agisse de ceux liés aux cybercriminels à la recherche d'un gain financier par rançongiciel ou à des acteurs étatiques hostiles visant à se positionner dans nos systèmes dans le but de potentiellement perturber la prestation des services.

Les compagnies d'électricité comprennent ces menaces et l'importance de protéger leurs actifs contre elles. La fiabilité du secteur de l'électricité est cruciale pour la sécurité des Canadiens, et des services essentiels en dépendent. C'est pourquoi la fiabilité, la résilience et la sécurité ont toujours été les grandes priorités de notre secteur. Notre rôle est de faire en sorte que les Canadiens ne subissent pas de pannes, et cela inclut la protection du réseau contre les menaces physiques et les cybermenaces.

Notre secteur dispose de programmes de cybersécurité robustes et bien développés. Nous sommes régis — comme cela a été mentionné précisément — par les normes de protection des infrastructures essentielles de la North American Electric Reliability Corporation, ou NERC CIP, qui sont adoptées par les provinces et appliquées par l'entremise de nos membres. Ces normes font en sorte que des mesures solides et complètes sont prises pour sécuriser le réseau.

We collaborate and share information on a regular basis with our partners in government, including Public Safety Canada, Natural Resources Canada and the Canadian Centre for Cyber Security, and our members already participate in programs like the Independent Electric System Operator of Ontario's Lighthouse, which provides a near real-time view into cyber-threats that might affect the system.

We share information among ourselves that enables the sharing of best practices and lessons learned. At Electricity Canada, we facilitate these discussions and work closely, as I said, to strengthen our collective resilience. Resilience is built by working together.

Bill C-8 has been part of public debate for some time. We recognize the need for this legislation, but we have two key concerns about how it may be implemented and potential unintended consequences.

First, there's a risk of regulatory duplication. As mentioned, we're governed by NERC CIP. Introducing new potentially conflicting federal requirements could create ambiguity, increase compliance burden and cause regulatory misalignment, undermining the bill's objective of enhancing security. In the other place, the legislation was amended to address this issue. It strengthens the consistency with regulatory and standards regime provisions, requiring regulations to align with existing frameworks and allowing equivalent regimes to be recognized for compliance under the legislation. We urge the committee to maintain these amendments.

Our second concern is the risk to partnerships between critical infrastructure operators and the Cyber Centre, which is part of the CSE. Today, our sector benefits from a strong, collaborative relationship with the Cyber Centre, built on the confidence that information shared is not disclosed to regulators, enforcement bodies or other government departments. Bill C-8 could require the CSE to share incident reports with regulators, provide advice or services to regulators on operators' compliance and supply-chain risk mitigation and authorize CSE staff to share information with other government entities to issue cybersecurity directions. These new roles and responsibilities risk creating a chilling effect, as operators may hesitate to share information with the Cyber Centre if it could later be used for regulatory enforcement.

Nous collaborons régulièrement avec nos partenaires gouvernementaux, notamment Sécurité publique Canada, Ressources naturelles Canada et le Centre canadien pour la cybersécurité, avec qui nous partageons des informations, et nos membres participent déjà à des programmes comme Lighthouse, de la Société indépendante d'exploitation du réseau d'électricité de l'Ontario, qui offre un aperçu quasi en temps réel des cybermenaces pouvant affecter le système.

Nous partageons entre nous des informations qui permettent la mise en commun des pratiques exemplaires et des leçons apprises. Chez Électricité Canada, nous facilitons ces discussions et travaillons en étroite collaboration avec d'autres intervenants, comme je l'ai indiqué, pour renforcer notre résilience collective. La résilience se construit en travaillant ensemble.

Le projet de loi C-8 fait partie du débat public depuis un certain temps. Nous reconnaissons la nécessité de ces dispositions législatives, mais avons deux préoccupations clés quant à leur mise en œuvre et à ses conséquences imprévues potentielles.

Premièrement, il y a un risque de chevauchement de la réglementation. Comme il a été mentionné, nous sommes régis par les normes NERC CIP. L'adoption de nouvelles exigences fédérales potentiellement conflictuelles pourrait créer une ambiguïté, accroître le fardeau de conformité et entraîner un désalignement réglementaire, ce qui compromettrait l'objectif du projet de loi d'améliorer la sécurité. À la Chambre des communes, la loi a été modifiée pour régler ce problème. Cela renforce la cohérence avec les dispositions des programmes de réglementation et de normalisation, fait en sorte que la réglementation s'aligne sur les cadres existants et permet à des programmes équivalents d'être reconnus pour la conformité au titre de la loi. Nous exhortons ce comité à conserver ces amendements.

Notre seconde préoccupation porte sur le risque pesant sur les partenariats entre les exploitants d'infrastructures essentielles et le Centre pour la cybersécurité, qui relève du Centre de la sécurité des télécommunications. Aujourd'hui, notre secteur bénéficie d'une forte relation de partenariat collaboratif avec le Centre pour la cybersécurité, qui est fondée sur la garantie que les informations partagées ne seront pas divulguées aux organismes de réglementation, aux autorités chargées de l'application de la loi ou à des ministères du gouvernement. Le projet de loi C-8 pourrait obliger le CST à partager les rapports d'incidents avec les responsables de la réglementation, à leur fournir des conseils ou des services concernant la conformité des exploitants et l'atténuation des risques liés à la chaîne d'approvisionnement, ainsi qu'à autoriser le personnel du CST à communiquer des renseignements à d'autres entités gouvernementales pour émettre des directives en cybersécurité. Ces nouveaux rôles et responsabilités risquent de créer un effet dissuasif, puisque les exploitants pourraient hésiter à partager des informations avec le Centre pour la cybersécurité si celles-ci

To protect these partnerships, we recommend that Bill C-8 better define information sharing between the CSE and the rest of government and protect voluntary information from being disclosed. If this clarification can't be achieved or provided through legislative amendments, we would urge the government to address these concerns through clear, transparent policies.

The pace of change in both the threat landscape and the electricity sector has never been greater. Emerging trends, including the use of AI to identify and exploit cybersecurity vulnerabilities, are accelerating the need for strong cybersecurity programs and sustained investment. As we enhance Canada's resilience to cyber-threats, we must ensure the new measures strengthen security and do not create duplication and unintended consequences for security partnerships.

Thank you for your time. I look forward to answering your questions.

**The Chair:** Thank you, Mr. Powell.

Mr. Warnell, please proceed.

**Todd Warnell, Chief Information Security Officer and Enterprise Resilience, Bruce Power:** Thank you, Madam Chair and members of the committee.

Bruce Power is Canada's only private sector nuclear generator. Since 2001, Bruce Power has supplied roughly one third of Ontario's electricity and produces medical isotopes used worldwide to fight cancer and sterilize medical equipment.

Thank you for the invitation to appear before the committee as you continue your study of Bill C-8. As with my previous testimony before both House and Senate committees, my comments today will largely reinforce what I shared previously but with an important update. The risk environment has accelerated faster than our original assumptions.

Bill C-8, and, in particular, Part 2 and the critical cyber systems protection act, is fundamentally about resilience. It is about ensuring the systems that Canadians rely on every day continue to operate safely and reliably in the face of a growing and increasingly sophisticated cyber-threat landscape. If

étaient susceptibles d'être utilisées ultérieurement à des fins d'application de la réglementation.

Pour protéger ces partenariats, nous recommandons que le projet de loi C-8 définisse plus précisément les limites de l'échange d'information entre le CST et le reste de l'administration publique et protège les renseignements fournis de manière volontaire contre toute divulgation. Si cette précision ne peut être obtenue par amendement législatif, nous invitons instamment le gouvernement à régler ces préoccupations par des politiques claires et transparentes.

Le rythme des changements, tant dans le paysage des menaces que dans le secteur de l'électricité, n'a jamais été aussi rapide. Les nouvelles tendances, notamment l'emploi de l'intelligence artificielle pour identifier et exploiter des vulnérabilités en cybersécurité, accentuent la nécessité de programmes robustes de cybersécurité et d'investissements soutenus. Alors que nous renforçons la résilience du Canada face aux cybermenaces, nous devons veiller à ce que les nouvelles mesures améliorent la sécurité et n'entraînent pas de chevauchement ni de conséquences non souhaitées pour les partenariats en matière de sécurité.

Merci de votre temps. Je suis prêt à répondre à vos questions.

**La présidente :** Merci, M. Powell.

M. Warnell, vous avez la parole. Je vous en prie.

**Todd Warnell, directeur de la sécurité de l'information et de la résilience de l'entreprise, Bruce Power :** Merci, madame la présidente, et merci aux membres de ce comité.

Bruce Power est le seul producteur privé d'énergie nucléaire au Canada. Depuis 2001, Bruce Power fournit environ un tiers de l'électricité de l'Ontario et produit des isotopes médicaux utilisés partout dans le monde pour lutter contre le cancer et stériliser le matériel médical.

Je vous remercie de m'avoir invité à comparaître devant ce comité dans le cadre de l'étude du projet de loi C-8. Comme lors de mes témoignages précédents devant des comités de la Chambre des communes et du Sénat, mes observations d'aujourd'hui vont essentiellement confirmer ce que j'ai déjà exposé, mais avec une mise à jour importante. Le contexte des risques a évolué plus rapidement que ce que nous avions prévu dans nos hypothèses initiales.

Le projet de loi C-8, notamment sa partie 2, qui édicte la Loi sur la protection des cybersystèmes essentiels, concerne essentiellement la résilience. Elle vise à garantir que les systèmes dont dépendent quotidiennement les Canadiens continuent de fonctionner de manière sûre et fiable face à un paysage de

anything, the world today is more unpredictable and contested than it was even just a year ago.

We are operating in a period of heightened geopolitical tension where cyber activity is not occurring in isolation but as part of broader strategic competition. Canadian and allied intelligence agencies have been clear: Nation-state actors and criminal organizations are actively pre-positioning within critical infrastructure networks. These are not abstract risks. They represent real, deliberate preparations for disruption, coercion or escalation during moments of potential crisis or broader conflict.

Against that backdrop, delay carries its own risk. Bill C-8 represents a necessary first step in establishing a national baseline for cybersecurity across Canada's critical infrastructure sectors while respecting existing regulatory regimes. Importantly, the legislation does not attempt to prescribe detailed technical controls. Instead, it establishes an enabling framework that supports risk-informed, outcomes-based regulation, tailored to the varying realities of different sectors. In my view, that approach is not a limitation; it is a strength.

In a threat environment that is evolving faster than legislation ever can, flexibility in language is a feature that allows government, regulators and operators to respond promptly to changing conditions, incorporate new threat intelligence and adapt expectations without reopening the act each time the risk landscape shifts. In cybersecurity, rigidity is vulnerability.

Within Canada's nuclear sector, we have demonstrated that this model works. Through sustained collaboration between industry, regulators and government, Canada has built a mature, performance-based cybersecurity regime that continues to evolve as threats evolve. Bill C-8 provides a mechanism to extend that same shared-responsibility model more broadly across other critical sectors.

The benefits of moving forward are clear. It strengthens national security and public safety by protecting essential services from increasingly capable adversaries. It drives proactive risk management, shifting organizations away from reactive response and toward continuous improvement. It enables decisive government action in high-risk or time-sensitive scenarios, helping prevent or limit cascading impacts. It keeps Canada aligned with our allies, many of whom are moving quickly to modernize their own critical-infrastructure resilience frameworks. And it protects economic security by reducing the likelihood of disruptive failures across interconnected systems.

cybermenaces qui s'étend et qui est de plus en plus sophistiqué. En fait, le monde d'aujourd'hui est plus imprévisible et remis en question qu'il ne l'était il y a tout juste un an.

Nous évoluons dans une période de tensions géopolitiques accrues, où les cyberactivités ne sont pas isolées, mais s'inscrivent dans une concurrence stratégique plus large. Les agences de renseignement du Canada et de ses alliés ont été explicites : des acteurs étatiques et des organisations criminelles s'implantent activement dans les réseaux d'infrastructures essentielles. Ces risques ne sont pas abstraits. Ils sont le fruit de préparatifs réels et délibérés pour causer des perturbations, exercer des pressions ou entraîner une escalade lors de crises potentielles ou de conflits plus étendus.

Dans ce contexte, le fait de tarder à agir comporte ses propres risques. Le projet de loi C-8 est une première étape nécessaire pour établir une base nationale de cybersécurité dans l'ensemble des secteurs d'infrastructures essentielles du Canada, tout en respectant la réglementation en place. Il importe de souligner que la loi n'impose pas de contrôles techniques détaillés. Elle établit plutôt un cadre habilitant qui favorise une réglementation fondée sur les risques et axée sur les résultats, qui est adaptée aux réalités diversifiées des différents secteurs. À mon avis, cette approche représente non pas une faiblesse, mais une force.

Dans un contexte de menaces qui évolue plus rapidement que la législation ne pourrait jamais le faire, cette souplesse est une caractéristique qui permet aux gouvernements, aux responsables de la réglementation et aux exploitants de réagir rapidement à l'évolution de la situation, d'intégrer de nouveaux renseignements sur les menaces et d'adapter les attentes, sans avoir à rouvrir la loi chaque fois que le contexte change. En cybersécurité, la rigidité est une vulnérabilité.

Dans le secteur nucléaire canadien, nous avons démontré que ce modèle fonctionne. Grâce à une collaboration soutenue entre l'industrie, les responsables de la réglementation et le gouvernement, le Canada a bâti un régime mature de cybersécurité fondé sur la performance, qui continue d'évoluer en parallèle avec les menaces. Le projet de loi C-8 offre un mécanisme pour étendre ce modèle de responsabilité partagée à d'autres secteurs essentiels.

Les avantages d'aller de l'avant sont clairs. Cela renforce la sécurité nationale et la sécurité publique en protégeant les services essentiels contre des adversaires toujours plus compétents. Cela encourage une gestion proactive des risques, faisant passer la démarche des organisations d'une attitude réactive à une amélioration continue. Cela permet au gouvernement d'agir de manière décisive dans des contextes à haut risque ou urgents, ce qui aide à prévenir ou limiter les impacts en cascade. Le Canada peut ainsi demeurer aligné avec ses alliés, qui sont nombreux à moderniser rapidement leurs cadres de résilience des infrastructures essentielles. Enfin, cela

In closing, Bill C-8 is not an end state; it is a foundation. However, in a world defined by greater volatility and uncertainty, establishing that foundation is urgent. The threat environment has evolved faster than our policy framework, and this legislation is an essential step toward closing that gap.

Thank you for the opportunity to appear before the committee. I look forward to your questions.

**The Chair:** Thank you, Mr. Warnell.

**Eric Smith, Senior Vice-President, Canadian Telecommunications Association:** Good evening. The Canadian Telecommunications Association is dedicated to building a better future for Canadians through connectivity. Our members include service providers, manufacturers and other organizations that invest in, build, maintain and operate Canada's world-class telecommunications networks.

Thank you for the opportunity to appear before you today to discuss Bill C-8. The security of Canada's telecommunications system is of the utmost importance. Telecommunications networks are critical infrastructure that underpins Canada's economy, national security and public safety. They enable essential services, support government operations and connect Canadians to health care, education, emergency services and one another.

Our members take this responsibility seriously. They invest significant resources to safeguard their networks from cyber-threats and actively collaborate through forums, such as the Canadian Security Telecommunications Advisory Committee, which facilitates the exchange of information between the private and public sectors, as well as strategic collaboration on current and evolving issues that may affect telecommunications systems, including cybersecurity threats.

We appreciate the government's objective of strengthening Canada's cybersecurity framework and recognize the importance of having the right tools in place to respond to evolving threats. We also welcome the meaningful improvements that have been made to Bill C-8 over the course of the legislative process.

At the same time, it is essential that government recognize that, under Bill C-8, telecommunications service providers will be responsible for implementing government orders that may have significant operational and financial implications. Ensuring

J'aimerais conclure en disant que le projet de loi C-8 n'est pas une fin en soi; c'est une base. Toutefois, dans un monde marqué par une volatilité et une incertitude accrues, il est urgent d'établir cette base. Le contexte des menaces a évolué plus rapidement que notre cadre politique, et ces dispositions législatives sont une étape essentielle pour combler l'écart entre les deux.

Merci de m'avoir donné l'occasion de m'exprimer devant ce comité. Je suis prêt à répondre à vos questions.

**La présidente :** Merci, M. Warnell.

**Eric Smith, vice-président principal, Association canadienne des télécommunications :** Bonsoir. L'Association canadienne des télécommunications s'engage à bâtir un avenir meilleur pour les Canadiens, grâce à la connectivité. Nos membres comprennent des fournisseurs de services, des fabricants et d'autres organisations qui investissent dans les réseaux de télécommunications de classe mondiale du Canada, les construisent, les entretiennent et les exploitent.

Je vous remercie de me donner l'occasion de m'adresser à vous aujourd'hui pour discuter du projet de loi C-8. La sécurité du système de télécommunications du Canada est d'une importance capitale. Les réseaux de télécommunications constituent des infrastructures essentielles qui soutiennent l'économie, la sécurité nationale et la sécurité publique du Canada. Ils permettent la prestation de services essentiels, soutiennent les opérations gouvernementales et relient les Canadiens entre eux, ainsi qu'aux soins de santé, à l'éducation et aux services d'urgence.

Nos membres prennent cette responsabilité au sérieux. Ils investissent des ressources importantes pour protéger leurs réseaux contre les cybermenaces et collaborent activement à des entités comme le Comité consultatif canadien pour la sécurité des télécommunications, qui facilite l'échange d'information entre les secteurs privé et public, ainsi que la collaboration stratégique sur les enjeux actuels et émergents susceptibles d'affecter les systèmes de télécommunications, y compris les cybermenaces.

Nous saluons l'objectif du gouvernement de renforcer le cadre de cybersécurité du Canada et reconnaissons l'importance de disposer des bons outils pour faire face à l'évolution des menaces. Nous accueillons également favorablement les améliorations substantielles apportées au projet de loi C-8 au cours du processus législatif.

Il est également essentiel que le gouvernement reconnaisse que, en vertu du projet de loi C-8, les fournisseurs de services de télécommunications seront responsables de la mise en œuvre de décrets gouvernementaux qui peuvent avoir des répercussions

protège la sécurité économique en réduisant la probabilité de défaillances perturbatrices dans les systèmes interconnectés.

that the legislation addresses this reality will be critical to its effectiveness.

With that in mind, I would like to highlight two areas where we think targeted refinements would strengthen the bill.

First, regarding compensation or cost recovery, Bill C-8 states that no one is entitled to compensation for financial losses resulting from compliance with the government orders. It is important to recognize the practical implications of this approach. Orders issued under this framework could require service providers to rapidly deploy new systems, reconfigure networks, replace equipment or take other actions that involve significant and unplanned costs. These are not routine operational expenses. They can be substantial, immediate and unbudgeted expenses that are incurred in the broader public interest to support national security objectives.

Failure to address the impact of extraordinary costs will have real consequences, not only for the sector but for all Canadians. Significant unplanned costs can constrain investment in network expansion, limit innovation and reduce the ability of providers to enhance service quality for Canadians. Uncertainty around whether these costs may be recoverable can also complicate internal decision making and delay the timely implementation of government orders.

While this applies across the industry, the impact is particularly acute for smaller and regional providers, which operate with less scale and tighter margins. For these providers, the financial burden of compliance can be especially challenging and, in some cases, may threaten their ability to continue operating, resulting in broader knock-on effects for competition, resilience and service availability.

For this reason, we recommend that the legislation explicitly confirm that the Governor-in-Council and the minister have the discretion to provide compensation to offset all or part of the costs incurred in complying with an order and that they make clear when issuing an order whether the affected parties will be entitled to compensation.

This is not a novel concept. Comparable approaches exist in other Canadian legislation. For example, Bill C-22 includes provisions that explicitly allow the minister to provide discretionary compensation to electronic service providers required to implement capabilities in support of lawful access.

opérationnelles et financières importantes. Il sera crucial d'en tenir compte pour assurer l'efficacité de ces dispositions législatives.

Dans cette optique, j'aimerais souligner deux domaines où nous pensons que des ajustements ciblés renforceraient le projet de loi.

Premièrement, en ce qui concerne l'indemnisation ou le recouvrement des coûts, le projet de loi C-8 précise que nul n'a droit à une indemnité pour les pertes financières résultant du respect des décrets gouvernementaux. Il est important de reconnaître les répercussions concrètes de cette approche. Les décrets émis dans ce cadre pourraient exiger que les fournisseurs déploient rapidement de nouveaux systèmes, reconfigurent des réseaux, remplacent du matériel ou prennent d'autres mesures entraînant des coûts importants et imprévus. Il ne s'agit pas de dépenses opérationnelles courantes. Il peut s'agir de coûts substantiels, immédiats et non budgétisés, qui sont engagés dans l'intérêt public plus large, en soutien aux objectifs de sécurité nationale.

Le fait de ne pas tenir compte de l'impact de ces coûts extraordinaires aura des conséquences réelles, non seulement pour le secteur, mais pour tous les Canadiens. De tels coûts imprévus importants peuvent restreindre les investissements dans l'expansion des réseaux, limiter l'innovation et réduire la capacité des fournisseurs à améliorer la qualité des services fournis aux Canadiens. L'incertitude quant à la possibilité de récupérer ces coûts peut également compliquer les décisions internes et retarder la mise en œuvre rapide des décrets gouvernementaux.

Bien que cela concerne l'ensemble du secteur, l'impact est particulièrement aigu pour les petits et moyens fournisseurs régionaux, qui ont des activités à plus petite échelle avec des marges plus étroites. Pour ces fournisseurs, le fardeau financier de la conformité peut s'avérer particulièrement lourd et, dans certains cas, menacer leur capacité à poursuivre leurs activités, entraînant des répercussions plus larges sur la concurrence, la résilience et la disponibilité des services.

C'est pourquoi nous recommandons que la loi confirme explicitement que le gouverneur en conseil et le ministre disposent du pouvoir discrétionnaire d'accorder une indemnisation destinée à couvrir tout ou partie des frais engagés pour se conformer à un décret, et qu'ils précisent clairement, lors de la promulgation d'un décret, si les parties concernées auront droit à une indemnisation.

Ce concept n'est pas nouveau. Des approches similaires existent dans d'autres lois canadiennes. Par exemple, le projet de loi C-22 comprend des dispositions qui autorisent explicitement le ministre à accorder une indemnisation discrétionnaire aux fournisseurs de services électroniques tenus de mettre en place des capacités permettant l'accès légal.

Internationally, similar principles are applied. In the United States, for example, the government has recognized that certain national security measures, such as the removal and replacement of high-risk network equipment, can impose significant financial burdens on telecommunications providers. To address this, funding programs have been established to compensate eligible carriers for these costs. Importantly, these programs have been supported through innovative funding mechanisms, including the use of proceeds from spectrum auctions to finance reimbursement initiatives.

These approaches reflect a practical reality. When governments require private sector actors to take extraordinary measures in the interest of national security, there should be a clear and transparent mechanism to consider compensation.

Our second issue relates to liability protection.

As currently drafted, telecommunications service providers could face civil, regulatory or contractual liability for actions taken in good faith to comply with government orders. This could arise where compliance affects service levels, contractual obligations or other regulatory requirements.

This creates risk at precisely the moment when decisive action may be required. We therefore recommend the inclusion of a safe harbour provision to protect providers and their personnel from liability when acting in good faith and in compliance with lawful orders. This reflects a basic legal principle that parties should not incur liability for actions taken to comply with a legal obligation.

In closing, we share the government's commitment to strengthening Canada's cybersecurity and protecting critical infrastructure. With targeted refinements, particularly with respect to cost recovery and liability, Bill C-8 can provide a framework that supports both national security objectives and continued investment in secure and resilient telecommunications networks.

Thank you.

**The Chair:** Thank you. We will now proceed to questions.

Au niveau international, des principes similaires sont appliqués. Aux États-Unis, par exemple, le gouvernement a reconnu que certaines mesures de sécurité nationale, telles que le retrait et le remplacement d'équipements réseau à haut risque, peuvent imposer un fardeau financier important aux fournisseurs de services de télécommunications. Pour y remédier, des programmes de financement ont été mis en place afin d'indemniser les transporteurs admissibles pour ces coûts. Il est important de noter que ces programmes ont été soutenus par des mécanismes de financement innovants, notamment l'utilisation des recettes issues des enchères du spectre pour financer les initiatives de remboursement.

Ces approches reflètent une réalité concrète. Lorsque les pouvoirs publics exigent des acteurs du secteur privé qu'ils prennent des mesures exceptionnelles dans l'intérêt de la sécurité nationale, il convient de mettre en place un mécanisme clair et transparent permettant d'envisager une indemnisation.

Notre deuxième point concerne la protection en matière de responsabilité.

Selon le libellé actuel, les fournisseurs de services de télécommunications pourraient engager leur responsabilité civile, réglementaire ou contractuelle pour des mesures prises de bonne foi afin de se conformer à des ordres émanant du gouvernement. Cela pourrait se produire lorsque la conformité a une incidence sur les niveaux de service, les obligations contractuelles ou d'autres exigences réglementaires.

Cela engendre un risque précisément au moment où une action décisive pourrait s'avérer nécessaire. Nous recommandons donc l'inclusion d'une disposition d'exonération visant à protéger les fournisseurs et leur personnel contre toute responsabilité lorsqu'ils agissent de bonne foi et conformément à des ordonnances légales. Cela reflète un principe juridique fondamental selon lequel les parties ne devraient pas être tenues responsables de mesures prises pour se conformer à une obligation légale.

Pour conclure, nous partageons l'engagement du gouvernement à renforcer la cybersécurité du Canada et à protéger les infrastructures essentielles. Grâce à des ajustements ciblés, notamment en matière de recouvrement des frais et de responsabilité, le projet de loi C-8 peut offrir un cadre qui soutient à la fois les objectifs de sécurité nationale et la poursuite des investissements dans des réseaux de télécommunications sûrs et résilients.

Merci.

**La présidente :** Merci. Nous allons maintenant passer aux questions.

Colleagues, this panel will be with us until about eight o'clock. As always, we'll each have four minutes. Our first question for this panel goes to the deputy chair, Senator Al Zaibak.

**Senator Al Zaibak:** Thank you all for being here.

We've heard a spectrum of responses from industry and stakeholders based in various sectors. My question is for Mr. Smith.

Telecommunications networks are certainly foundational for all other sectors. You raised two concerns and suggestions for the improvement of the bill. I'm wondering whether you have raised those concerns with the House of Commons. If so, what kinds of reactions did your suggestions receive?

**Mr. Smith:** Yes, we certainly have.

With respect to the issue of at least making clear in the legislation that the minister and the Governor-in-Council have the discretion to award or consider compensation or cost recovery, you probably heard Minister Joly speaking before the House of Commons committee, saying the government views that as the cost of doing business. To a certain extent, that's correct. Our members, as part of their business, take cybersecurity seriously. It's part of their budgeting and risk management, and they spend a lot of money on that.

However, this bill gives the government a very broad scope in making orders to telecommunications providers, including extraordinary measures. I talked about orders to remove high-risk equipment. We know that is on the table. We know that industry has already been cooperating with government in that respect, but we're talking significant sums of money. We're talking probably over $1 billion in terms of costs.

If you look at the United States, they've set up funds of approximately $3 billion or $4 billion, which is still underfunded, to compensate eligible carriers for taking those actions. You heard from Mr. Arbour from ISED today. I think his words were "a slate of measures" that they're very anxious to implement in our industry, including things around making networks more resilient against severe weather events. Well, if you look around the world and at how other countries view those things, like Australia, for example, they've put a number of programs in place to deal with resiliency. As part of that, they've put in funding to help industry harden their networks.

Chers collègues, ce groupe de témoins sera avec nous jusqu'à 20 heures environ. Comme d'habitude, nous disposerons chacun de quatre minutes. C'est notre vice-président, le sénateur Al Zaibak, qui va poser la première question.

**Le sénateur Al Zaibak :** Merci à tous d'être ici.

Nous avons recueilli toute une gamme de réactions de la part des acteurs du secteur et des parties prenantes issues de divers domaines. Ma question s'adresse à M. Smith.

Les réseaux de télécommunications constituent sans aucun doute un pilier fondamental pour tous les autres secteurs. Vous avez soulevé deux préoccupations et formulé deux suggestions visant à améliorer le projet de loi. Je me demande si vous avez fait part de ces préoccupations à la Chambre des communes. Si tel est le cas, quel accueil vos suggestions ont-elles reçu?

**M. Smith :** Oui, certainement.

Pour ce qui est de préciser au moins dans la loi que le ministre et le gouverneur en conseil ont le pouvoir discrétionnaire d'accorder ou d'envisager une indemnisation ou un recouvrement des coûts, vous avez sans doute entendu la ministre Joly dire devant le comité de la Chambre des communes que le gouvernement considère cela comme un coût d'exploitation. Dans une certaine mesure, c'est exact. Nos membres, dans le cadre de leurs activités, prennent la cybersécurité très au sérieux. Cela fait partie de leur budgétisation et de leur gestion des risques, et ils y consacrent beaucoup d'argent.

Toutefois, ce projet de loi confère au gouvernement une marge de manœuvre très large pour imposer des ordonnances aux fournisseurs de services de télécommunications, y compris des mesures exceptionnelles. J'ai parlé des ordres de retrait d'équipements à haut risque. Nous savons que cette option est envisagée. Nous savons que le secteur coopère déjà avec le gouvernement à cet égard, mais il s'agit là de sommes considérables. Les coûts s'élèveraient probablement à plus de 1 milliard de dollars.

Si l'on prend l'exemple des États-Unis, ils ont mis en place des fonds d'environ 3 ou 4 milliards de dollars, ce qui reste insuffisant, pour indemniser les transporteurs admissibles qui prennent ces mesures. Vous avez entendu aujourd'hui M. Arbour, d'ISDE. Je crois qu'il a parlé d'une « série de mesures » qu'ils sont très impatients de mettre en œuvre dans notre secteur, notamment des mesures visant à rendre les réseaux plus résilients face aux conditions météorologiques violentes. Eh bien, si l'on regarde ce qui se passe ailleurs dans le monde et la façon dont d'autres pays abordent ces questions, comme l'Australie par exemple, on constate qu'ils ont mis en place un certain nombre de programmes pour renforcer la résilience. Dans ce cadre, ils ont débloqué des fonds pour aider le secteur à renforcer ses réseaux.

If you look at the U.K., they were considering requirements to provide backup power for mobile cell sites. What they found in their preliminary investigation was that requiring every cell site to have just one hour of backup power would cost almost C$2 billion, and that doesn't take into account that to provide backup power, you have to rely on other things in the supply chain — for example, fuel supply in order to replenish your generators.

All we're saying is we have an example in Bill C-22 where the government has said that compensation and cost recovery are important as part of ordering telecommunications providers to do things. Yet here, we're being told it's the cost of doing business, and that has serious knock-on effects. It's important we make sure to consider those.

**Senator Al Zaibak:** Thank you.

**Senator Cardozo:** I have questions for Mr. Smith and Mr. Powell, but I just want to mention, Mr. Warnell, I've been familiar with the isotope issue for some time. I congratulate you for that. I also happen to be, as of recently, the Senate co-chair of the cancer caucus of Parliament. I co-chair with a couple of MPs. It's something that we certainly watch closely, and we count on you to produce those, as you do for Canada, and you export as well.

Mr. Powell, if I can paraphrase, you said you want to ensure the information you provide to CSE is not shared with others. I'd like you to say a little bit more about what kind of information you're talking about. When you say if it's not an amendment, you would like to see a policy. Does that mean regulation?

Mr. Smith, in terms of compensation for adjustments, I asked the question earlier with regard to small- and medium-sized businesses and non-profits, but I think you're talking about big businesses. I want you to respond to this: One might say these measures are not just things the government is telling you to do but are essential to your business. If that is the case, why would you not be making those investments in your business?

**Mr. Powell:** To be clear, I think we're concerned about the sharing of voluntary information that's provided to the Cyber Centre and others.

The goal of the legislation is to encourage information sharing between industry and government, and I would suggest that's already taking place. Our members, as I said, participate in a

Si l'on prend l'exemple du Royaume-Uni, les autorités envisageaient d'exiger une alimentation de secours pour les stations de base de téléphonie mobile. Leur examen préliminaire a révélé que le fait d'exiger que chaque station de base dispose d'une heure d'alimentation de secours coûterait près de 2 milliards de dollars canadiens, sans compter que, pour assurer cette alimentation de secours, il faut faire appel aux autres maillons de la chaîne d'approvisionnement — par exemple, l'approvisionnement en carburant nécessaire pour alimenter les génératrices.

Tout ce que nous voulons dire, c'est que le projet de loi C-22 nous fournit un exemple où le gouvernement a reconnu que l'indemnisation et le recouvrement des coûts jouent un rôle important lorsqu'il s'agit d'imposer des obligations aux fournisseurs de services de télécommunications. Or, dans le cas présent, on nous dit qu'il s'agit simplement du coût de l'activité, ce qui a de graves répercussions. Il est important de veiller à en tenir compte.

**Le sénateur Al Zaibak :** Merci.

**Le sénateur Cardozo :** J'ai des questions à poser à M. Smith et à M. Powell, mais je tiens tout d'abord à vous dire, Monsieur Warnell, que je suis le dossier des isotopes depuis un certain temps déjà. Je vous en félicite. Il se trouve également que je suis, depuis peu, le coprésident du groupe parlementaire sur le cancer au Sénat. Je copréside ce groupe avec quelques députés. C'est un sujet que nous suivons de très près, et nous comptons sur vous pour produire ces isotopes, comme vous le faites pour le Canada, et que vous exportez également.

Monsieur Powell, si je peux me permettre de paraphraser, vous avez dit que vous souhaitiez vous assurer que les informations que vous fournissez au CST ne soient pas divulguées à des tiers. J'aimerais que vous nous en disiez un peu plus sur le type d'informations dont vous parlez. Lorsque vous dites que, s'il ne s'agit pas d'un amendement, vous souhaiteriez voir mettre en place une politique, cela signifie-t-il une réglementation?

Monsieur Smith, en ce qui concerne l'indemnisation pour les ajustements, j'ai posé la question tout à l'heure au sujet des petites et moyennes entreprises et des organismes à but non lucratif, mais je crois que vous faites référence aux grandes entreprises. J'aimerais que vous répondiez à ceci : on pourrait dire que ces mesures ne sont pas seulement des directives du gouvernement, mais qu'elles sont essentielles à votre entreprise. Si tel est le cas, pourquoi ne feriez-vous pas ces investissements dans votre entreprise?

**M. Powell :** Pour être clair, je pense que ce qui nous préoccupe, c'est l'échange volontaire de renseignements fournis au Centre pour la cybersécurité et à d'autres entités.

L'objectif de cette loi est d'encourager l'échange d'informations entre l'industrie et le gouvernement, et je dirais que cela se produit déjà. Comme je l'ai dit, nos

program called Lighthouse, which connects directly to the Cyber Centre. When we have our security meetings in Ottawa, they are often held in the offices of the Canadian Centre for Cyber Security. There's a regular flow of information back and forth. The concern, at the moment, is that regulatory measures are added where there are potential penalties. It could add a chill that discourages open-ended information sharing.

We would suggest that voluntary information sharing, what's already happening, should be protected to ensure it stays in that space. That's already standard in the United States. I mentioned the North American Electric Reliability Corporation, or NERC. They have an information-sharing agency called the Electricity Information Sharing and Analysis Center, or E-ISAC, and information shared with them is kept separate from the regulator. I think that's what we're looking to make sure of.

The goal of the legislation should be to make our system more secure and add safety. I would suggest that by creating a risk that information be shared less forthrightly because of legal concerns, it would get in the way. We would rather it be in the legislation. We made suggestions at the House of Commons. However, ultimately, if it's done by regulation or other policy, that would be the next best thing.

**Senator Cardozo:** Okay. Thank you.

**Mr. Smith:** To answer your question, certainly, it is part of doing business. As I said, millions of dollars are being spent every year on this. But we also have to consider situations where there are extraordinary orders, for example, to do things that are not contemplated as the ordinary course of business. We've already seen some orders with respect to high-risk suppliers in some countries, which will be coming to Canada.

That was not always the case. When that equipment was first procured, they were not considered high-risk vendors. We, obviously, are seeing right now quite a lot of changes in our geopolitical world. With countries that were trusted, and companies from those countries that were trusted suppliers, in the future, the government may say they don't trust them anymore. Where it was once fine for us to spend billions of dollars to buy their equipment with a lifespan of 20 years, the government may now want us to take that out and replace it with something else.

We're talking about those types of things. We also have to be mindful that our industry works in an interesting environment where this legislation is not in a silo. We have other legislation

membres participent à un programme appelé Lighthouse, qui est directement relié au Centre pour la cybersécurité. Lorsque nous tenons nos réunions sur la sécurité à Ottawa, celles-ci ont souvent lieu dans les locaux du Centre canadien pour la cybersécurité. Il y a un échange régulier d'informations entre les deux parties. Ce qui nous préoccupe actuellement, c'est l'ajout de mesures réglementaires pouvant donner lieu à des sanctions, ce qui pourrait créer un climat de réticence décourageant l'échange volontaire de renseignements.

Nous suggérons que l'échange volontaire de renseignements, qui est déjà une réalité, soit protégé afin de garantir qu'il reste dans ce cadre. C'est déjà la norme aux États-Unis. J'ai évoqué la North American Electric Reliability Corporation, ou NERC. Celle-ci dispose d'un organisme d'échange de renseignements appelé Electricity Information Sharing and Analysis Center, ou E-ISAC, et les renseignements qui lui sont communiqués sont conservés séparément de ceux de l'autorité de réglementation. Je pense que c'est ce dont nous voulons nous assurer.

L'objectif de cette loi devrait être de renforcer la sécurité de notre système et d'améliorer la sûreté. Je crains que le fait de créer un risque que les informations soient partagées avec moins de franchise en raison de préoccupations juridiques ne constitue un obstacle. Nous préférerions que cela figure dans la loi. Nous avons formulé des suggestions à la Chambre des communes. Toutefois, en fin de compte, si cela se faisait par voie réglementaire ou par le biais d'autres mesures, ce serait une autre solution.

**Le sénateur Cardozo :** D'accord. Merci.

**M. Smith :** Pour répondre à votre question, bien sûr, cela fait partie des coûts d'exploitation. Comme je l'ai dit, des millions de dollars sont dépensés chaque année à cette fin. Mais nous devons également tenir compte des situations où des décrets exceptionnels sont pris, par exemple pour prendre des mesures qui ne relèvent pas du cours normal des affaires. Nous avons déjà vu certains décrets concernant des fournisseurs à haut risque dans certains pays, qui vont être appliquées au Canada.

Cela n'a pas toujours été le cas. Lorsque ce matériel a été acheté pour la première fois, ces fournisseurs n'étaient pas considérés comme présentant un risque élevé. Nous assistons évidemment en ce moment à de nombreux changements dans notre environnement géopolitique. Le gouvernement pourrait, à l'avenir, décider de ne plus faire confiance à des pays qui étaient auparavant considérés comme fiables, ni aux entreprises de ces pays qui étaient des fournisseurs de confiance. Alors qu'il nous semblait tout à fait normal de dépenser des milliards de dollars pour acheter leur équipement d'une durée de vie de 20 ans, le gouvernement pourrait désormais exiger que nous le retirions et le remplacions par un autre matériel.

C'est de ce genre de choses dont nous parlons. Nous devons également garder à l'esprit que notre secteur évolue dans un environnement particulier où cette législation ne fait pas figure

that has been passed or that will potentially be passed in the future that will continually increase the cost of doing business. At the same time, we're trying to keep costs down for consumers.

**Senator Batters:** My first question is for Mr. Powell with Electricity Canada. You were talking about this a bit, but I want to give you more time to discuss it.

During the testimony of your colleague before the House of Commons, an important concern was raised that, because of sections 15 to 19, operators might hesitate to provide information to the Canadian Centre for Cyber Security if they fear it could then circulate to regulatory bodies and be used for compliance purposes.

Could you give us a concrete example of the kind of consequence that it could have in practice? How do you think the bill should be amended to avoid that chilling effect and preserve the voluntary sharing of information with the Cyber Centre?

I know that in your opening remarks you also said that if it can't be done through legislation — which, of course, it can, and we're in the business of making legislation better here — it could be done through policy. But given what we're talking about here, that obviously wouldn't have the kind of teeth that you would be looking for.

**Mr. Powell:** I will work backwards. We provided recommended legislative language to the House of Commons, which I'm happy to circulate to you after.

**Senator Batters:** Thank you. Yes, if you could, please.

**Mr. Powell:** The focus is on voluntary information sharing. We talk about what folks might be seeing on their systems and where there might be concerns.

I'm sure we're all familiar with this in other parts. The moment that there is a regulatory piece where a risk could become involved, it changes the conversation about how information is shared with other parties.

What we have right now is a very collaborative, open-ended relationship where some people have a ".gc.ca" email address and others have an "our members.ca" email address, but we're all working on the same team because the outcome is the same.

d'exception. D'autres textes législatifs ont été adoptés ou pourraient l'être à l'avenir, ce qui ne fera qu'alourdir les coûts d'exploitation. Parallèlement, nous nous efforçons de limiter les coûts pour les consommateurs.

**La sénatrice Batters :** Ma première question s'adresse à M. Powell, d'Électricité Canada. Vous avez déjà brièvement abordé ce sujet, mais je voudrais vous laisser davantage de temps pour en parler.

Lors du témoignage de votre collègue devant la Chambre des communes, une préoccupation importante a été soulevée : en raison des articles 15 à 19, les exploitants pourraient hésiter à fournir des informations au Centre canadien pour la cybersécurité s'ils craignent que celles-ci ne soient ensuite transmises aux organismes de réglementation et utilisées à des fins de vérification de la conformité.

Pourriez-vous nous donner un exemple concret des conséquences que cela pourrait avoir en pratique? Selon vous, comment faudrait-il modifier le projet de loi pour éviter cet effet dissuasif et préserver l'échange de renseignements avec le Centre pour la cybersécurité?

Je sais que dans votre introduction, vous avez également indiqué que si cela ne pouvait pas se faire par la voie législative — ce qui, bien sûr, est possible, et notre rôle ici est justement d'améliorer les lois —, cela pourrait se faire par le biais de politiques. Mais compte tenu de ce dont nous parlons ici, cela n'aurait manifestement pas la force d'action que vous recherchez.

**M. Powell :** Je vais procéder à rebours. Nous avons transmis à la Chambre des communes des propositions de formulation législative, que je me ferai un plaisir de vous faire parvenir par la suite.

**La sénatrice Batters :** Merci. Oui, s'il vous plaît.

**M. Powell :** L'accent est mis sur l'échange volontaire de renseignements. Nous parlons de ce que les gens pourraient voir dans leurs systèmes et de ce qui pourrait susciter des préoccupations.

Je suis sûr que nous connaissons tous cette situation dans d'autres domaines. Dès qu'une disposition réglementaire implique un risque, cela modifie la manière dont les renseignements sont échangés avec les autres parties.

À l'heure actuelle, nous entretenons une relation très collaborative et ouverte, dans laquelle certaines personnes ont une adresse courriel « .gc.ca » et d'autres une adresse « nosmembres.ca », mais nous travaillons tous au sein de la même équipe, car l'objectif est le même.

The risk of regulatory compliance — where there are penalties involved, if it's not clear how voluntary information is being shared, it creates an added risk about how that can be provided right now.

The status quo — in the electricity sector, anyway — is that members are able to and do share information with their partners in government, the Canadian Centre for Cyber Security and elsewhere. We just wouldn't want to create a situation where, inadvertently, in an effort to encourage information sharing, you kind of get in the way of that.

Again, if you look to our counterparts in the United States — well, it's in the United States, but it's a North American entity, the NERC E-ISAC. When you go to their office, they have different key codes and everything to get into different parts. The people who work on the information-sharing business are different than the regulatory side.

I don't think we need to go that far, but just being certain and clear and embedding in the legislation that when we're thinking about protecting the grid, we're focused on that and not potential risk from legal issues elsewhere.

**Senator Batters:** Thank you. To Mr. Smith with the Canadian Telecommunications Association, I recall when Bill C-26 was being discussed and the government was being insistent that they would be providing assistance for small- and medium-sized businesses, including financially, I believe. We were trying to pin them down on what exactly they were talking about. But here is an example, as you mentioned, where there could be major consequences for smaller and regional providers from your association from having an explicit no go for compensation or cost recovery.

Tell us a bit more about that and what types of smaller and regional providers could be affected by this if this isn't changed.

**Mr. Smith:** It depends on what the order from the government is and its impact. If you look at the example of the United States in terms of their "rip and replace" program regarding certain Chinese-sourced equipment, there are deadlines involved, and some smaller providers have said they have to stop providing services, and, in some cases, they're the only provider in the community.

Le risque lié au respect de la réglementation — lorsqu'il y a des sanctions à la clé — fait que, si les modalités de l'échange de renseignements fournis à titre volontaire ne sont pas clairement définies, cela crée un risque supplémentaire quant à la manière dont ces renseignements peuvent être fournis à l'heure actuelle.

À l'heure actuelle — du moins dans le secteur de l'électricité —, les membres sont en mesure de partager des informations avec leurs partenaires au sein du gouvernement, du Centre canadien pour la cybersécurité et d'autres organismes, et ils le font effectivement. Nous ne voudrions tout simplement pas créer une situation où, par inadvertance, en cherchant à encourager l'échange de renseignements, on finirait par y faire obstacle.

Encore une fois, si l'on prend l'exemple de nos homologues aux États-Unis — enfin, c'est aux États-Unis, mais il s'agit d'une entité nord-américaine, le E-ISAC de la NERC. Lorsque vous vous rendez dans leurs locaux, il faut utiliser différents codes d'accès pour accéder aux différentes zones. Les personnes qui s'occupent de l'échange de renseignements ne sont pas les mêmes que celles chargées de la réglementation.

Je ne pense pas qu'il soit nécessaire d'aller aussi loin, mais il faut simplement être clair et précis, et inscrire dans la loi que, lorsque nous réfléchissons à la protection du réseau, nous nous concentrons sur cet aspect et non sur les risques potentiels liés à des questions juridiques ailleurs.

**La sénatrice Batters :** Merci. Monsieur Smith, de l'Association canadienne des télécommunications, je me souviens que, lors des débats sur le projet de loi C-26, le gouvernement insistait sur le fait qu'il apporterait son aide aux petites et moyennes entreprises, notamment sur le plan financier, si je ne me trompe pas. Nous essayions de lui faire préciser exactement de quoi il parlait. Mais voici un exemple, comme vous l'avez mentionné, où le refus explicite d'accorder une compensation ou un recouvrement des coûts pourrait avoir des conséquences majeures pour les petits fournisseurs et les fournisseurs régionaux de votre association.

Pourriez-vous nous en dire un peu plus à ce sujet et nous indiquer quels types de petits fournisseurs et de fournisseurs régionaux pourraient être concernés si cette situation ne change pas?

**M. Smith :** Tout dépend de la nature du décret et de ses répercussions. Si l'on prend l'exemple des États-Unis et de leur programme de « remplacement total » concernant certains équipements d'origine chinoise, des délais ont été fixés, et certains petits fournisseurs ont déclaré qu'ils devaient cesser de fournir leurs services; or, dans certains cas, ils sont les seuls fournisseurs dans la collectivité.

I don't think we will see that in Canada, necessarily, with respect to the initial concern around Chinese equipment here, but we don't know what's coming down the pipe.

It's important to remember the impact not just for this bill but all bills you consider. To the extent bills add costs of doing business, all carriers' options involve cutting their costs elsewhere. We have seen that some of the largest carriers have cut their capital investment by billions of dollars in part because of regulatory overhang, or they pass on the cost to consumers.

Our industry contributes about $2 billion to $2.5 billion to the Canadian government's coffers every year in a number of different ways. We have paid about $30 billion in spectrum auction fees to the government. All we're saying is that some of that money can be used to offset the impact on Canadian consumers. This is a national priority.

**Senator Batters:** Thank you.

**Senator McNair:** Mr. Powell, you made two comments. The first one was on the risk of regulatory overlap or duplication. From what I understand, the amendment made in the other place fixes the problem. You were saying to leave it in place with respect to that.

**Mr. Powell:** Yes, that's a fair assessment.

**Senator McNair:** Mr. Smith, I want to talk about the fact that the orders for either the minister or the cabinet now require them to consider the financial impact on the affected telecommunication service providers.

Does that not give you any comfort around the concerns you're raising?

**Mr. Smith:** It gives me more comfort than if it were not there, but it just requires them to consider. It certainly doesn't necessarily contemplate helping fund some of the measures, especially for extraordinary costs. It just says it has to consider.

We have heard the minister say this is just the cost of doing business. I don't know how those balance one another out, but we have heard the Minister of Industry say that, no, this is the cost of doing business. There is no consideration of any type of funding.

Je ne pense pas que nous en arriverons nécessairement là au Canada, en ce qui concerne les inquiétudes initiales liées à l'utilisation d'équipements chinois ici, mais nous ne savons pas ce que l'avenir nous réserve.

Il est important de garder à l'esprit l'impact non seulement de cette loi-ci, mais aussi de toutes celles que vous examinez. Dans la mesure où les lois alourdissent les coûts d'exploitation, tous les transporteurs n'ont d'autre choix que de réduire leurs coûts ailleurs. Nous avons constaté que certains des plus grands transporteurs ont réduit leurs investissements en capital de plusieurs milliards de dollars, en partie en raison de la pression réglementaire, ou qu'ils refilent ces coûts aux consommateurs.

Notre secteur apporte chaque année entre 2 et 2,5 milliards de dollars aux caisses du gouvernement canadien, et ce, de différentes manières. Nous avons versé au gouvernement environ 30 milliards de dollars au titre des droits de mise aux enchères du spectre. Tout ce que nous disons, c'est qu'une partie de cet argent pourrait servir à atténuer l'impact sur les consommateurs canadiens. Il s'agit d'une priorité nationale.

**La sénatrice Batters :** Merci.

**Le sénateur McNair :** Monsieur Powell, vous avez formulé deux remarques. La première portait sur le risque de chevauchement ou de double emploi en matière de réglementation. Si j'ai bien compris, l'amendement adopté par l'autre chambre résout ce problème. Vous proposiez donc de maintenir la disposition en vigueur à cet égard.

**M. Powell :** Oui, c'est bien cela.

**Le sénateur McNair :** Monsieur Smith, je voudrais aborder le fait que pour prendre un décret, le ministre ou le Cabinet doivent désormais tenir compte des répercussions financières pour les fournisseurs de services de télécommunications concernés.

Cela ne vous rassure-t-il pas quelque peu quant aux préoccupations que vous soulevez?

**M. Smith :** Cela me rassure davantage que si cette disposition n'existait pas, mais elle les oblige simplement à examiner la question. Elle n'envisage certainement pas nécessairement de contribuer au financement de certaines de ces mesures, en particulier pour les dépenses exceptionnelles. Elle stipule simplement qu'il faut examiner la question.

Nous avons entendu le ministre dire que cela faisait simplement partie des coûts d'exploitation. Je ne sais pas comment ces éléments s'équilibrent, mais nous avons entendu le ministre de l'Industrie affirmer que non, il s'agit bien des coûts inhérents à l'activité. Aucune forme de financement n'est envisagée.

**Senator McNair:** Mr. Warnell, when you testified before us on Bill C-26, you were clear at the time that it was urgent and we should be passing this legislation. Tonight, you made the point that the continuing delay is a further risk and that the legislation itself is an enabling framework that's both flexible and adaptable, which is a good thing.

Can I assume your position remains unchanged, and that is to pass the legislation as quickly as possible?

**Mr. Warnell:** Yes. That is correct, senator. The broadness of the legislation allows it to adapt to the changing threat landscape, which is rapidly evolving, as we can all see through various news headlines and impacts on companies and countries over the past number of years.

I will reiterate that it's a strong foundation that we need to build forward from. If you look at other jurisdictions, like with the U.K.'s Cyber Security and Resilience Bill and Australia's Security of Critical Infrastructure Act and capabilities, they go a number of steps further than what Bill C-8 is contemplating. This will get us to at least a starting foundation, but, candidly, we have more work to do in this space.

**Senator McNair:** Understood. Thank you.

[*Translation*]

**Senator Youance:** My question is for Mr. Powell. You raised some concerns regarding the overlap between Bill C-8 and NERC's CIP standards. Could you outline the main areas of overlap or duplication between Bill C-8 and these standards, particularly in relation to risk management, incident reporting and auditing?

If these standards are not specifically aligned with Bill C-8, do you think that this new bill is likely to weaken rather than strengthen the resilience of electrical grids by diminishing compliance efforts?

[*English*]

**Mr. Powell:** Our concern was — and I think the amendments help address this — that we would see a secondary, parallel cybersecurity regulation created. This is a broad bill, as my colleague from Bruce Power said, but those of us in the electricity sector are very far along on our cybersecurity journey. We're on the front lines. We have been "shields up" for a long time. There is a reason why there is a North American standard for cybersecurity for critical infrastructure providers in the electricity space.

**Le sénateur McNair :** Monsieur Warnell, lorsque vous avez témoigné devant nous au sujet du projet de loi C-26, vous aviez alors clairement indiqué qu'il s'agissait d'une question urgente et que nous devions adopter cette loi. Ce soir, vous avez souligné que tout nouveau retard constituait un risque supplémentaire et que la loi elle-même offrait un cadre habilitant à la fois souple et adaptable, ce qui est une bonne chose.

Puis-je considérer que votre position reste inchangée, à savoir qu'il faudrait adopter la loi le plus rapidement possible?

**M. Warnell :** Oui. C'est exact, monsieur le sénateur. Le caractère général de cette loi lui permet de s'adapter à un environnement de menaces en constante évolution, comme nous pouvons tous le constater à travers les différents titres de l'actualité et les répercussions sur les entreprises et les pays au cours des dernières années.

Je tiens à rappeler que c'est sur des bases solides que nous devons nous appuyer pour aller de l'avant. Si l'on examine d'autres pays, comme le Royaume-Uni avec son projet de loi sur la cybersécurité et la résilience, ou l'Australie avec sa loi sur la sécurité des infrastructures critiques et les capacités qui en découlent, on constate qu'ils vont bien au-delà de ce que prévoit le projet de loi C-8. Cela nous permettra au moins de disposer d'une base de départ, mais, pour être franc, il nous reste encore du travail à accomplir dans ce domaine.

**Le sénateur McNair :** Je comprends. Merci.

[*Français*]

**La sénatrice Youance :** Ma question s'adresse à M. Powell. Vous avez soulevé certaines préoccupations ayant trait au chevauchement du projet de loi C-8 avec les normes CIP du NERC. Pouvez-vous préciser les principaux chevauchements ou doublons entre le projet de loi C-8 et ces normes, notamment en matière de gestion des risques, de signalement des incidents et d'audit?

Sans harmonisation explicite avec le projet de loi C-8, pensez-vous que ce nouveau projet de loi aura tendance à affaiblir plutôt qu'à renforcer la résilience des réseaux électriques en dispersant les efforts de conformité?

[*Traduction*]

**M. Powell :** Notre crainte était — et je pense que les amendements contribuent à y remédier — de voir se mettre en place une réglementation secondaire et parallèle en matière de cybersécurité. Il s'agit d'un projet de loi de grande envergure, comme l'a souligné mon collègue de Bruce Power, mais ceux d'entre nous qui évoluons dans le secteur de l'électricité avons déjà bien avancé dans notre démarche de cybersécurité. Nous sommes en première ligne. Cela fait longtemps que nous sommes sur la défensive. Ce n'est pas sans raison qu'il existe une norme nord-américaine en matière de cybersécurité pour

What we saw — and we heard this from the testimony from the Canada Energy Regulator, or CER, in the last panel — is that NERC has created a North American standard for participants in the bulk electric system, so people who generate and transmit power at the system level, not so much at your house. That already requires certain protections, rules and plans. It already has mandatory reporting. So we see this legislation that creates a potential parallel.

Our hope — and I think the amendment in the House of Commons allows for this — is a recognition that participation in NERC CIP satisfies the obligations that this might require. Obviously, we would also have to report to the energy regulator, but I see that's where it is.

I think it's worth noting that things are happening in parallel at the provincial level as well, including in Ontario, where they are looking at a reporting system through Lighthouse and the Independent Electricity System Operator, or IESO, as well.

**Senator Kutcher:** I have two questions. One is to Mr. Warnell, which I will ask first. Then I have one for Mr. Smith. You can think about the answer while Mr. Warnell is answering me.

Mr. Warnell, you said that the threat environment is evolving faster than anticipated, and that's what we've heard from other witnesses. Are there any things that you would add to this bill to strengthen it against that threat environment that would not delay its passage?

Mr. Smith, I just asked AI what the net profit margins were for this type of industry in Canada. This is not me; it's just AI telling me, so I don't know if it's true or not, but anyway, here I am.

The average net profit margin for telecommunications is 12.5%. Banking is 30%, so maybe we should all get into banking. Grocery and retail is 2.4%. Wholesale trucking is 6.4%.

Your industry is actually doing pretty well compared to most Canadian industries. Are you looking for full or partial government support? Can you share with us — if not today,

les fournisseurs d'infrastructures critiques dans le secteur de l'électricité.

Ce que nous avons constaté — et cela ressortait lors du témoignage de la Régie de l'énergie du Canada ou REC avec le groupe de témoins précédent —, c'est que la NERC a établi une norme nord-américaine à l'intention des acteurs du système électrique à grande échelle, c'est-à-dire des acteurs qui produisent et transportent l'électricité au niveau du système, et non pas tant au niveau de votre domicile. Cette norme prévoit déjà certaines mesures de protection, des règles et des plans. Elle impose déjà des obligations de déclaration. Nous constatons donc que ce projet de loi crée un parallèle potentiel.

Notre souhait — et je pense que l'amendement adopté à la Chambre des communes va dans ce sens — est que l'on reconnaisse que l'adhésion aux normes CIP de la NERC satisfait aux obligations que cela pourrait impliquer. Bien entendu, nous devrions également rendre compte à l'organisme de réglementation de l'énergie, mais je constate que c'est là où nous en sommes.

Je pense qu'il convient de noter que des initiatives sont également en cours au niveau provincial, notamment en Ontario, où l'on étudie la mise en place d'un système de signalement par l'intermédiaire de Lighthouse et de la Société indépendante d'exploitation du réseau d'électricité ou SIERE.

**Le sénateur Kutcher :** J'ai deux questions. La première s'adresse à M. Warnell, et je vais la poser tout de suite. Ensuite, j'en ai une pour M. Smith. Vous pouvez réfléchir à votre réponse pendant que M. Warnell me répond.

Monsieur Warnell, vous avez indiqué que la menace évolue plus rapidement que prévu, ce que d'autres témoins ont également souligné. Y a-t-il des éléments que vous ajouteriez à ce projet de loi afin de le renforcer face à cette menace, sans pour autant retarder son adoption?

Monsieur Smith, je viens de demander à l'intelligence artificielle quelles étaient les marges bénéficiaires nettes pour ce type d'industrie au Canada. Ce n'est pas moi qui le dis; c'est simplement l'intelligence artificielle qui me le dit, donc je ne sais pas si c'est vrai ou non, mais bon, voilà.

La marge bénéficiaire nette moyenne dans le secteur des télécommunications est de 12,5 %. Dans le secteur bancaire, elle est de 30 %; on pourrait donc se dire qu'il vaudrait peut-être mieux se lancer tous dans la banque. Dans l'alimentation et le commerce de détail, elle est de 2,4 %. Dans le camionnage de gros, elle est de 6,4 %.

Votre secteur se porte en réalité plutôt bien par rapport à la plupart des secteurs d'activité canadiens. Envisagez-vous de solliciter une aide publique totale ou partielle? Pourriez-vous

then later — the financial arguments so we can actually see some numbers?

**Mr. Warnell:** Thank you for your question, Senator Kutcher.

I would direct the committee to look at legislation in Australia as a good example. We are talking today about the critical cyber systems protection act, but cybersecurity doesn't exist in a vacuum.

When you think of it as an integrated total security mindset, that includes personnel security risks, physical security risks and really taking a broader resilience view to this bill, either in its current incarnation or in successive iterations. That would be my recommendation to both the Senate and House of Commons committees as we move forward in a rapidly evolving cyber-threat landscape from nation-states and global cybercriminal gangs as well as, candidly, at the hands of AI at the fingertips of an ordinary person. The threats of cyber acts are becoming much more prevalent than they ever were.

**Mr. Smith:** I will follow up in writing. I will say, first of all, remember: Don't trust AI. It's not always right.

**Senator Kutcher:** I knew you would say that.

**Mr. Smith:** There are a couple figures to keep in mind, though. I mentioned that the industry provides the federal government between $2 and $2.5 billion. That's equal to half the value of the net income of the industry itself, just to put it in relative terms.

Also, when you look at many of the operators, our largest operators have different lines of business. When you look at just the telecommunications services business, it's essentially revenue — there's no growth right now. That's partly because of demographic changes, as well as competition, where, for example, wireless prices are down by 50% since 2020.

As you add regulatory costs and you have no growth, something has to be done, and usually that means cost-cutting. So what we're looking at is, in extraordinary circumstances, having government consider — as they do by funding other industries for different things — ways to help meet those priorities.

nous présenter — si ce n'est pas aujourd'hui, alors plus tard — les arguments financiers afin que nous puissions avoir une idée concrète des chiffres?

**M. Warnell :** Merci pour votre question, sénateur Kutcher.

Je recommanderais à ce comité de s'inspirer de la législation australienne, qui constitue un bon exemple. Nous discutons aujourd'hui de la loi sur la protection des systèmes cybercritiques, mais la cybersécurité ne s'inscrit pas dans le vide.

Si l'on envisage cela comme une approche globale et intégrée de la sûreté, cela englobe les risques en matière de sûreté du personnel, les risques en matière de sûreté physique et, surtout, une vision plus large de la résilience dans le cadre de ce projet de loi, que ce soit dans sa version actuelle ou dans ses versions ultérieures. Telle serait ma recommandation aux comités du Sénat et de la Chambre des communes alors que nous évoluons dans un paysage de cybermenaces en rapide évolution, provenant d'États-nations et de gangs cybercriminels mondiaux, ainsi que, pour être franc, de l'intelligence artificielle à la portée de tout un chacun. Les menaces liées aux cyberactes sont beaucoup plus importantes qu'elles ne l'ont jamais été.

**M. Smith :** Je vous en dirai plus par écrit. Je tiens tout d'abord à vous rappeler ceci : ne faites pas confiance à l'intelligence artificielle. Elle n'a pas toujours raison.

**Le sénateur Kutcher :** Je savais que vous diriez cela.

**M. Smith :** Il y a toutefois quelques chiffres à garder à l'esprit. J'ai mentionné que ce secteur rapportait au gouvernement fédéral entre 2 et 2,5 milliards de dollars. Cela équivaut à la moitié du bénéfice net du secteur lui-même, pour donner un ordre de grandeur.

De plus, si l'on examine la situation de nombreux exploitants, on constate que nos plus grands exploitants exercent leurs activités dans différents secteurs. Si l'on se concentre uniquement sur le secteur des services de télécommunications, on constate que les revenus stagnent : il n'y a actuellement aucune croissance. Cela s'explique en partie par les changements démographiques, mais aussi par la concurrence, qui a notamment entraîné une baisse de 50 % des tarifs de la téléphonie mobile depuis 2020.

Lorsque les coûts liés à la réglementation augmentent et que la croissance est au point mort, il faut agir, ce qui se traduit généralement par des réductions de coûts. Nous envisageons donc, dans des circonstances exceptionnelles, que le gouvernement examine — comme il le fait en soutenant financièrement d'autres secteurs pour divers projets — les moyens de contribuer à la réalisation de ces priorités.

**Senator Kutcher:** I won't read what AI says about your growth. Thank you for that. It will be very helpful for us to have a better understanding of what those numbers are that you're talking about.

**Senator Yussuff:** Thank you, witnesses, for being here. Mr. Warnell, let me start with you. My compliments for what Bruce Power is doing writ large for the province, and for a very life-saving medication that you have developed, which has been a godsend for many, many families struggling with cancers who require it, and also for the supply market that you are also involved in.

Mr. Powell, I have a question that is a bit challenging for me. Voluntary reporting is to try to understand what is going on and how we can make the system more resilient. I understand your members do that, and, obviously, there is value to it. It helps the sector, but it also helps, writ large, with how we could prevent cybersecurity from damaging one part of the economy of this country.

It may be, from time to time, that some of that may be necessary, but we also need to improve the regulatory regime to ensure that this is consistent across all regions and geographies across the country. Why would you be against that? I don't get it.

**Mr. Powell:** We are not against mandatory reporting. The goal is a protection for information that is shared outside of the regulatory context.

**Senator Yussuff:** You're the only witness who has come here who doesn't recognize that the voluntary sharing of information is a good thing, however it may improve the system.

**Mr. Powell:** What we're hoping to see is that information, when it's shared on a voluntary, confidential basis — with, say, the Canadian Centre for Cyber Security — remains on a sort of voluntary and confidential basis.

That's how it works with the most comparable organization. We have talked a little bit about NERC CIP. The Canada Energy Regulator witness from earlier talked about how they require participants that are CER regulated in the international power line space to adhere to NERC CIP. They have an information-sharing system where, again, when information is provided voluntarily, it is protected from being shared with regulators. That's really what we're focused on, not the stuff that would meet the requirement under the act or a future regulation for mandatory reporting or sharing. It is more knowing that you can keep that free flow of information going on a voluntary basis without worrying or having legal concerns that doing so could

**Le sénateur Kutcher :** Je ne vais pas lire ce que l'intelligence artificielle dit à propos de votre croissance. Merci de votre prudence. Cela nous sera très utile pour mieux comprendre de quels chiffres vous parlez.

**Le sénateur Yussuff :** Merci à vous, mesdames et messieurs les témoins, d'être ici. Monsieur Warnell, je commencerai par vous. Je tiens à vous féliciter pour l'action remarquable menée par Bruce Power en général au service de la province, ainsi que pour le traitement vital que vous avez mis au point, qui a été une véritable bénédiction pour de très nombreuses familles confrontées au cancer et qui en ont besoin, et enfin pour le marché de l'offre auquel vous participez.

Monsieur Powell, il y a une chose que je ne comprends pas très bien. Le signalement volontaire vise à comprendre ce qui se passe et comment nous pouvons rendre le système plus résilient. Je sais que vos membres le font, et cela présente évidemment un intérêt. Cela aide le secteur, mais cela contribue aussi, en général, à déterminer comment nous pourrions empêcher que la cybersécurité ne porte préjudice à une partie de l'économie de ce pays.

Il se peut que, de temps à autre, certaines de ces mesures s'avèrent nécessaires, mais nous devons également améliorer le cadre réglementaire afin de garantir sa cohérence dans toutes les régions et zones géographiques du pays. Pourquoi seriez-vous contre cela? Je ne comprends pas.

**M. Powell :** Nous ne sommes pas opposés à l'obligation de signalement. L'objectif est de protéger les informations qui sont communiquées en dehors du cadre réglementaire.

**Le sénateur Yussuff :** Vous êtes le seul témoin qui se soit présenté ici à ne pas reconnaître que l'échange volontaire de renseignements est une bonne chose, alors que cela peut permettre d'améliorer le système.

**M. Powell :** Ce que nous espérons, c'est que ces informations, lorsqu'elles sont communiquées à titre volontaire et confidentiel — par exemple au Centre canadien pour la cybersécurité —, continuent d'être traitées sur cette base volontaire et confidentielle.

C'est ainsi que cela fonctionne au sein de l'organisme le plus comparable. Nous avons brièvement évoqué les normes CIP de la NERC. Le témoin de la Régie de l'énergie du Canada, qui s'est exprimé tout à l'heure, a expliqué qu'ils exigeaient des participants réglementés par la REC dans le domaine des lignes internationales qu'ils se conforment à ces normes. Ils disposent d'un système d'échange de renseignements dans lequel, là encore, lorsque les informations sont fournies volontairement, elles sont protégées contre toute divulgation aux organismes de réglementation. C'est vraiment ce sur quoi nous nous concentrons, et non pas sur les éléments qui répondraient aux exigences de la loi ou d'une future réglementation en

add to some risk in the future for information being shared. Your information is yours.

**Senator Yussuff:** My point is voluntary information sharing about cybersecurity is fundamental to how we can improve the system writ large.

**Mr. Powell:** Yes.

**Senator Yussuff:** As legislators and regulators, there is a greater authority for us to protect the nation. How do we balance that when sometimes we may see a weakness? If the system is vulnerable, we want to make sure we can do whatever is necessary to help protect the system. It is for your self-interest, but it's also for the consumers and Canadians in general, whom we serve.

**Mr. Powell:** I would say our members have had a very good track record of allowing information to be shared within the sector. They participate in information-sharing systems through Electricity Canada and our partner organizations, but also with organizations like Lighthouse and the NERC E-ISAC and with the Canadian Centre for Cyber Security.

The question is this: How do we make sure we continue to incent that information sharing on our side? Nothing stops the government from talking to us.

And when there are regulatory reporting requirements, that's absolutely fine. It's just, outside that non-emergency space, making sure that the conversation can continue.

**Senator Yussuff:** Thank you.

**Senator Dasko:** My question is for Mr. Warnell. You're the only representative of a company here today. You have spoken favourably about the bill. What will Bruce Power look like after this bill is implemented? Will it look different? If so, how? In what ways?

**Mr. Warnell:** Thank you for your question, Senator Dasko. Candidly, the nuclear industry in Canada has been regulated, from a cybersecurity standpoint — formally, as a discrete domain — since 2014. We do not anticipate a large delta before or after the bill passes.

matière de déclaration ou d'échange de renseignements obligatoires. Il s'agit davantage de savoir que vous pouvez maintenir cette libre circulation de l'information sur une base volontaire sans vous inquiéter ou avoir de préoccupations juridiques quant au fait que cela pourrait accroître le risque futur lié à l'échange de renseignements. Vos informations vous appartiennent.

**Le sénateur Yussuff :** Ce que je veux dire, c'est que l'échange volontaire de renseignements sur la cybersécurité est essentiel pour améliorer le système en général.

**M. Powell :** Oui.

**Le sénateur Yussuff :** En tant que législateurs et organismes de réglementation, nous disposons d'un pouvoir accru pour protéger la nation. Comment trouver le juste équilibre lorsque nous constatons parfois une faille? Si le système présente des vulnérabilités, nous voulons nous assurer de pouvoir prendre toutes les mesures nécessaires pour contribuer à le protéger. C'est dans votre propre intérêt, mais c'est aussi dans celui des consommateurs et des Canadiens en général, que nous servons.

**M. Powell :** Je dirais que nos membres ont toujours fait preuve d'une grande ouverture en matière d'échange de renseignements au sein du secteur. Ils participent à des systèmes d'échange de renseignements par l'intermédiaire d'Électricité Canada et de nos organisations partenaires, mais aussi avec des organismes tels que Lighthouse et l'E-ISAC de la NERC, ainsi qu'avec le Centre canadien pour la cybersécurité.

La question est la suivante : comment pouvons-nous nous assurer de continuer à offrir une incitation à l'échange de renseignements de notre côté? Rien n'empêche le gouvernement de communiquer avec nous.

Lorsqu'il y a des exigences en matière de rapports, cela ne pose aucun problème. Il s'agit simplement, en dehors du contexte d'urgence, de veiller à ce que le dialogue puisse se poursuivre.

**Le sénateur Yussuff :** Merci.

**La sénatrice Dasko :** Ma question s'adresse à M. Warnell. Vous êtes le seul représentant d'une entreprise présent ici aujourd'hui. Vous vous êtes exprimé favorablement au sujet de ce projet de loi. À quoi ressemblera Bruce Power une fois ce projet de loi mis en œuvre? Y aura-t-il des changements? Si oui, lesquels? De quelle manière?

**M. Warnell :** Merci pour votre question, sénatrice Dasko. En toute franchise, l'industrie nucléaire canadienne fait l'objet d'une réglementation en matière de cybersécurité — officiellement, en tant que domaine distinct — depuis 2014. Nous ne prévoyons pas de changement significatif avant ou après l'adoption du projet de loi.

We are already an industry that puts safety first in all aspects, and we equate cybersecurity to safe operations and to reliable operations. Candidly, we don't anticipate a material change in our posture, our thinking or our actions.

We are probably also here to advocate that moving forward on the bill is important because we recognize that we're not an island unto ourselves. We operate within a system of systems. We are integrated with the electricity distribution organizations.

We participate in NERC CIP in collaboration with our partners in broader energy. We drive for maturity across broader energy organizations through things like the Energy Security Technical Advisory Committee, or E-STAC. I would say our existing mature capabilities can also be used to help lift all boats.

That broader resilience for Canada, and the energy sector overall, can be improved because it is an ever-increasingly challenging and dangerous time in very unpredictable waters.

**Senator Dasko:** So the regulator won't be able to throw anything at you?

**Mr. Warnell:** Absolutely they can. The existing regulator is the Canadian Nuclear Safety Commission. They will absolutely potentially have new powers, but we already have the requirements for cybersecurity programs. We are regularly audited through the regulator as well as other partners. We participate internationally in information-sharing domains with other nuclear operators and other critical infrastructure partners to also drive for excellence in our operations, because excellence in cyber means safe, reliable operations.

To my point, I don't see — or we don't anticipate — a major delta. However, again, one of the differences with what we do in nuclear is we work in collaboration with industry, the operators and the regulator, through the Canadian Standards Association — much like the Canadian Energy Regulator — to co-create the standards that we're held to.

It's known as the CSA N290.7 standard, which is cybersecurity for nuclear facilities. We already do that; we've

Notre secteur accorde déjà la priorité à la sécurité dans tous les domaines, et nous considérons que la cybersécurité est indissociable de la sécurité et de la fiabilité de nos opérations. Pour être franc, nous ne prévoyons pas de changement significatif dans notre approche, notre raisonnement ou nos actions.

Nous sommes sans doute également ici pour souligner qu'il est important d'aller de l'avant avec ce projet de loi, car nous sommes conscients que nous ne sommes pas une île isolée. Nous évoluons au sein d'un système de systèmes. Nous sommes étroitement liés aux organismes de distribution d'électricité.

Nous adhérons aux normes CIP de la NERC en collaboration avec nos partenaires du secteur énergétique au sens large. Nous œuvrons à la maturation des organisations de ce secteur par le biais d'initiatives telles que le Comité consultatif technique sur la sécurité énergétique ou E-STAC. Je dirais que nos capacités déjà bien établies peuvent également servir à faire progresser l'ensemble du secteur.

La résilience globale du Canada, ainsi que celle du secteur énergétique dans son ensemble, peut être renforcée, car nous traversons une période de plus en plus difficile et périlleuse, dans un contexte extrêmement imprévisible.

**La sénatrice Dasko :** Donc, l'organisme de réglementation n'aura rien à vous imposer?

**M. Warnell :** Il en aura certainement la possibilité. L'organisme de réglementation actuel est la Commission canadienne de sûreté nucléaire. Il est tout à fait possible qu'elle se voie attribuer de nouveaux pouvoirs, mais nous avons déjà les exigences relatives aux programmes de cybersécurité. Nous faisons régulièrement l'objet d'audits menés par l'organisme de réglementation ainsi que par d'autres partenaires. Nous participons à des initiatives internationales d'échange de renseignements avec d'autres exploitants nucléaires et d'autres partenaires du secteur des infrastructures essentielles afin de viser l'excellence dans nos opérations, car l'excellence en matière de cybersécurité est synonyme d'opérations sûres et fiables.

Pour en venir au fait, je ne vois pas — ou nous ne prévoyons pas — de différence majeure. Cependant, encore une fois, l'une des particularités de notre approche dans le domaine nucléaire réside dans le fait que nous travaillons en collaboration avec l'industrie, les exploitants et l'organisme de réglementation, par l'intermédiaire de l'Association canadienne de normalisation — tout comme la Régie de l'énergie du Canada — afin d'élaborer conjointement les normes auxquelles nous sommes tenus de nous conformer.

Il s'agit de la norme CSA N290.7, qui porte sur la cybersécurité des installations nucléaires. Nous appliquons déjà

been doing it for over a decade. We expect and continue to deliver iterations on excellence under those frameworks.

**Senator Dasko:** Okay, thank you. I have another question for you.

You've mentioned the threat actors; more specifically, you've mentioned criminal organizations and state actors.

I asked the minister a question at the beginning. He was a little reluctant to say much about it. Can you tell me any more about these threats? Who are the criminal organizations? Where do they reside? Where are they from? And what about the state actors? Are there any state actors who are actually trying to perpetrate crimes on nuclear in Canada?

**Mr. Warnell:** I'll reference what is already in the public domain.

**Senator Dasko:** Yes, for sure.

**Mr. Warnell:** I know the minister said earlier they can go deeper in a more classified scenario.

Especially over the past two to three years, there has been declassification of information related to known threat actors, including China, Russia and others around the world, who are known to be and are demonstrated to have been actively pre-positioning in critical infrastructure sectors, including energy and telecommunications.

You might have heard reference to language like "Volt Typhoon" or "Salt Typhoon." Those sorts of threat actor names are typically associated with Chinese state actors with the explicit intention of being in those networks to cause disruption or delay, should it be required.

It doesn't mean it's escalated to that impact, but the possibility is there. Again, this is work that would have been very much not in the public eye many years ago. But with the urgency and the impact, obviously, our intelligence partners in Canada, with our allies in Five Eyes and other nations around the world, have been able to bring that down, declassify it and make it part of the public discourse and conversation.

It is real. It is no longer hypothetical. We're not just paranoid security professionals. It is happening, and we need to continue to mature our respective capabilities to build resilience.

cette norme; nous le faisons depuis plus de 10 ans. Nous nous attendons à ce que ces cadres nous permettent de continuer à améliorer sans cesse l'excellence de nos pratiques.

**La sénatrice Dasko :** D'accord, merci. J'ai une autre question à vous poser.

Vous avez évoqué les acteurs malveillants; plus précisément, vous avez mentionné les organisations criminelles et les acteurs étatiques.

J'ai posé une question au ministre au début. Il s'est montré un peu réticent à s'étendre sur le sujet. Pouvez-vous m'en dire davantage sur ces menaces? De quelles organisations criminelles s'agit-il? Où se trouvent-elles? D'où viennent-elles? Et qu'en est-il des acteurs étatiques? Y a-t-il des acteurs étatiques qui tentent réellement de commettre des crimes contre des installations nucléaires au Canada?

**M. Warnell :** Je vais parler de ce qui est déjà du domaine public.

**La sénatrice Dasko :** Oui, bien sûr.

**M. Warnell :** Je sais que le ministre a déclaré plus tôt qu'ils pouvaient aller plus loin dans un contexte plus confidentiel.

Ces deux ou trois dernières années en particulier, des informations ont été rendues publiques concernant des acteurs malveillants connus, notamment la Chine, la Russie et d'autres pays à travers le monde, dont on sait qu'ils ont réalisé un déploiement actif dans des secteurs d'infrastructures critiques, tels que l'énergie et les télécommunications, et dont il a été démontré qu'ils l'ont fait.

Vous avez peut-être entendu parler de groupes tels que « Volt Typhoon » ou « Salt Typhoon ». Ce genre de noms désignant des acteurs malveillants est généralement associé à des acteurs étatiques chinois dont l'intention explicite est de s'infiltrer dans ces réseaux afin de provoquer des perturbations ou des retards, si nécessaire.

Cela ne signifie pas que la situation a atteint un tel niveau d'impact, mais cette possibilité existe bel et bien. Encore une fois, il s'agit d'un travail qui, il y a de nombreuses années, n'aurait certainement pas été porté à l'attention du public. Mais compte tenu de l'urgence et de l'ampleur des enjeux, nos partenaires du renseignement au Canada, ainsi que nos alliés du Groupe des cinq et d'autres pays à travers le monde, ont manifestement réussi à mettre fin à cette situation, à déclassifier ces informations et à les intégrer dans le débat public.

C'est une réalité. Ce n'est plus une hypothèse. Nous ne sommes pas simplement des professionnels de la sûreté paranoïaques. Cela se produit bel et bien, et nous devons continuer à renforcer nos capacités respectives afin de développer notre résilience.

**Senator Dasko:** Are the criminal organizations looking for money, information or —

**Mr. Warnell:** All of the above.

**The Chair:** Thank you, Mr. Warnell. We appreciate that.

**Senator Al Zaibak:** I have two questions, actually, directed to Mr. Powell and Mr. Warnell.

From your perspectives, what are the most immediate cyber vulnerabilities in Canada's energy grid, particularly in the context of geopolitical tensions?

How prepared are your systems to defend against AI-driven cyberattacks, such as automated disruption of control systems? Mr. Powell?

**Mr. Powell:** Building on what Mr. Warnell said, there are identified threats that we have heard about from the Canadian Centre for Cyber Security in the National Cyber Threat Assessments. There are nation-state actors like China and Russia, and Iran has been on that list as well. On top of that, there are threats from criminal organizations, who may or may not be state affiliated. This is all in the public record.

**Senator Al Zaibak:** I'm sorry, just a correction — I'm asking what the vulnerabilities are, not who the threats are.

**Mr. Powell:** Part of it is that you don't know what you don't know. We have an increasingly connected system that works to be more integrated and is technologically aware.

There's not a list that I'm given — as an association person — of the specific threats that they may see, but I do think that this is an area where there are constant challenges, both at the operational level and at the IT level. It's something that requires constant vigilance.

No one knows where their next threat is coming from. We've seen conversations in the last few weeks around AI tools, like Mythos, that may change the game and present zero-day vulnerabilities much sooner than we would have seen. That requires a level of vigilance that we haven't seen before and is accelerating the risks that are coming at us. As Mr. Warnell said, the world is getting more dangerous faster, and we have to keep up.

**Mr. Warnell:** Senator Al Zaibak, I don't know that this is the right forum to talk about where vulnerabilities directly exist, given that it is a public forum. There are follow-up conversations we can have.

**La sénatrice Dasko :** Les organisations criminelles recherchent-elles de l'argent, des informations ou...

**M. Warnell :** Tout ce qui précède.

**La présidente :** Merci, Monsieur Warnell. Nous comprenons cela.

**Le sénateur Al Zaibak :** J'ai, en fait, deux questions à poser à M. Powell et à M. Warnell.

Selon vous, quelles sont les vulnérabilités cybernétiques les plus pressantes du réseau énergétique canadien, notamment dans le contexte des tensions géopolitiques?

Dans quelle mesure vos systèmes sont-ils prêts à se défendre contre les cyberattaques basées sur l'IA, telles que la perturbation automatisée des systèmes de contrôle? Monsieur Powell?

**M. Powell :** Pour faire suite à ce qu'a dit M. Warnell, il existe des menaces identifiées dont nous avons pris connaissance par l'intermédiaire du Centre canadien pour la cybersécurité dans le cadre des évaluations nationales des menaces cybernétiques. Il s'agit d'acteurs étatiques tels que la Chine et la Russie, et l'Iran figure également sur cette liste. À cela s'ajoutent les menaces émanant d'organisations criminelles, qui peuvent ou non être affiliées à des États. Tout cela est de notoriété publique.

**Le sénateur Al Zaibak :** Excusez-moi, juste une petite précision : je veux savoir quelles sont les vulnérabilités, et non pas qui sont les acteurs malveillants.

**M. Powell :** Cela tient en partie au fait que l'on ignore ce que l'on ignore. Nous disposons d'un système de plus en plus interconnecté, qui tend à être plus intégré et qui est en veille technologique.

En tant que responsable d'association, on ne me fournit pas de liste des menaces spécifiques auxquelles nous pourrions être confrontés, mais je pense sincèrement qu'il s'agit d'un domaine où les défis sont permanents, tant sur le plan opérationnel que sur le plan TI. C'est un sujet qui exige une vigilance constante.

Personne ne sait d'où viendra la prochaine menace. Ces dernières semaines, nous avons assisté à des discussions concernant des outils d'IA, tels que Mythos, qui pourraient changer la donne et révéler des vulnérabilités de type « jour zéro » bien plus tôt que nous ne l'aurions imaginé. Cela exige un niveau de vigilance sans précédent et accélère l'intensification des risques auxquels nous sommes confrontés. Comme l'a dit M. Warnell, le monde devient de plus en plus dangereux à un rythme effréné, et nous devons suivre le mouvement.

**M. Warnell :** Sénateur Al Zaibak, je ne suis pas sûr que ce soit l'endroit approprié pour évoquer les failles existantes, étant donné qu'il s'agit d'un forum public. Nous pourrons en discuter plus en détail ultérieurement.

However, you can look at events that have already happened in the public eye. You can look at the Colonial Pipeline disruption in the United States a number of years ago. That had nothing to do with actually impairing their operational systems that deliver oil and gas. It was a ransomware event that took out their business systems, and, out of an abundance of caution, the operator shut down their pipeline impacts, which then impacted millions of Americans on the eastern seaboard who were unable to get energy. Those have happened, and those are relatively, I would say, immature attacks.

If you can broaden that to what the possibility is, there are some significant opportunities for us to uplift collective resilience. And this bill can start to lay that foundation to really drive that integrated resilience improvement.

**Senator Al Zaibak:** Thank you so much.

**The Chair:** Thank you very much. This concludes our time and our questions this evening, but I want to thank Mr. Powell, Mr. Warnell and Mr. Smith for taking the time to meet with us today. We appreciate your testimony as we consider this bill. I also want to acknowledge that all three of you represent really significant and large groups of employees, and that's also an appropriate way for us to finish this evening, so we do appreciate that acute testimony.

Just before we finish, I would like to turn the microphone to Senator Kutcher.

**Senator Kutcher:** Thank you very much, chair, and I realize we're still in public.

However, I just want to raise for our committee — and we all have shared this with each other, personally — our awareness of the stellar work that Senator Yussuff has done as chair of this committee over his tenure. When he came to this job, he said he wouldn't keep it for a lifetime. I told him that was probably true, but he meant to do it for a short period of time.

I think we would all agree that he has guided us fairly, reasonably, respectfully and responsibly. He's been aided by the members of the steering committee — he has spoken to me about all the work that the steering committee has done — and also by Ericka Paajanen, our clerk, who goes unsung as a heroine, but she certainly is one. I just want the record to show that the members of this committee recognize and appreciate Senator Yussuff's contribution to the running of this group. Thank you, Senator Yussuff.

**Hon. Senators:** Hear, hear!

Vous pouvez toutefois vous pencher sur des événements qui se sont déjà produits et qui ont retenu l'attention du grand public. Prenez, par exemple, la perturbation du pipeline Colonial aux États-Unis, il y a quelques années. Cela n'avait rien à voir avec une atteinte effective à ses systèmes opérationnels chargés de l'acheminement du pétrole et du gaz. Il s'agissait d'une attaque par rançongiciel qui a paralysé les systèmes d'entreprise et, par excès de prudence, l'exploitant a fermé ses pipelines, ce qui a ensuite eu des répercussions sur des millions d'Américaines et d'Américains de la côte Est qui se sont retrouvés privés d'énergie. De tels incidents se sont produits, et il s'agit là, je dirais, d'attaques relativement rudimentaires.

Si l'on élargit cette réflexion pour envisager toutes les possibilités, il existe des opportunités significatives qui nous permettront de renforcer notre résilience collective. Et ce projet de loi peut commencer à jeter les bases nécessaires pour réellement favoriser une amélioration intégrée de la résilience.

**Le sénateur Al Zaibak :** Merci beaucoup.

**La présidente :** Merci beaucoup. Cela conclut notre réunion et nos questions de ce soir, mais je tiens à remercier M. Powell, M. Warnell et M. Smith d'avoir pris le temps de nous rencontrer aujourd'hui. Vos témoignages nous sont précieux alors que nous examinons ce projet de loi. Je tiens également à souligner que vous représentez tous les trois des groupes très importants d'employées, et c'est là une manière tout à fait appropriée de clore cette soirée; nous vous sommes donc reconnaissants de ces témoignages pertinents.

Avant de conclure, j'aimerais céder la parole au sénateur Kutcher.

**Le sénateur Kutcher :** Merci beaucoup, Madame la présidente, et je suis conscient que nous sommes toujours en séance publique.

Je tiens toutefois à souligner, au nom de notre comité — et nous en avons tous déjà parlé entre nous, à titre personnel —, l'excellent travail accompli par le sénateur Yussuff en tant que président de ce comité tout au long de son mandat. Lorsqu'il a pris ses fonctions, il a déclaré qu'il ne resterait pas à ce poste toute sa vie. Je lui ai répondu que c'était sans doute vrai, mais qu'il comptait le faire pour une courte période.

Je pense que nous sommes tous d'accord pour dire qu'il nous a guidés avec équité, raison, respect et le sens des responsabilités. Il a été secondé par les membres du comité directeur — il m'a fait part de tout le travail accompli par ce comité — ainsi que par Ericka Paajanen, notre greffière, qui est une héroïne méconnue, mais qui en est bel et bien une. Je tiens simplement à ce que le document mentionne que les membres du comité reconnaissent et apprécient la contribution du sénateur Yussuff au bon fonctionnement de ce groupe. Merci, sénateur Yussuff.

**Des voix :** Bravo!

**Senator Yussuff:** I'm not going to say much except thank you, Stan, for your kind words. If I knew leaving this committee would receive this kind of applause, I would have done so sooner.

Let me quickly say thanks to my wonderful staff for helping me: Ceanray Harris-Read, who has been here, and Joel Bowen from time to time. I also want to thank Ericka. She made me laugh quite often and reminded me of the silliness of our committee members, even though we didn't share that with them. Just kidding.

I want to thank Anne-Marie Therrien-Tremblay and Ariel Shapiro for their wonderful guidance as analysts for the committee. I want to thank the technical people for making the meetings run seamlessly. Equally, I want to thank the steering committee members and this entire committee. There are few committees I have worked with where we have never had any tension in steering. I can say that without a doubt. While we do argue, we always come to a conclusion about the greater good of the work we're doing here.

I thank Senator Carignan for his friendship and kindness. I want to thank Senator Cardozo for his friendship and kindness, and also our deputy chair, Senator Al Zaibak, for his work. I've learned a lot from being in the chair, but I have also learned a lot from sitting here. While I'm not in the chair, I will continue to sit here and participate. As with everything else we do in this wonderful place, the Senate, sometimes we have to make space for others. I'm glad to have made space for my colleagues, but equally, I'm thrilled. People ask why I am leaving. I'm leaving because I think I've done my job and it's time to give others a chance to succeed. I want to wish my colleague all the best in her responsibilities. All of us will do our best to support you.

**The Chair:** Thank you very much, and thank you to the panel for joining us for this part of our meeting.

Senator Kutcher and Senator Yussuff, thank you. This concludes our meeting for today. Our next meeting will take place on Monday, May 25, at our usual time: four o'clock. We will continue our consideration of Bill C-8.

With that, I wish you a very good evening. Thank you.

(The committee adjourned.)

**Le sénateur Yussuff :** Je ne vais pas m'étendre sur le sujet, mais je tiens simplement à vous remercier, monsieur Kutcher, pour vos aimables paroles. Si j'avais su que mon départ de ce comité susciterait un tel applaudissement, je l'aurais fait plus tôt.

Je tiens à remercier rapidement ma formidable équipe pour son aide : Ceanray Harris-Read, qui a été présente tout au long du projet, et Joel Bowen, qui nous a aidés de temps à autre. Je tiens également à remercier Mme Paajanen. Elle m'a souvent fait rire et m'a rappelé à quel point les membres de notre comité pouvaient être loufoques, même si nous ne le leur avons pas dit. Je plaisante.

Je tiens à remercier Anne-Marie Therrien-Tremblay et Ariel Shapiro pour leurs précieux conseils en tant qu'analystes au sein du comité. Je tiens également à remercier l'équipe technique d'avoir assuré le bon déroulement des réunions. De même, je tiens à remercier les membres du comité directeur ainsi que l'ensemble de ce comité. Rares sont les comités avec lesquels j'ai travaillé où nous n'avons jamais connu de tensions au sein du comité directeur. Je peux l'affirmer sans l'ombre d'un doute. Même si nous avons parfois des désaccords, nous parvenons toujours à une conclusion qui sert l'intérêt supérieur du travail que nous accomplissons ici.

Je remercie le sénateur Carignan pour son amitié et sa gentillesse. Je tiens à remercier le sénateur Cardozo pour son amitié et sa gentillesse, ainsi que notre vice-président, le sénateur Al Zaibak, pour son travail. J'ai beaucoup appris en occupant le poste de président, mais j'ai également beaucoup appris en siégeant ici. Même si je ne suis plus au poste de président, je continuerai à siéger ici et à participer. Comme pour tout ce que nous faisons dans ce merveilleux endroit qu'est le Sénat, nous devons parfois faire de la place aux autres. Je suis heureux d'avoir cédé la place à mes collègues, et j'en suis ravi. Les gens me demandent pourquoi je pars. Je pars parce que je pense avoir fait mon travail et qu'il est temps de donner à d'autres la chance de réussir. Je souhaite à ma collègue beaucoup de succès dans ses nouvelles responsabilités. Nous ferons tous de notre mieux pour vous soutenir.

**La présidente :** Merci beaucoup, et merci aux témoins de s'être joints à nous pour cette partie de notre réunion.

Messieurs les sénateurs Kutcher et Yussuff, merci. Cela conclut notre réunion d'aujourd'hui. Notre prochaine réunion aura lieu le lundi 25 mai, à l'heure habituelle, soit 16 heures. Nous poursuivrons l'examen du projet de loi C-8.

Sur ce, je vous souhaite une très bonne soirée. Merci.

(La séance est levée.)