EVIDENCE

OTTAWA, Monday, November 4, 2024

The Standing Senate Committee on National Security, Defence and Veterans Affairs met with videoconference this day at 4:01 p.m. [ET] to study Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.

Senator Tony Dean (*Chair*) in the chair.

[*English*]

The Chair: Good afternoon, colleagues, before we begin, I would like to ask senators and other in-person participants to consult the cards on the table for guidelines to prevent audio feedback incidents. Thank you all for your cooperation.

Colleagues, before we begin today, I would like to take a moment to acknowledge our dear friend and colleague, the Honourable Murray Sinclair, who passed away this morning, as many of you know.

Senator Sinclair represented Manitoba in the Senate from 2016 to 2021. He had a highly distinguished law career prior to his appointment here, notably serving as the first Indigenous judge appointed in Manitoba. Senator Sinclair also served as the chair of the Truth and Reconciliation Commission, later receiving awards, including the Meritorious Service Cross, and the Order of Canada for his work on the commission.

Senator Sinclair, as you know, was dedicated to the community in many ways and was a force to be reckoned with in the Senate. He will be dearly missed by all of us and many beyond this place. I invite you now to share a moment of silence in his memory.

Thank you, colleagues.

Welcome to this meeting of the Standing Senate Committee on National Security, Defence, and Veterans Affairs. I'm Tony Dean, senator from Ontario, and I chair the committee. I'm joined today by my fellow committee members whom I welcome to introduce themselves, beginning with the deputy chair.

[*Translation*]

Senator Dagenais: Jean-Guy Dagenais from Quebec.

[*English*]

Senator Richards: David Richards from New Brunswick.

TÉMOIGNAGES

OTTAWA, le lundi 4 novembre 2024

Le Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants se réunit aujourd'hui à 16 h 1 (HE), avec vidéoconférence, pour étudier le projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois

Le sénateur Tony Dean (*président*) occupe le fauteuil.

[*Traduction*]

Le président : Bon après-midi, chers collègues. Avant de commencer, j'invite les sénateurs et les autres participants qui sont sur place à consulter les fiches disposées sur la table pour prendre connaissance des directives à respecter pour prévenir les incidents de rétroaction acoustique. Merci à vous tous de votre collaboration.

Chers collègues, avant toutes choses, je vais prendre un moment pour saluer la mémoire de notre cher ami et collègue, l'honorable Murray Sinclair, qui est décédé ce matin, comme bon nombre d'entre vous le savent.

Le sénateur Sinclair a représenté le Manitoba au Sénat de 2016 à 2021. Il a mené une brillante carrière en droit avant sa nomination au Sénat, notamment à titre de premier juge autochtone nommé au Manitoba. Le sénateur Sinclair a également présidé la Commission de vérité et réconciliation, et reçu des distinctions, notamment la Croix du service méritoire et l'Ordre du Canada, pour son travail à la commission.

Comme vous le savez, le sénateur Sinclair était dévoué à la collectivité à bien des égards et il a été une force remarquable au Sénat. Il nous manquera beaucoup à nous tous ainsi qu'à bien d'autres personnes. Je vous invite maintenant à observer un moment de silence en sa mémoire.

Merci, chers collègues.

Bienvenue à cette séance du Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants. Je suis Tony Dean, sénateur de l'Ontario, et je préside le comité. Je suis accompagné aujourd'hui de mes collègues du comité, que j'invite à se présenter, en commençant par le vice-président.

[*Français*]

Le sénateur Dagenais : Jean-Guy Dagenais, du Québec.

[*Traduction*]

Le sénateur Richards : David Richards, du Nouveau-Brunswick.

Senator M. Deacon: Welcome, Marty Deacon from Ontario.

Senator Cardozo: Andrew Cardozo, Ontario.

Senator Dasko: Donna Dasko, senator from Ontario.

Senator LaBoucane-Benson: Patti LaBoucane-Benson from Treaty 6 territory, Alberta.

Senator Boehm: Peter Boehm, Ontario.

Senator McNair: Welcome, John McNair, senator from New Brunswick.

Senator Yussuff: Hassan Yussuff, Ontario.

Senator Batters: Denise Batters. I'm a senator from Saskatchewan.

The Chair: Thank you colleagues. To my left is the committee's clerk, Ericka Paajanen, and to my right, or Library of Parliament analysts, Ms. Anne-Marie Therrien-Tremblay and Mr. Ariel Shapiro.

We continue our study of Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts. We're going to hear from three panels of witnesses today who will share their insights on this bill.

In this first panel, I'm pleased to welcome here in the room, Jennifer Quaid, Executive Director of the Canadian Cyber Threat Exchange, Kate Robertson, Senior Research Associate, Citizen Lab at the University of Toronto. And by video conference, Aaron Shull, Managing Director and General Counsel at the Centre for International Governance Innovation. Thank you all for joining us today.

We now invite you to provide your opening remarks, which will be followed by questions from our members. I remind you that you each have five minutes to present, and we begin today with Ms. Jennifer Quaid. Please proceed whenever you're ready.

Jennifer Quaid, Executive Director, Canadian Cyber Threat Exchange: Good afternoon, Mr. Chair, and thank you for inviting me to participate in this critically important process.

Before I begin, I would like to clarify that my comments today will be limited to Part 2 of Bill C-26, the Critical Cyber Systems Protection Act. I'm honoured to be here representing the Canadian Cyber Threat Exchange, or CCTX, an organization created by Canadian companies to provide a safe environment for members to share cyber threat information and build cyber

La sénatrice M. Deacon : Bienvenue, Marty Deacon, de l'Ontario.

Le sénateur Cardozo : Andrew Cardozo, de l'Ontario.

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

La sénatrice LaBoucane-Benson : Patti LaBoucane-Benson, du territoire du Traité n^{o} 6, en Alberta.

Le sénateur Boehm : Peter Boehm, de l'Ontario.

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

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

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

Le président : Merci, chers collègues. À ma gauche se trouve la greffière du comité, Ericka Paajanen, et à ma droite, prennent place les analystes de la Bibliothèque du Parlement, Mme Anne-Marie Therrien-Tremblay et M. Ariel Shapiro.

Nous poursuivons notre étude du projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois. Nous entendrons aujourd'hui trois groupes de témoins qui nous présenteront leur point de vue sur le projet de loi.

Voici le premier groupe de témoins. J'ai le plaisir d'accueillir Jennifer Quaid, directrice générale d'Échange canadien sur les menaces cybernétiques, et Kate Robertson, associée de recherche principale au Citizen Lab de l'Université de Toronto. Et par vidéoconférence, comparaît Aaron Shull, directeur général et avocat général du Centre pour l'innovation dans la gouvernance internationale. Merci à vous tous de vous joindre à nous aujourd'hui.

Nous vous invitons maintenant à faire votre déclaration liminaire, qui sera suivie des questions des membres du comité. Je vous rappelle que vous avez chacun cinq minutes pour faire votre exposé. Nous allons commencer par Mme Jennifer Quaid. Veuillez commencer dès que vous serez prête.

Jennifer Quaid, directrice générale, Échange canadien de menaces cybernétiques : Bonjour, monsieur le président, et merci de m'avoir invitée à participer à cette étude d'une importance cruciale.

Avant de commencer, je précise que mes observations se limiteront à la partie 2 du projet de loi C-26, la Loi sur la protection des cybersystèmes essentiels. Je suis honorée d'être là pour représenter Échange canadien de menaces cybernétiques, ou ECMC. Cette organisation a été créée par des entreprises canadiennes pour offrir un environnement sécuritaire où les

resilience by collaborating to understand threats and share best practices and ideas, to prevent successful attacks and the corresponding need to report. In a world where it's not if but when an organization will be the target of an attack, the goal is to build resilience, not just in our critical infrastructure, but in all organizations to create a stronger economic environment for all.

With 190 members representing 15 sectors and more than 1.5 million employees, many of our members represent the sectors impacted by this legislation, while others may cut their supply chain, many of whom are small and medium-sized businesses, like so much of the Canadian economy.

There's no question that this bill will strengthen Canada's cybersecurity posture. It creates that common level of security for critical infrastructure across Canada, and it will provide increased awareness of what is impacting critical infrastructure, and that will be good for all of us.

The legislation will also assure our global partners that cyber security is a priority, and that measures are being taken to protect our critical infrastructure.

My concern with this legislation, as it is written, is that it focuses solely on reporting after a successful attack. In other words, it looks at how to close the barn door after the horses have gone.

The goal of the CCTX is to enable organizations to prevent a successful attack through improved knowledge and understanding. The rapidly evolving cyber threat environment necessitates sharing and collaboration among organizations, not only with the government. Cybersecurity is a team sport.

No organization can adequately develop and maintain the required level of cyber resilience on its own. Cyber resilience requires a broader approach. It is more than incident reporting. It requires sharing best practices and experiences in implementing the very security programs established here in this bill, sharing methods, preventing attacks and comparing experiences and technologies.

Many of the critical infrastructure organizations covered in this bill also participate in the CCTX because they realize the value in that collaboration, but their participation is limited by the perceived risk of exposure and litigation. They are sharing

membres peuvent échanger de l'information sur les cybermenaces et renforcer la cyberrésilience en collaborant pour comprendre les menaces et échanger des pratiques exemplaires et des idées, de façon à prévenir les attaques réussies et à répondre aux besoins en matière de signalement. Dans un monde où il ne s'agit pas de savoir si une organisation sera la cible d'une attaque, mais quand elle le sera, l'objectif est de renforcer la résilience, non seulement dans nos infrastructures essentielles, mais aussi dans toutes les organisations, afin de créer un environnement économique plus solide pour tous.

ECMC compte 190 membres représentant 15 secteurs et plus de 1,5 million d'employés. Bon nombre de nos membres représentent les secteurs touchés par le projet de loi, tandis que d'autres font partie de leur chaîne d'approvisionnement. Bon nombre sont des petites et moyennes entreprises, ce qui est conforme à ce qu'on observe dans une grande partie de l'économie canadienne.

Il ne fait aucun doute que le projet de loi renforcera la position du Canada en matière de cybersécurité. Il crée un niveau commun de sécurité pour les infrastructures essentielles partout au Canada, ce qui permettra de mieux faire savoir ce qui risque d'avoir un impact sur ces infrastructures et sera bon pour nous tous.

Le projet de loi garantira également à nos partenaires du monde entier que la cybersécurité est une priorité et que des mesures sont prises pour protéger nos infrastructures essentielles.

Ce qui me préoccupe dans le projet de loi ainsi qu'il est conçu, c'est qu'il se concentre uniquement sur le signalement après une attaque réussie. En d'autres termes, il porte sur les moyens de fermer la porte de l'écurie une fois que les chevaux sont partis.

L'objectif d'ECMC est de permettre aux organisations de prévenir les attaques réussies en améliorant leurs connaissances et leur compréhension. L'évolution rapide des cybermenaces exige une mise en commun de l'information et une collaboration entre les organisations, et pas seulement avec le gouvernement. La cybersécurité est un sport d'équipe.

Aucune organisation ne peut acquérir et maintenir à elle seule le niveau de cyberrésilience requis. La cyberrésilience exige une approche plus large. Elle ne se limite pas au signalement des incidents. Il faut communiquer les pratiques exemplaires et les expériences dans la mise en œuvre des programmes de sécurité prévus dans le projet de loi, mettre les méthodes en commun, prévenir les attaques et comparer les expériences et les technologies.

Bon nombre des organismes chargés d'infrastructures essentielles visés par le projet de loi participent également aux activités d'ECMC parce qu'ils sont conscients de la valeur de cette collaboration, mais leur participation est limitée parce

information in the U.S. that they feel they can't share here in Canada.

If the objective of this legislation is to prevent cyber incidents, then we need to encourage and enable all parties to go beyond the required controls and reporting to regulators. We need to encourage them to create stringent controls in all systems and enable them to share relevant and timely information with their greater community and supply chain, many of whom are connected directly to their systems.

We need to create legal safeguards, so that they can share information and experiences, in order to warn others. This legislation provides us with an opportunity to create the legal protections we need. With a few minor adjustments, this bill could create safe harbour legislation that would have a truly lasting impact on the resilience of all organizations.

Safe harbour laws enable organizations to share information beyond operational capability with the greater community without fear of reprisal, information that may fall below the threshold for required reporting to regulators.

When done in conjunction with legislative requirements like these, we provide additional motivation for adopting increased security in all areas, not just critical systems.

We would create an environment that strengthens defences for all, a carrot and a stick.

Bill C-26, with a small change, presents an opportunity for the government to help thousands of companies strengthen their ability to protect personal information and sensitive data and create a truly resilient supply chain and economy.

Thank you.

The Chair: Thank you very much, Ms. Quaid.

Colleagues, we'll now hear from Kate Robertson.

Ms. Robertson, whenever you're ready, please proceed.

Kate Robertson, Senior Research Associate, Citizen Lab: Good afternoon, my name is Kate Robertson. I am a lawyer and currently a researcher at the University of Toronto's Citizen Lab. My comments today draw on Citizen Lab's research in cybersecurity and telecommunications, as well as constitutional law analysis I've submitted in a brief to this committee. Parts 3

qu'ils ont l'impression de s'exposer à des risques et à des litiges. Ils échangent aux États-Unis des renseignements qu'ils estiment ne pas pouvoir communiquer ici, au Canada.

Si l'objectif du projet de loi est de prévenir les cyberincidents, nous devons encourager toutes les parties à aller au-delà des contrôles et des rapports à remettre aux organismes de réglementation et leur permettre de le faire. Nous devons les encourager à créer des contrôles rigoureux dans tous les systèmes et leur permettre de communiquer des renseignements pertinents et opportuns avec leur milieu et les éléments de leur chaîne d'approvisionnement, dont bon nombre sont directement connectés à leurs systèmes.

Nous devons créer des garanties juridiques de sorte qu'il soit possible de mettre en commun l'information et les expériences, afin d'avertir les autres. Le projet de loi nous donne l'occasion de créer les protections juridiques dont nous avons besoin. Avec quelques rajustements mineurs, le projet de loi pourrait créer des dispositions d'exonération qui auraient un impact vraiment durable sur la résilience de toutes les organisations.

Les dispositions d'exonération permettent aux organisations d'échanger de l'information qui dépasse les capacités opérationnelles avec l'ensemble de leur milieu sans crainte de représailles, de l'information qui peut tomber sous le seuil de déclaration obligatoire aux organismes de réglementation.

Si cela se fait en conjonction avec des exigences législatives comme celles-ci, nous offrons une motivation supplémentaire pour la mise en place d'une sécurité accrue dans tous les domaines, et pas seulement dans les systèmes essentiels.

Nous mettrions en place un environnement propre à renforcer les défenses pour tous, par des encouragements et des sanctions.

Le projet de loi C-26, avec une modeste modification, offre au gouvernement l'occasion d'aider des milliers d'entreprises à renforcer leur capacité de protéger les renseignements personnels et les données sensibles et à créer une chaîne d'approvisionnement et une économie vraiment résilientes.

Merci.

Le président : Merci beaucoup, madame Quaid.

Chers collègues, nous allons maintenant entendre Kate Robertson.

Maître Robertson, si vous êtes prête, allez-y.

Me Kate Robertson, associée de recherche principale, Citizen Lab : Bonjour, je m'appelle Kate Robertson. Je suis avocate et chercheuse au Citizen Lab de l'Université de Toronto. Mes observations d'aujourd'hui s'inspirent des recherches de Citizen Lab en cybersécurité et en télécommunications, ainsi que de l'analyse du droit constitutionnel que j'ai présentée dans un

and 4 of my brief set out recommended amendments to address constitutional deficits and a cybersecurity danger in the bill.

My brief builds on a report co-authored by a former colleague, Dr. Christopher Parsons, as well as analysis that I published earlier this year in *The Globe and Mail* with my colleague, Professor Ron Deibert, which warns of the encryption-breaking powers in Bill C-26.

I had the opportunity to observe last week's hearing on this bill. Today, it would be most useful for me to be very clear on two key points. First, Bill C-26 does give the government power to make Canada's networks less secure, such as by issuing orders to compromise encryption standards in 5G technology for lawful access purposes. Recommendation 13 of my brief, which has also been the subject of a parallel recommendation from numerous civil society groups, asks this committee to amend Bill C-26 to stipulate that the minister's powers cannot be used to compromise the confidentiality or integrity of telecommunications services. This should not be a controversial amendment.

There are, unfortunately, pervasive vulnerabilities at the heart of the world's mobile networks. Canada needs mandatory, uncompromised, and network-wide security standards. A defining feature of this law should be that no one — neither telecommunication companies, nor the federal government — should have the power to cut corners or compromise the security of Canada's networks.

For years, analysts have warned of the security risks of lawful access back doors. When similar laws were pushed forward in the United States, the FBI discounted and minimized the warnings of cybersecurity experts. However over the last month, reporting in *The Washington Post* documents how a devastating security breach is unfolding in the government-mandated access points in U.S. telecom carriers, which are, as we speak, being exploited in a China-based hacking and spy operation.

As of yesterday, *The Washington Post* reporting suggests that the hack is ongoing — that's the belief — and has now left millions of mobile phone users on the networks of three major carriers ongoingly vulnerable to government surveillance by a foreign agency. This has included the phones of candidates for the President and Vice President of the United States, and senior campaign staff on the eve of the U.S. presidential election.

mémoire soumis au comité. Les parties 3 et 4 de mon mémoire proposent des modifications au projet de loi pour combler des lacunes au plan constitutionnel et éliminer un danger en matière de cybersécurité.

Mon mémoire s'appuie sur un rapport rédigé avec un ancien collègue, M. Christopher Parsons, ainsi que sur une analyse que j'ai publiée cette année dans le *Globe and Mail* avec mon collègue, Ron Deibert, et qui lance une mise en garde au sujet des pouvoirs permettant de casser le cryptage prévus dans le projet de loi C-26.

J'ai pu suivre la séance de la semaine dernière consacrée au projet de loi. Aujourd'hui, il serait très utile que je sois très claire sur deux points clés. Premièrement, le projet de loi C-26 donne au gouvernement le pouvoir de rendre les réseaux du Canada moins sûrs, notamment en prenant des décrets visant à compromettre les normes de chiffrement de la technologie 5G pour assurer un accès légal. La recommandation 13 de mon mémoire, qui a également fait l'objet d'une recommandation parallèle de la part de nombreux groupes de la société civile, demande au comité de modifier le projet de loi C-26 pour préciser que les pouvoirs du ministre ne peuvent être utilisés pour compromettre la confidentialité ou l'intégrité des services de télécommunications. Cet amendement ne devrait pas prêter à controverse.

Malheureusement, les vulnérabilités sont omniprésentes au cœur des réseaux mobiles mondiaux. Le Canada a besoin de normes de sécurité obligatoires, sans compromis et à l'échelle du réseau. Une caractéristique déterminante de cette loi devrait être que personne — ni les entreprises de télécommunications ni le gouvernement fédéral — ne devrait avoir le pouvoir de tourner les coins ronds ou de compromettre la sécurité des réseaux du Canada.

Depuis des années, les analystes lancent des mises en garde contre les risques pour la sécurité que présentent les portes dérobées donnant un accès légal. Lorsque des lois semblables ont été adoptées aux États-Unis, le FBI a écarté du revers de la main et minimisé les avertissements des experts en cybersécurité. Au cours du dernier mois, pourtant, le *Washington Post* a publié un article sur une atteinte à la sécurité dévastatrice qui a lieu à cause des points d'accès imposés par le gouvernement aux entreprises de télécommunications américaines et qui, au moment où on se parle, sont exploités dans une opération de piratage et d'espionnage basée en Chine.

Selon un article paru hier dans le *Washington Post*, le piratage est en cours — c'est ce qu'on croit — et des millions d'utilisateurs de téléphones mobiles sur les réseaux de trois grandes entreprises sont toujours vulnérables à la surveillance gouvernementale exercée par un organisme étranger. Cela comprend les téléphones des candidats aux postes de président et de vice-président des États-Unis, ainsi que du personnel de campagne à la veille de l'élection présidentielle américaine.

In a letter from United States Senator, Ron Wyden, about the hack, which I referenced on page 18 of my brief, the senator states this needs to be a wake-up call for the U.S. government.

Here in Canada, these events illustrate the significance of what is at stake and should be a wake-up call for us on Bill C-26 as well. Reporting by the CBC in 2017 demonstrated that for a member of Parliament, all that was needed was his phone number to understand and be able to surreptitiously monitor his phone calls, texts and locations.

I would urge you to heed the warnings of experts and civil society groups and ask you to make this critical amendment to the legislation.

A second point should also be clear. There was some suggestion made last week that this bill may not result in the Communications Security Establishment Canada, or CSE, collecting and using private data from telecommunication companies. However, there is no doubt that the current text of the bill, which is what matters, creates a broad and warrantless power to collect sensitive data from telecommunication companies and to disclose it to federal agencies, including the CSE and the Canadian Security Intelligence Service, or CSIS.

Contrary to what was implied last week, Canada's national security bodies would not need new powers to create this extraordinary effect.

Telecommunication providers are conveyors of the most private information known to our legal system. The absence of Federal Court oversight is an enormous gap, and a constitutional deficiency in this bill. Recommendations 6 and 7 of my brief put this bill on stronger constitutional footing.

Because of my time limit, I would specifically invite a follow-up question from this committee on concerns why the current measures in the legislation are not adequate to this task.

Thank you.

The Chair: Thank you, Ms. Robertson.

Finally, on behalf of the Centre for International Governance Innovation, or CIGI, Mr. Aaron Shull. The floor is yours whenever you're ready.

Aaron Shull, Managing Director and General Counsel, Centre for International Governance Innovation: Thank you, honourable chair and members of the committee, for the opportunity to speak today on Bill C-26, a vital bill that aims to

Dans une lettre au sujet du piratage, dont je traite à la page 18 de mon mémoire, le sénateur américain Ron Wyden affirme que cela doit être un signal d'alarme pour le gouvernement américain.

Au Canada, ces faits illustrent l'importance de l'enjeu et devraient également être un signal d'alarme au sujet du projet de loi C-26. Des reportages de la CBC, en 2017, ont montré qu'il suffit de connaître le numéro de téléphone d'un député pour arriver à comprendre et à surveiller subrepticement ses appels et ses messages texte et à savoir où il se trouve.

Je vous exhorte à tenir compte des avertissements des experts et des groupes de la société civile et vous demande d'apporter cette modification essentielle au projet de loi.

Un deuxième point devrait aussi être clair. On a laissé entendre la semaine dernière que le projet de loi pourrait ne pas permettre que le Centre de la sécurité des télécommunications du Canada, ou CST, recueille et utilise des données privées provenant d'entreprises de télécommunications. Il ne fait pourtant aucun doute que le libellé actuel du projet de loi — qui est ce qui compte — crée un vaste pouvoir permettant de recueillir sans mandat des données sensibles auprès des entreprises de télécommunications et de les communiquer aux organismes fédéraux, y compris le CST et le Service canadien du renseignement de sécurité, ou SCRS.

Contrairement à ce qu'on a laissé entendre la semaine dernière, les organismes de sécurité nationale du Canada n'auraient pas besoin de nouveaux pouvoirs pour obtenir cet effet extraordinaire.

Les fournisseurs de services de télécommunications sont les transporteurs des renseignements les plus privés que notre système juridique connaisse. L'absence de surveillance de la part de la Cour fédérale constitue une lacune énorme dans le projet de loi et aussi une lacune au plan constitutionnel. Les recommandations 6 et 7 de mon mémoire auraient pour effet de renforcer la constitutionnalité du projet de loi.

Étant donné que je n'ai pas beaucoup de temps, j'inviterais le comité à poser une question complémentaire sur les raisons pour lesquelles les mesures prévues dans le projet de loi ne sont pas adéquates.

Merci.

Le président : Merci, maître Robertson.

Enfin, au nom du Centre pour l'innovation dans la gouvernance internationale, ou CIGI, Me Aaron Shull. Vous pouvez intervenir quand vous serez prêt.

Me Aaron Shull, directeur général et avocat général, Centre pour l'innovation dans la gouvernance internationale : Merci à vous, monsieur le président, ainsi qu'aux membres du comité, de me donner l'occasion de parler

secure Canada's telecommunications and critical infrastructure sectors against rising cyber-threats.

While this legislation marks significant progress, there are specific areas that warrant closer examination to ensure a balanced and effective approach to cybersecurity.

First, the issue of procedural fairness. While Bill C-26 represents a substantial advancement in safeguarding Canada's critical infrastructure, there's incongruity between clauses 15.9(1) (c) and (e) that warrant further consideration.

Clause (c) rightly recognizes an applicant should be reasonably informed of the case against them in a summary of the evidence which is crucial for procedural fairness, yet clause (e) allows the judge to base decisions on the evidence that the applicant may never see. This discrepancy could hinder an applicant's ability to mount an effective defence and risks undermining transparency and trust in the judicial process. It also puts at risk an applicant's ability to respond fully, which is fundamental to procedural fairness.

To address this, I would suggest the committee consider adding a mechanism for independent counsel or a special advocate. This addition could help ensure fairness by allowing for a full review of the evidence on the applicant's behalf while maintaining the confidentiality of sensitive information. Such an approach could help harmonize these provisions and reinforce the integrity of the process.

Second, information sharing standards. The bill establishes different standards for sharing information within the Government of Canada versus external entities. Clause 15.6 allows sharing internally, but restricts it to purposes such as compliance and enforcement, whereas clause 15.7 permits external information sharing, such as with foreign states or provinces, based on a much broader standard. That is to say, if the information is deemed ". . . relevant to securing the Canadian telecommunication systems . . . ." This discrepancy could lead to inconsistent oversight and may impact public trust in how sensitive information is handled. Aligning these standards would support a uniform and secure framework for information sharing, ensuring that all exchanges meet rigorous criteria for necessity and security.

Third, and finally, supporting small- and medium-sized enterprises and encouraging innovation. Small- and medium-sized enterprises, or SMEs, are essential to the supply chains of

aujourd'hui du projet de loi C-26, un projet de loi crucial qui vise à protéger les secteurs des télécommunications et des infrastructures essentielles du Canada contre des cybermenaces croissantes.

Bien que le projet de loi constitue un progrès important, il y a des domaines précis qui méritent un examen plus approfondi si nous voulons adopter une approche équilibrée et efficace en matière de cybersécurité.

Premièrement, la question de l'équité procédurale. Bien que le projet de loi C-26 améliore beaucoup la protection des infrastructures essentielles du Canada, il y a une divergence entre les alinéas 15.9(1)c) et e) qui justifie un examen plus poussé.

L'alinéa c) reconnaît, à juste titre, qu'un demandeur devrait être suffisamment informé de la thèse retenue contre lui par un résumé des éléments de preuve qui est essentiel à l'équité procédurale, mais l'alinéa e) permet au juge de fonder ses décisions sur des éléments de preuve que le demandeur pourrait ne jamais voir. Cette divergence pourrait nuire à la capacité d'un demandeur de préparer une défense efficace et risquerait de miner la transparence du processus judiciaire et la confiance dans ce processus. Elle met également en péril la capacité d'un demandeur de donner une réponse complète, ce qui est indispensable à l'équité procédurale.

Pour régler ce problème, je propose que le comité envisage d'ajouter un mécanisme faisant appel à des avocats indépendants ou à des avocats spéciaux. Cet ajout pourrait contribuer à assurer l'équité en permettant un examen complet de la preuve au nom du demandeur tout en préservant la confidentialité des renseignements de nature délicate. Une telle approche pourrait aider à harmoniser ces dispositions et à renforcer l'intégrité du processus.

Deuxièmement, les normes de communication de l'information. Le projet de loi établit des normes différentes pour l'échange de renseignements au sein du gouvernement du Canada par opposition aux entités externes. L'article 15.6 permet l'échange à l'interne, mais le restreint à des fins comme le respect des dispositions, tandis que l'article 15.7 permet la communication de renseignements à l'extérieur, comme avec des États étrangers ou des provinces, en fonction d'une norme beaucoup plus large : si les renseignements sont considérés comme « utiles pour sécuriser le système canadien de télécommunications... » Cette divergence pourrait entraîner une incohérence dans la surveillance et avoir une incidence sur la confiance du public à l'égard du traitement des renseignements de nature délicate. L'harmonisation de ces normes favoriserait un cadre uniforme et sûr pour l'échange de renseignements, en veillant à ce que tous les échanges répondent à des critères rigoureux de nécessité et de sécurité.

Enfin, troisièmement, le soutien des petites et moyennes entreprises et l'incitation à l'innovation. Les petites et moyennes entreprises, ou PME, sont essentielles aux chaînes

critical infrastructure sectors, but they often lack resources for robust cybersecurity, and they appear nowhere in this bill. Incentives, such as a tax credit for CyberSecure Canada certification would help SMEs strengthen their defences and contribute to overall resilience. However, given the urgency of passing Bill C-26, these supportive measures may be better addressed in Canada's forthcoming national cybersecurity strategy where they can receive focused attention.

Similarly, there is a risk that operators may approach the bill's requirements as a minimum standard, meeting only basic compliance requirements rather than striving for continuous improvement in cybersecurity practices. This compliance-focused mindset could stifle innovation in cybersecurity, an area that demands adaptability to keep pace with evolving threats. Encouraging innovation through the broader cybersecurity strategy could complement Bill C-26's foundational requirements and foster a culture of proactive security.

In conclusion, Mr. Chair, Bill C-26 is a significant step toward strengthening Canada's cybersecurity framework. By addressing the issues of fairness, aligning information standards and supporting SMEs and innovation through the forthcoming cybersecurity strategy, we can maximize the bill's effectiveness and reinforce Canada's resilience against cyber-threats.

Thank you, and I look forward to further discussion on these critical issues.

The Chair: Thank you very much, Mr. Shull. We will now proceed to questions, starting with our deputy chair, Senator Dagenais.

[*Translation*]

Senator Dagenais: My question is for Ms. Quaid. I would like you to expand on the dangers we face. Your reports and assessments refer directly to cyber-threats from countries like China, Russia, Iran and North Korea. Based on your observations, is it fair to say that the current government's deteriorating relations with the leaders of those countries are systematically leading to an increase in cyberattacks? If not, how might enemy activity vary? I see you smiling.

[*English*]

Ms. Quaid: It won't be helping. The deterioration of relations won't be helping, but truthfully, the countries you mentioned, nation states that are attacking us and so many other countries in

d'approvisionnement du secteur des infrastructures essentielles, mais elles manquent souvent de ressources pour assurer une cybersécurité robuste. Il n'en est question nulle part dans le projet de loi. Des incitatifs, comme un crédit d'impôt pour la certification CyberSécuritaire Canada, aideraient les PME à renforcer leurs défenses et contribueraient à la résilience globale. Toutefois, étant donné qu'il est urgent d'adopter le projet de loi C-26, il serait peut-être préférable d'aborder la question dans la future stratégie nationale de cybersécurité du Canada, qui pourrait leur accorder une attention particulière.

De même, il y a un risque que les exploitants considèrent les exigences du projet de loi comme une norme minimale, ne répondant qu'à des exigences de conformité de base plutôt que de chercher à améliorer continuellement les pratiques en matière de cybersécurité. Si on se limite ainsi à la stricte conformité, cela pourrait étouffer l'innovation en cybersécurité, un domaine qui exige une grande capacité d'adaptation pour suivre le rythme de l'évolution des menaces. Encourager l'innovation par l'entremise de la stratégie globale de cybersécurité serait un moyen complémentaire s'ajoutant aux exigences fondamentales du projet de loi C-26 et favoriserait une culture de sécurité proactive.

En guise de conclusion, monsieur le président, je dirai que le projet de loi C-26 est une étape importante vers le renforcement du cadre de la cybersécurité au Canada. En nous attaquant aux questions d'équité, en harmonisant les normes d'information et en appuyant les PME et l'innovation grâce à la prochaine stratégie de cybersécurité, nous pouvons maximiser l'efficacité du projet de loi et renforcer la résilience du Canada face aux cybermenaces.

Je vous remercie et j'ai hâte de poursuivre la discussion sur ces questions cruciales.

Le président : Merci beaucoup, maître Shull. Nous allons maintenant passer aux questions, en commençant par le vice-président, le sénateur Dagenais.

[*Français*]

Le sénateur Dagenais : Ma question s'adresse à Mme Quaid. J'aimerais vous entendre davantage sur le danger qui nous menace. Vos rapports et évaluations font directement référence aux cybermenaces venant de pays comme la Chine, la Russie, l'Iran et la Corée du Nord. Vos observations permettent-elles de dire que la détérioration des relations du gouvernement actuel avec les dirigeants de ces pays entraîne systématiquement une augmentation des cyberattaques? Dans la négative, comment les activités ennemies peuvent-elles varier? Je vous vois sourire.

[*Traduction*]

Mme Quaid : Il n'y a là rien de favorable. La détérioration des relations ne sera pas utile, mais en vérité, les pays que vous avez énumérés, les États-nations qui nous attaquent, nous et tant

this world, have been doing it for a long time, and they are doing it for a variety of reasons. North Korea is effectively funding its nuclear program through successful cyberattacks. That's not dependent on relations with our government. That's simply demand and greed, and the others are doing it for long-term political gain.

[*Translation*]

Senator Dagenais: I'd like to talk about the potential sabotage of critical infrastructure in this country.

Have our intelligence services successfully thwarted any such attacks in recent years? How will Bill C-26 really improve our ability to protect ourselves?

[*English*]

Ms. Quaid: The benefit that we're going to see from Bill C-26 in protecting critical infrastructure and its supply chain in many ways comes down to the supply chain. Truthfully, the larger organizations in our critical infrastructure have some of the most sophisticated cyber programs you can imagine. They're good, they're strong and they follow the highest levels of all the global standards, particularly those that deal with the cross-border side of things, like our energy sector.

But Bill C-26 enables the critical infrastructure organizations to push the cyber requirements down through their supply chain, so they are going to have to enable those suppliers to be stronger.

The truth is, nowadays all systems are integrated. Suppliers are connecting directly into their clients. That is a risk. Bill C-26 may help to stop some of that risk. However, I will point out what Aaron Shull said. Many of these organizations, these suppliers, are small and medium businesses. They're going to need help, and they're going to need support, but that is one of the benefits of Bill C-26.

[*Translation*]

Senator Dagenais: Ms. Robertson, can you tell us more about the constitutional issues and risks you foresee with Bill C-26?

[*English*]

Ms. Robertson: Thank you for the question. In my remarks, I have identified privacy deficits that have been analyzed in my brief as being a significant gap in the constitutional footing of this bill.

d'autres pays dans le monde, le font depuis longtemps, et ce, pour diverses raisons. La Corée du Nord finance efficacement son programme nucléaire au moyen de cyberattaques fructueuses. Ce n'est pas à cause des relations avec notre gouvernement. C'est simplement un effet de la demande et de la cupidité. Les autres recherchent des gains politiques à long terme.

[*Français*]

Le sénateur Dagenais : J'aimerais aborder le volet du sabotage potentiel d'infrastructures critiques au pays.

Est-ce que nos services de renseignement en ont déjoué de façon significative au cours des dernières années? En quoi le projet de loi C-26 va-t-il réellement améliorer notre capacité de protection?

[*Traduction*]

Mme Quaid : L'avantage que nous retirerons du projet de loi C-26 pour la protection des infrastructures essentielles et de leur chaîne d'approvisionnement, à bien des égards, concerne la chaîne d'approvisionnement. Honnêtement, les grandes organisations de nos infrastructures essentielles ont certains des programmes cybernétiques les plus perfectionnés imaginables. Ils sont bons, ils sont forts et ils respectent les normes les plus élevées de tous les pays, en particulier celles qui touchent la dimension transfrontalière, comme dans notre secteur de l'énergie.

Mais le projet de loi C-26 permet aux organisations des infrastructures essentielles d'étendre les exigences en matière de cybersécurité à leur chaîne d'approvisionnement. Ces fournisseurs seront ainsi plus forts.

La vérité, c'est que, de nos jours, tous les systèmes sont intégrés. Les fournisseurs communiquent directement avec leurs clients. C'est un risque. Le projet de loi C-26 pourrait contribuer à éliminer une partie de ce risque. Je reviens sur un point qu'Aaron Shull a souligné : bon nombre de ces organisations, de ces fournisseurs, sont des PME, qui auront besoin d'aide et de soutien. C'est l'un des avantages du projet de loi C-26.

[*Français*]

Le sénateur Dagenais : Madame Robertson, pouvez-vous nous en dire davantage sur les enjeux et les risques constitutionnels que vous entrevoyez avec le projet de loi C-26?

[*Traduction*]

Me Robertson : Je vous remercie de la question. Dans mes observations, j'ai dit que les lacunes en matière de protection de la vie privée analysées dans mon mémoire constituent une lacune importante dans le fondement constitutionnel du projet de loi.

In addition to those issues, which I outlined, the free expression deficits follow very closely on the heels of those privacy gaps in the legislation. By that, I mean the non-disclosure orders that attach to ministerial powers, which are virtually unlimited in scope and will have the potential to meaningfully interfere with public debate about matters of critical importance to the public interest.

In the judicial review proceedings that are in the Telecommunications Act, for example, there is some provision for secrecy. However, it is specifically limited to matters which are injurious to international relations, National Defence or national security or endanger the safety of any person.

For the non-disclosure orders which attach to the ministerial powers, there is no limit on the reasons that the minister may apply for requiring non-disclosure, and they are virtually time unlimited in temporal nature as well. Both of these privacy issues, as well as what is, ultimately, a free expression problem, are significant in this legislation, notwithstanding some very considerable improvements since it was studied in the House of Commons.

[*Translation*]

Senator Dagenais: Thank you very much, Ms. Robertson.

[*English*]

Senator Boehm: Thank you, witnesses, for being here. I have a question for each of you.

Ms. Quaid, I was quite interested in your mentioning safe harbour. Could you give us a little more detail on that in terms of the partnership that you envision?

I'm going to ask all three of my questions so that they're out there.

Ms. Robertson, in part, you've answered just now with Senator Dagenais the question that I had. Of course, Citizen Lab has a long history of supporting advocacy for privacy rights. Could you provide a little more detail in terms of how this bill could improve? I know you have proposed amendments, but the privacy protections, particularly with respect to surveillance, capabilities and critical infrastructure.

Mr. Shull, the last question for you goes back to a recent article that you had co-authored. You're saying now the government is finally taking national security more seriously. To go back to the bill specifically, how would you assess the alignment of the bill with international best practices, and in particular, what can Canada learn from similar legislation in Group of Seven, or G7, countries given that we will be chairing the G7 process next year?

En plus de ces problèmes, que j'ai décrits, les lacunes en matière de liberté d'expression suivent de très près celles qui concernent la protection de la vie privée. J'entends par là les décrets de non-divulgation qui se rattachent aux pouvoirs ministériels, dont la portée est à peu près illimitée et qui risquent de nuire de façon significative au débat public sur des questions d'une importance cruciale pour l'intérêt public.

Dans les procédures de contrôle judiciaire prévues dans la Loi sur les télécommunications, par exemple, figure une disposition relative au secret. Toutefois, elle se limite expressément à ce qui porte atteinte aux relations internationales, à la défense nationale ou à la sécurité nationale ou met en danger la sécurité de toute personne.

Pour les arrêts de non-divulgation qui se rattachent aux pouvoirs ministériels, il n'y a pas de limite aux raisons que le ministre peut invoquer pour demander la non-divulgation, et elles sont pratiquement illimitées dans le temps également. Ces deux questions de protection de la vie privée, ainsi que ce qui est, au bout du compte, un problème de liberté d'expression, sont importantes dans ce projet de loi, malgré quelques améliorations considérables apportées depuis son étude à la Chambre des communes.

[*Français*]

Le sénateur Dagenais : Merci beaucoup, madame.

[*Traduction*]

Le sénateur Boehm : Je remercie les témoins d'être là. J'ai une question à poser à chacun d'entre eux.

Madame Quaid, j'ai trouvé très intéressant que vous mentionniez la notion d'exonération. Pourriez-vous nous donner un peu plus de détails sur le partenariat que vous envisagez?

Je vais poser mes trois questions tout de suite. Ce sera chose faite.

Maître Robertson, vous venez de répondre en partie à ma question en vous adressant au sénateur Dagenais. Bien sûr, Citizen Lab appuie depuis longtemps la défense des droits à la vie privée. Pourriez-vous nous donner un peu plus de détails sur la façon d'améliorer le projet de loi? Je sais que vous avez proposé des amendements, mais il s'agit de mesures de protection de la vie privée, particulièrement en ce qui concerne la surveillance, les capacités et les infrastructures essentielles.

Maître Shull, ma dernière question porte sur un article récent dont vous êtes l'un des auteurs. Vous dites que le gouvernement prend enfin la sécurité nationale plus au sérieux. Pour revenir au projet de loi, comment évalueriez-vous l'harmonisation du projet de loi avec les pratiques exemplaires internationales et, en particulier, ce que le Canada peut apprendre d'une loi semblable dans les pays du Groupe des sept, le G7, étant donné que nous présiderons le G7 l'an prochain?

Ms. Quaid: Thank you for the question. When I refer to "safe harbour legislation" and the type of information that it would enable companies to provide to the greater community, first and most important, I'm not suggesting that information should not be shared with regulators and with our Canadian Centre for Cyber Security. That is critical — absolutely critical. I'm talking about the type of information that in our industry we would call "Left of Boom," before an attack happens, or before a successful attack happens, because attacks happen in the thousands per day. It's the type of information that an organization, if they talk about it, it could show weaknesses in their system, and that could create litigation problems for them. So they don't speak.

Every system has its flaws because the attackers are changing things on a daily basis. It is the type of information that, if they were able to share it, would help other organizations to strengthen their defences, so that a single attack stays as a single attack, as opposed to being a successful one-time that becomes multiples. That's what we would like to see happen.

Senator Boehm: Thank you.

Ms. Robertson: With respect to privacy details in the legislation, there was some discussion last week as to the existing measures in the legislation, which some witnesses offered as protective with respect to privacy.

One of those measures is that there is a carve out that predated the explicit addition of this amendment that states that the bill does not authorize the interception of private communications. However, telecommunication carriers host troves of sensitive data that can be collected in ways that do not fit the technical definition of interception of private communications. That's a very specific legal term that has a narrower scope compared to what telecommunication data includes.

The Privacy Commissioner of Canada testified in the House of Commons, and I agree with his testimony when he stated that if the collection and sharing powers are not more specifically constrained, this could lead to the inappropriate collection and sharing of data such as subscriber account information, communication data, website visits, metadata, location data and financial data. This speaks to the enormity of the potential reach of this very broad collection power, which in section 15.4 gives the minister the ability to ask for any information from these entities.

Mr. Shull: Thank you, Senator Boehm. It's a pleasure to see you as well. I'll touch on the two big pieces, the first on critical infrastructure protection.

Mme Quaid : Je vous remercie de la question. Lorsque je parle de « loi d'exonération » et du type de renseignements qu'elle permettrait aux entreprises de fournir au milieu plus large de la cybersécurité, d'abord et avant tout, je ne dis pas que ces renseignements ne devraient pas être communiqués aux organismes de réglementation et au Centre canadien pour la cybersécurité. C'est absolument essentiel. Je parle du type d'information dont nous dirons dans notre industrie qu'elle se situe « Left of Boom », c'est-à-dire avant l'incident, avant qu'une attaque ne se produise, ou avant qu'une attaque ne réussisse, car les attaques se comptent en milliers par jour. C'est le genre d'information qui, si une organisation en parle, risque de trahir les faiblesses de son système, ce qui pourrait lui occasionner des litiges. Elle n'en parle donc pas.

Chaque système a ses failles parce que les attaquants changent la donne quotidiennement. C'est le genre de renseignements qui, s'il était possible de les communiquer, aideraient d'autres organisations à renforcer leurs défenses, de sorte qu'une seule attaque reste isolée au lieu que le succès initial ne soit répété à de multiples reprises. C'est ce que nous souhaitons.

Le sénateur Boehm : Merci.

Me Robertson : À propos des dispositions du projet de loi portant sur la protection de la vie privée, il y a eu des discussions la semaine dernière au sujet des mesures existantes, selon certains témoins, qui peuvent protéger la vie privée.

L'une de ces mesures est une exclusion antérieure à l'ajout explicite de l'amendement qui dispose que le projet de loi n'autorise pas l'interception de communications privées. Toutefois, les entreprises de télécommunications hébergent des masses de données sensibles qui peuvent être recueillies d'une manière qui ne correspond pas à la définition technique de l'interception de communications privées. C'est un terme juridique très précis qui a une portée plus étroite que ce que comprennent les données de télécommunication.

Le commissaire à la protection de la vie privée du Canada a témoigné à la Chambre des communes, et je suis d'accord avec lui lorsqu'il dit que si les pouvoirs de collecte et d'échange ne sont pas plus précisément limités, cela pourrait mener à la collecte et à l'échange inappropriés de données comme les renseignements sur les comptes des abonnés, les données de communication, les visites de sites Web, les métadonnées, les données de localisation et les données financières. Cela montre l'ampleur de la portée que pourrait avoir le très vaste pouvoir de collecte, qui, à l'article 15.4, permet au ministre de demander des renseignements à ces entités.

Me Shull : Merci, sénateur Boehm. C'est aussi un plaisir de vous voir. Je vais parler des deux grands éléments, le premier étant la protection des infrastructures essentielles.

It roughly lines up. The U.K. has the network and information systems regulations. The U.S., through the Cybersecurity and Infrastructure Security Agency, or CISA, has various mandates. Australia has the Security of Critical Infrastructure Act. They're roughly similar. They're focusing on critical infrastructure because it's, well, critical. There are differences, to be sure.

Also focusing on telecommunications security and high-risk vendors. Again, that focus is exactly right, looking at how you manage risk from high-risk vendors. They do it in the U.K. and the U.S. The one point I would raise is this bill is largely silent on an explicit criteria or process for designating and banning specific high-risk vendors. The U.S. has been clear — Huawei and ZTE — but there's no comparable criteria within this bill to make those designations.

Senator M. Deacon: Thank you to our witnesses and all of you for being here today. It is a very important topic, and your work is important.

As I was thinking about this yesterday, I was thinking about duopolies and monopolies in our telecommunications at risk. I've formulated a question that I hope is something you can respond to. I think I'll start with you, Mr. Shull.

Looking at the current state, frankly, of Canada's telecommunications sector and what it might mean for cybersecurity, whenever we discuss this topic, I can't help but be reminded of the Rogers blackout in 2022, not that long ago, which wasn't even an attack. It was simply human error that brought the lives and businesses of 12 million people to a standstill for days.

It seems that annually, the telecommunications options for Canadians are dwindling. I'm specifically thinking about the recent Shaw acquisition by Rogers, for instance.

Given how important these services are to our daily lives, is consolidation in this field a threat? It would seem on the surface that taking down one or two big targets could potentially cripple the country's internet services. I wonder if we should be encouraging competition here while also hitting the brakes on consolidation.

Mr. Shull: That's a great point, senator. It's nice to see you as well. The standard kind of logic would say that you're building in a single point of failure, that you're reducing diversity and resilience and that you are effectively bringing your supply chain under one roof, so if there is a vulnerability in the supply chain, it's going to permeate those. Also, there is a concentration of sensitive data. All of that stuff is true. There is also a greater risk

C'est à peu près la même chose partout. Le Royaume-Uni a des règlements sur les réseaux et les systèmes d'information. Les États-Unis, par l'entremise de la Cybersecurity and Infrastructure Security Agency, ou CISA, ont divers mandats. L'Australie a la Security of Critical Infrastructure Act. Ces mesures sont à peu près semblables. Elles se concentrent sur les infrastructures essentielles parce que, justement, c'est essentiel. Il y a certainement des différences.

Nous mettons également l'accent sur la sécurité des télécommunications et les fournisseurs à risque élevé. Encore une fois, il est tout à fait juste de se concentrer sur la façon de gérer les risques liés à ces fournisseurs. C'est ce que font le Royaume-Uni et les États-Unis. Ce que je tiens à dire, c'est que le projet de loi ne prévoit pas de critères ou de processus explicites pour désigner et interdire certains fournisseurs à risque élevé. Les États-Unis ont été clairs — Huawei et ZTE —, mais il n'y a pas de critères comparables dans le projet de loi à l'étude pour faire ces désignations.

La sénatrice M. Deacon : Merci aux témoins et à vous tous d'être là. C'est un sujet de la plus grande importance, et votre travail est aussi important.

En réfléchissant à la question hier, je songeais aux duopoles et aux monopoles dans nos télécommunications à risque. J'ai formulé une question à laquelle vous pourrez répondre, je l'espère. Je vais commencer par vous, maître Shull.

Franchement, si je considère l'état actuel du secteur des télécommunications au Canada et ce que cela pourrait signifier pour la cybersécurité, chaque fois que nous abordons ce sujet, je ne peux m'empêcher de penser à la panne de Rogers en 2022, il n'y a pas si longtemps, qui n'était même pas la conséquence d'une attaque. C'est simplement une erreur humaine qui a paralysé pendant des jours la vie et les affaires de 12 millions de personnes.

Il semble que, chaque année, les options de télécommunications à la disposition des Canadiens se font moins nombreuses. Je songe notamment à l'acquisition récente de Shaw par Rogers.

Compte tenu de l'importance de ces services dans notre quotidien, la consolidation dans ce domaine constitue-t-elle une menace? À première vue, il semble que l'élimination d'une ou deux cibles importantes pourrait paralyser les services Internet au Canada. Je me demande si nous ne devrions pas encourager la concurrence tout en freinant la consolidation.

Me Shull : C'est un excellent point, sénatrice. Je suis heureux de vous voir également. Selon la logique courante, lorsqu'il n'y a qu'un point d'échec, que la diversité et la résilience sont réduites et que la chaîne d'approvisionnement est regroupée sous un même toit, si cette dernière présente une vulnérabilité, celle-ci va se répandre partout. On assiste aussi à une concentration de données sensibles. Tout cela est vrai. Il y a

of insider threats because if there is only one and there's one insider, then you have a real problem. There are certainly national security implications.

I might remain silent on the competition and innovation side, except to say that I think I personally pay too much for my cell phone. If we can deal with that, for sure. I know what I know, and cell phone amalgamation isn't on my list.

Senator M. Deacon: Line up for that cell phone reduction. Would either of you care to comment before I go to a second part? Okay. That's great. Thank you.

If we look at this and we carry on and we have a duopoly or fewer providers, what could the government do to ensure there are redundancies in the event of an attack? Do you think the legislation covers or addresses this?

Mr. Shull: I think that's kind of what it's going toward as it relates to critical cybersystems, at least, and making sure that we don't have bad gear in our back end. I think that is precisely the evil that is being remedied here — making sure there is no problematic gear in the supply chain.

Also, for what it's worth, it may be outside the ambit of this bill, but there is the cyber centre, and they are doing good work. For what it's worth, CSE are among the best in the world. I know many of them, and they are hard working.

This is what it comes down to, this idea of issuing directives and cybersecurity orders. While it's not specifically enumerated in the bill, there is technical assistance and support that's available. There are tools that are at play, but it is precisely that issue, senator, that you raise that I think is the principal evil being remedied as a consequence of this bill.

Senator M. Deacon: Thank you. Ms. Robertson, there were a number of amendments made to the legislation in the other place related to reasonableness, oversight and privacy protection before it arrived in the Senate. You mentioned a number of changes you would like to see, and I wonder if any of the amendments they did got it right, in your view, before we get to this table.

aussi un risque plus grand de menaces internes, car si tout est concentré à un seul endroit, cela pose un réel problème et a certainement des répercussions au niveau de la sécurité nationale.

Je n'aborderai peut-être pas la concurrence et l'innovation, sauf pour dire que je crois personnellement payer trop cher pour mon téléphone cellulaire. Si nous pouvons régler cette question, d'accord. Je connais mes limites, et la fusion des services de téléphonie cellulaire ne figure pas sur la liste des choses au sujet desquelles j'ai des connaissances.

La sénatrice M. Deacon : Je ne retiendrais pas mon souffle pour ce qui est de la réduction du coût des services de téléphonie cellulaire. Est-ce que l'un d'entre vous voudrait faire un commentaire avant que je passe à la deuxième partie de ma question? D'accord. C'est bien. Merci.

Toujours dans la même veine, avec un duopole ou moins de fournisseurs, que pourrait faire le gouvernement pour s'assurer qu'il y a des options de rechange en cas d'attaque? Pensez-vous que la loi couvre ou règle ce problème?

Me Shull : Je pense que c'est ce vers quoi nous allons, en ce qui concerne les cybersystèmes essentiels, à tout le moins, de même que l'assurance de ne pas avoir de mauvais équipements en fin de compte. Je pense que c'est précisément le mal auquel on est en train de s'attaquer ici — s'assurer qu'il n'y a pas d'équipements problématiques dans la chaîne d'approvisionnement.

De plus, et c'est peut-être en dehors de la portée de ce projet de loi, il y a le cybercentre, où il se fait du bon travail. Selon moi, le Centre de la sécurité des télécommunications est l'un des meilleurs au monde. Je connais beaucoup de gens qui y travaillent, et ils s'acquittent très bien de leurs responsabilités.

Voilà à quoi cela se résume, cette notion d'émettre des directives et des décrets en matière de cybersécurité. Bien que ce ne soit pas précisé dans le projet de loi, de l'aide technique et du soutien sont disponibles. Il y a des outils en jeu, mais c'est précisément le problème que vous soulevez, sénatrice, que ce projet de loi vise à corriger, à mon avis.

La sénatrice M. Deacon : Merci. Maître Robertson, un certain nombre d'amendements ont été apportés au projet de loi à l'autre endroit relativement au caractère raisonnable, à la surveillance et à la protection de la vie privée, avant qu'il n'arrive au Sénat. Vous avez mentionné un certain nombre de changements que vous aimeriez voir, et je me demande si, à votre avis, l'un ou l'autre des amendements qui ont été proposés, avant que le projet de loi nous soit soumis, ont amélioré les choses.

Ms. Robertson: I would simply note — maybe one of your colleagues can explore this further — many of those amendments are actually inapplicable to the information collection powers in clause 15.4.

Senator Yussuff: Thank you, witnesses, for being here.

Ms. Quaid, if I could come back to you, you raised an issue about supply chains. As you know, the supply chain is not just in Canada; it extends beyond our borders, and our ability to find out whether or not that supply chain is compromised is not adequate or does not meet our standard and is very problematic. Most of our major telecom companies currently outsource a significant portion of the work and the processing of data outside of the country.

How can we assure Canadians that their information is protected? Equally, if there is a breach, how would we ever know, given we have no control over what happens to this information?

Ms. Quaid: Thank you for the question. That is part of what this bill will do. The organizations that are governed by this are responsible for their supply chain.

Let's remember that just because you have offshored something doesn't mean that you are no longer responsible for it, and they know that. They are currently responsible for that, and they treat the information and the protections with the respect that they require and deserve. This bill will simply help to ensure the reporting on any of that.

Senator Yussuff: Let me continue. If our information were to be breached outside of the country, it would be very hard for us to know, given some of the countries that we're dealing with — and we have incredible tension right now with India. A significant amount of our information is processed in China, given the contracting out. How would we ever know if that were the case?

In the specific case of India, we have a specific diaspora in our country who are worried about how they are being targeted by the Indian government. How do we even assure them that, yes, we understand the companies are responsible, but the company can't even tell me if my information has been breached in India?

Ms. Quaid: I think that's true of almost any organization and company that you are doing business with. You specifically referenced the telcos, but I think retail and so many different organizations offshore are still responsible for parts of their data

Me Robertson : J'aimerais simplement souligner — peut-être qu'un de vos collègues pourra approfondir la question — que bon nombre de ces amendements ne s'appliquent pas aux pouvoirs de collecte de renseignements prévus à l'article 15.4.

Le sénateur Yussuff : Je remercie les témoins de leur présence.

Madame Quaid, si je peux revenir à vous, vous avez soulevé une question au sujet des chaînes d'approvisionnement. Comme vous le savez, la chaîne d'approvisionnement ne se limite pas au Canada; elle s'étend au-delà de nos frontières, et notre capacité de déterminer si elle est compromise ou non est inadéquate ou ne répond pas à nos normes, et cela est très problématique. La plupart de nos grandes entreprises de télécommunications impartissent actuellement une partie importante de leur travail et du traitement des données à l'extérieur du pays.

Comment pouvons-nous assurer aux Canadiens que leurs renseignements sont protégés? De même, s'il y avait une atteinte à la vie privée, comment pourrions-nous le savoir, étant donné que nous n'avons aucun contrôle sur ce qu'il advient de ces renseignements?

Mme Quaid : Je vous remercie de la question. C'est en partie ce que fera ce projet de loi. Les organisations qui y sont assujetties sont responsables de leurs chaînes d'approvisionnement.

Il ne faut pas oublier que ce n'est pas parce que vous délocalisez quelque chose que vous n'en êtes plus responsable, et ces organisations le savent. Elles en assument actuellement la responsabilité, et elles traitent les renseignements et leur protection avec le respect qu'ils méritent et qui est nécessaire. Le projet de loi contribuera simplement à assurer la production de rapports à ce sujet.

Le sénateur Yussuff : Permettez-moi de poursuivre. Si nos renseignements personnels devaient être compromis à l'extérieur du pays, il nous serait très difficile de le savoir, compte tenu de certains des pays avec lesquels nous traitons — et du fait que nous avons actuellement des tensions incroyables avec l'Inde. Une grande partie de nos renseignements sont traités en sous-traitance en Chine. Comment pourrions-nous prendre connaissance de cela, le cas échéant?

Dans le cas précis de l'Inde, il y a une diaspora précise au Canada qui s'inquiète de la façon dont elle est ciblée par le gouvernement indien. Comment pouvons-nous même donner une assurance à ces personnes, alors que, oui, il est entendu que les entreprises sont responsables, mais elles ne peuvent même pas me dire si mes renseignements ont été compromis en Inde?

Mme Quaid : Je pense que c'est le cas de presque toutes les organisations et entreprises avec lesquelles vous faites affaire. Vous avez plus précisément parlé des entreprises de télécommunications, mais je crois que les entreprises du

collection and data privacy. If it has been breached and they are aware, then they would have to inform.

This is where I'm going to reiterate what Mr. Shull has said, and that is, our Canadian Centre for Cyber Security is very good at what they do. The CSE is very good at what they do. They are there to help the organizations — and they will — to determine whether or not there has been a breach and how large it is.

Senator Yussuff: Let me continue on this because this is one of the areas I'm trying to focus on.

In the context of a breach of information, I understand the obligation and responsibility. I'm coming back to the fact that given how important our network is to the vitality of our country — to our government and industry — if that information is stored outside the country and the country may not be able to say with any certainty that we can allow our information to be stored, isn't it problematic for us passing a piece of legislation that has no curtain around where that information should be stored?

Ms. Quaid: It may be problematic, but that becomes the purview of a bill on privacy, and PIPEDA would govern part of that. This bill really deals with the critical cybersecurity systems, and that's its focus. So, you may have a very good point. It just might not be the purview of this piece of legislation, unfortunately.

Ms. Robertson: I very respectfully have to disagree with my colleague here because I certainly appreciate that this is a privacy issue, and it was mentioned last week that the Personal Information Protection and Electronic Documents Act, or PIPEDA, would have some applicability here. This is what the Citizen Lab has been saying with respect to the historical deficiency in telecommunication networks that are subject to a range of complex, interlocking threats that have led to significant deficits in the security of our telecommunications services. The layers and layers of contracting and subcontracting is a locus point for some of these deficits, including pervasive geolocation surveillance, which is perpetuated around the world based on some of the signalling protocols that operate as a result of some of these contracts and subcontracts.

This is why we have said that it's wrong in this legislation to fixate too much on select, high-risk vendors to the exclusion of some of the ongoing historical deficiencies that have been plaguing the world's networks for a very long time, and why we need public transparency about how these orders are used or not

commerce de détail et de nombreuses organisations étrangères sont toujours responsables d'une partie de leur collecte de données et de la confidentialité de celles-ci. S'il y a eu violation et qu'elles sont au courant, elles doivent en informer le gouvernement.

Je vais répéter ce que Me Shull a dit, à savoir que le Centre canadien pour la cybersécurité fait un excellent travail. Le Centre de la sécurité des télécommunications fait également du très bon travail. Ces entités sont là pour aider les organisations à déterminer si des données ont été compromises ou non et dans quelle mesure, et elles vont le faire.

Le sénateur Yussuff : Permettez-moi de poursuivre dans la même veine, car c'est l'un des domaines sur lesquels je souhaite me concentrer.

Dans le contexte d'une atteinte à la sécurité de l'information, je comprends les notions d'obligation et de responsabilité. Je reviens sur le fait que, compte tenu de l'importance de notre réseau pour la vitalité de notre pays — pour notre gouvernement et notre industrie —, si ces renseignements sont stockés à l'extérieur du pays et qu'il n'est pas possible de confirmer que cela est permis, n'est-il pas problématique pour nous d'adopter un projet de loi qui ne prévoit aucune restriction quant à l'endroit où ces renseignements devraient être stockés?

Mme Quaid : C'est peut-être problématique, mais cela relève d'un projet de loi sur la protection de la vie privée, et la Loi sur la protection des renseignements personnels et les documents électroniques en régit une partie. Ce projet de loi porte vraiment sur les systèmes essentiels de cybersécurité, et c'est sur cela qu'il met l'accent. Il se peut que vous ayez raison, mais malheureusement, cela ne relève peut-être pas de ce projet de loi.

Me Robertson : En tout respect, je ne suis pas d'accord avec ma collègue, car je comprends qu'il s'agit d'une question de protection de la vie privée, et il a été mentionné la semaine dernière que la Loi sur la protection des renseignements personnels et les documents électroniques, ou LPRPDE, s'appliquerait dans une certaine mesure. C'est ce que pense Citizen Lab au sujet des lacunes historiques des réseaux de télécommunications, ceux-ci faisant l'objet d'une gamme de menaces complexes et interreliées, qui ont entraîné des déficits importants dans la sécurité de nos services de télécommunications. Les multiples couches de sous-traitance sont à l'origine de certaines de ces lacunes, y compris la surveillance par géolocalisation omniprésente, qui se répand partout dans le monde en raison des protocoles de signalisation qui sont utilisés dans le cadre de certains de ces contrats et de la sous-traitance.

C'est la raison pour laquelle nous avons dit que ce projet de loi ne devrait pas trop mettre l'accent sur les fournisseurs à risque élevé, en laissant de côté certaines des lacunes historiques qui affligent les réseaux mondiaux depuis très longtemps. C'est aussi la raison pour laquelle nous avons besoin de transparence sur la

used. That's because part of these risks are a direct result of passive or lack of regulation among jurisdictions around the world. I'm happy to provide in writing after this meeting some of the parallel processes that are happening in the U.K. right now with the Office of Communications, or Ofcom, to specifically address the cybersecurity threats related to third party contracting.

Senator Yussuff: If you could do that, it would be very helpful for the committee.

Senator McNair: Thank you again to the people testifying today. This is a question for all three of you, and I expect there will be a difference of opinion on it.

You talk about this bill. We're putting it in place to try to implement cybersecurity infrastructure to deal with cyberattacks. Ms. Quaid, you correctly indicate that our concern is that the number of attacks taking place each day is multiple thousands. We're trying to avoid successful attacks. There are some timing issues with this legislation.

Ms. Robertson, one of your colleagues from the Munk School of Global Affairs & Public Policy was before our committee on another matter and used the quote, "Don't let the perfect become the enemy of the good." If you had to choose at this point whether to pass the bill as it is with over 40 amendments that have been made at the House of Commons — I understand, Ms. Robertson, that you would say that they do not deal properly with some of the issues relating to clause 15 — would you pass this legislation and work on improving it after the fact or would you hold it? That's for all three of you. Ms. Quaid, maybe you could start.

Ms. Quaid: I'm glad I'm not in your chair. I would probably pass it because we are eight years behind some of our colleagues in putting forward legislation like this. It has been a very long time in coming. We have lost the faith of some of our colleagues because we don't have these protections in place. I would probably pass it, reluctantly.

Ms. Robertson: We're speaking about historical deficiencies that have been persisting for decades. I also don't envy your seat. However, for me, the decision is clear that we need powers that have a compass point that is focused and directed to the destination that we want to go. With respect to the part 1 powers that are proposed in this act, they are not pointed to the correct compass point because at bottom we need laws that say that neither the government nor telecommunication companies have the power to compromise our networks.

The unspoken conversation that is happening in this bill — conversations that you did not have last week — is that these powers give the government to compromise our next-generation

façon dont ces décrets sont utilisés ou non, ces risques étant en partie le résultat direct d'une réglementation passive ou de l'absence de réglementation dans d'autres pays du monde. Après cette réunion, je me ferai un plaisir de vous fournir par écrit un aperçu de quelques-uns des processus parallèles qui ont actuellement cours au Royaume-Uni, avec l'Office of Communications, ou Ofcom, et qui s'attaquent précisément aux menaces à la cybersécurité liées à la passation de marchés avec des tiers.

Le sénateur Yussuff : Si vous pouviez le faire, ce serait très utile pour le comité.

Le sénateur McNair : Merci encore aux témoins qui comparaissent aujourd'hui. Ma question s'adresse à vous trois, et je m'attends à ce que vous divergiez d'opinions à ce sujet.

L'objectif de ce projet de loi est d'essayer de mettre en place une infrastructure de cybersécurité pour lutter contre les cyberattaques. Madame Quaid, vous avez raison de dire que ce qui nous préoccupe, c'est que plusieurs milliers d'attaques ont lieu chaque jour. Nous essayons de les déjouer. Ce projet de loi pose certains problèmes d'échéancier.

Maître Robertson, l'un de vos collègues de la Munk School of Global Affairs & Public Policy a comparu devant notre comité sur un autre sujet et a dit que le mieux ne devait pas devenir l'ennemi du bien. Si vous deviez choisir à ce stade-ci d'adopter le projet de loi tel quel, avec plus de 40 amendements qui ont été apportés à la Chambre des communes — et je comprends bien, maître Robertson, que vous dites qu'ils ne traitent pas adéquatement de certaines des questions liées à l'article 15 — le feriez-vous, avec comme objectif de l'améliorer après coup, ou y mettriez-vous un terme? Ma question s'adresse à vous trois. Madame Quaid, vous pourriez peut-être commencer.

Mme Quaid : Je suis heureuse de ne pas être à votre place. Je l'adopterais probablement parce que nous avons huit ans de retard sur certains de nos homologues pour ce qui est de présenter un projet de loi comme celui-ci. Il a fallu attendre très longtemps. Nous avons perdu la confiance de certains de nos homologues parce que nous n'avons pas ces protections. Je l'adopterais probablement, mais à contrecœur.

Me Robertson : Nous parlons de lacunes historiques qui persistent depuis des décennies. Je n'envie pas non plus votre position. Cependant, pour moi, la décision est claire : nous avons besoin de pouvoirs nous servant de repères pour nous rendre où nous voulons aller. En ce qui concerne les pouvoirs prévus à la partie 1 du projet de loi, ils ne vont pas dans la bonne direction parce qu'il nous faut des dispositions législatives qui stipulent que ni le gouvernement ni les entreprises de télécommunications ne doivent avoir le pouvoir de compromettre nos réseaux.

Ce que sous-entend ce projet de loi — et ce qui n'a pas été abordé la semaine dernière — c'est que ces pouvoirs permettent au gouvernement de compromettre nos solutions de la prochaine

solutions. If we're going to compromise those solutions, then I'm not sure what this bill is for, because functionally it is akin to saying that we should drill holes in the hull of a cruise ship in order to bring more life rafts or balers or life jackets aboard. That, quite frankly, doesn't make sense. We do know that there have been some — I believe it was put last week — arrangements that are being made through various agreements to improve the status quo. But if we're going to create a law on this, it needs to be the right law.

Mr. Shull: I would just preface this comment by saying that I am a huge fan of both Ms. Quaid and Ms. Robertson. I am going to diverge a little bit here. I say, "Pass it, and pass it as quickly as you can." I am a big fan of judicial review, and if you can add in special advocates for the most sensitive aspects, that gets you 95% of the way there. Were it different, I would have offered more amendments, but as it currently stands, it's a pretty good bill and I wouldn't let the perfect get in the way of the good enough.

Also, as it relates to your colleague's previous question, there is an entire ecosystem around this. If I were advising a private client, we would be conducting vendor risk assessments, using threat intelligence and monitoring tools, deploying end-point security solutions, implementing supply chain visibility and inspecting software and firm ware updates. We would be putting authentication controls up and down the chain; we would be red teaming and pen testing our networks and looking for indications of compromise, putting in zero-trust architecture, reviewing vendor-incident reports and requiring disclosures. This bill does not exist on its own. There is an entire ecosystem of cyber-experts and cyber-lawyers like me, who, if we're doing our job properly, we're going to be mitigating the risks my colleagues have done an admirable job of setting out.

Senator Batters: Thank you to all of you for being here and for your important work on these topics. The idea of "Don't let the perfect be the enemy of the good" might be my least favourite expressions. We are the Senate of Canada. It is our job to make bills more perfect. I am the critic of the bill, so I think it's part of my job to help make this bill better.

I also want to point out the House of Commons had this bill for two years. We only received it on the very last day we sat in June. Really, we've just been dealing with it for a bit over a month. We can afford to give it a little bit more time and good scrutiny. After all, we are the body of sober second thought.

génération. Si ces solutions doivent être compromises, je ne sais pas à quoi sert ce projet de loi, car sur le plan fonctionnel, cela s'apparente à percer des trous dans la coque d'un navire de croisière, afin de pouvoir amener plus de radeaux ou de gilets de sauvetage à bord. Franchement, cela n'a pas de sens. Nous savons qu'il y a des dispositions — je crois que cela a été dit la semaine dernière — qui sont en train d'être prises dans le cadre de diverses ententes pour améliorer la situation actuelle. Mais si nous voulons créer une loi à ce sujet, il faut qu'elle soit appropriée.

Me Shull : Je tiens d'abord à dire que je suis une grande admiratrice de Mme Quaid et de Me Robertson. Je vais m'écarter un peu du sujet. Selon moi, il faut l'adopter et le faire le plus rapidement possible. Je suis très partisane du contrôle judiciaire, et s'il est possible d'ajouter des avocats spéciaux pour les aspects les plus délicats, on arrive presque à l'objectif. S'il avait été différent, j'aurais proposé d'autres amendements, mais c'est un assez bon projet de loi dans sa forme actuelle, et je ne laisserais pas le mieux l'emporter sur le bien.

De plus, pour revenir à la question précédente de votre collègue, il y a tout un écosystème autour de cela. Si je conseillais un client privé, nous procéderions à des évaluations des risques des fournisseurs, en utilisant des outils de surveillance et de renseignements sur les menaces, en déployant des solutions de sécurité pour les points de terminaison, en assurant la visibilité de la chaîne d'approvisionnement et en inspectant les mises à jour des logiciels et des programmes intégrés. Nous mettrions en place des contrôles d'authentification en amont et en aval de la chaîne, des équipes rouges et des tests d'intrusion pour nos réseaux, nous chercherions des indications de compromission, nous mettrions en place une architecture de sécurité sans périmètre, nous examinerions les rapports d'incident des fournisseurs et nous exigerions des divulgations. Ce projet de loi n'existe pas seul. Il y a tout un écosystème de cyberexperts et de cyberjuristes comme moi qui, s'ils font bien leur travail, contribueront à atténuer les risques que mes collègues ont si bien exposés.

La sénatrice Batters : Merci à vous tous pour votre présence ici et pour l'important travail que vous faites sur ces sujets. Ne pas laisser le mieux être l'ennemi du bien est peut-être l'expression que je déteste le plus. Nous sommes le Sénat du Canada. C'est notre travail de rendre les projets de loi plus parfaits. Je suis la porte-parole de ce projet de loi, et je crois qu'une partie de mon travail consiste à le bonifier.

Je tiens également à souligner que la Chambre des communes a débattu de ce projet de loi pendant deux ans. Nous ne l'avons reçu que le dernier jour de séance, en juin. En fait, nous nous en occupons depuis un peu plus d'un mois. Nous pouvons nous permettre de lui accorder un peu plus de temps et un examen approfondi. Après tout, nous sommes l'organe de second examen objectif.

I would like to start with Ms. Robertson from the Citizen Lab. What are the most crucial amendments to make to Bill C-26 to improve it and strengthen privacy protections for Canadians? You were referencing your updated brief in your remarks, but we as committee members don't have it yet because it has to be translated before we receive it, so we don't have it today. That's important so that we can have it in both official languages. We don't have it. You were making good references to it, but I haven't been able to see it yet.

I was just looking at clause 15.4, which is a shockingly broad section as it exists right now. Maybe that's something you want to speak about?

Ms. Robertson: Thank you for the question. I certainly understand the disadvantage that the timing of the filing and translation has put the committee in, in terms of consideration of the issues.

I'll start with what is textually both problematic in terms of your question on the core privacy problems because it starts from the exceptionally broad language of clause 15.4, as you note in your question. I would go farther from there to look at some of the measures that are currently being offered or described as the measures for oversight or review.

Right now, judicial review was mentioned last week as a way that the courts will be involved. It is not applicable to the collection power in clause 15.4.

There is a new parliamentary reporting obligation added in the study of Bill C-26 in the House. It is not applicable to the collection power in 15.4. There are new notification obligations for the National Security and Intelligence Review Agency, or NSIRA and the National Security and Intelligence Committee of Parliamentarians, or NSICOP that are not applicable to the minister's collection power in clause 15.4. There is a theme here.

There is also mention made that there is no interception of private communications in this bill. I spoke about how that only carves out a small subset of the data that is at issue and at stake here. One of the other measures that have been proffered — which was proffered during the study of the legislation, I don't believe, as a result of a request for that amendment — which is to cite the Privacy Act, which we know applies. However, the government is not required to comply with the Privacy Act for the totality of its privacy obligations. It's required to comply with the Constitution. Leaving aside the many statements by the Department of Justice Canada, parliamentary committees and the Privacy Commissioner, which have all had a refrain that the Privacy Act is sorely outdated, it is still not enough for this task.

J'aimerais commencer par Me Robertson, de Citizen Lab. Quels sont les amendements les plus cruciaux à apporter au projet de loi C-26 pour l'améliorer et renforcer la protection de la vie privée des Canadiens? Vous avez fait référence à votre mémoire mis à jour dans votre exposé, mais les membres du comité ne l'ont pas encore reçu parce qu'il doit être traduit avant de nous être distribué. Nous ne l'avons donc pas devant nous aujourd'hui. Il est important que nous l'ayons dans les deux langues officielles, ce qui n'est pas le cas. Vous en avez bien parlé, mais je n'ai pas encore eu la chance de le voir.

Je viens d'examiner l'article 15.4, qui a une portée étonnamment vaste dans sa forme actuelle. Est-ce quelque chose dont vous aimeriez parler?

Me Robertson : Je vous remercie de la question. Je comprends tout à fait les inconvénients que représente pour le comité le moment choisi pour déposer le rapport et la nécessité de le faire traduire.

Je vais commencer par ce qui est problématique sur le plan du libellé, dans le contexte de votre question, les problèmes fondamentaux liés à la protection de la vie privée découlant du libellé exceptionnellement général de l'article 15.4, comme vous l'avez souligné. J'irais plus loin en examinant certaines des mesures qui sont actuellement offertes ou décrites comme des mesures de surveillance ou de contrôle.

Le contrôle judiciaire a été mentionné la semaine dernière comme un moyen de faire intervenir les tribunaux, mais il ne s'applique pas au pouvoir de collecte prévu à l'article 15.4.

L'étude du projet de loi C-26 à la Chambre a donné lieu à l'ajout d'une nouvelle obligation de faire rapport au Parlement. Elle ne s'applique pas au pouvoir de collecte dont il est question à l'article 15.4. Il y a aussi de nouvelles obligations de notification pour l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, ou OSSNR, et le Comité des parlementaires sur la sécurité nationale et le renseignement, ou CPSNR, qui ne s'appliquent pas au pouvoir de collecte du ministre prévu à l'article 15.4. Il y a une constante ici.

On dit aussi qu'il n'est pas question d'interception de communication privée dans ce projet de loi. J'ai parlé du fait que cela ne touche qu'un petit sous-ensemble des données qui sont en jeu ici. L'une des autres mesures qui ont été proposées — et qui l'ont été pendant l'étude du projet de loi, sans que ce soit à la suite d'une demande d'amendement, d'après ce que je comprends — est de citer la Loi sur la protection des renseignements personnels, qui, nous le savons, s'applique. Cependant, le gouvernement n'est pas tenu de se conformer à la Loi sur la protection des renseignements personnels pour l'ensemble de ses obligations en cette matière. Il est tenu de respecter la Constitution. Dans ce contexte, il ne suffit pas de laisser de côté les nombreuses déclarations du ministère de la

That's precisely why federal agencies that currently have the authority to collect data from privacy telecommunication companies do not turn to the Privacy Act for their authority. They have specialized legislation that requires that, for a collection power of this extraordinary magnitude — the most private information that our legal system recognizes — the courts review requests, and they can exercise restraints around retention, the scope of use and sharing.

That is the most significant gap in this legislation: The Federal Court has been essentially ousted from a review of the collection power itself. That's what we recommend in recommendation 6, which you will ultimately receive, which refers to the need for Federal Court review. However, recommendation 7 in the brief is also there to recommend that these powers do not balloon, essentially, into surveillance or national security powers. This committee was told that this bill is about cybersecurity and not about national security. However, we know from the departmental positions of national security bodies like the CSE, data received for cybersecurity purposes will be used across its mandate. That ballooning effect should be constrained through what I recommend as recommend 7, which is to limit the use of this data to cybersecurity mandates alone.

Senator Batters: Thank you. I will go on a second round, if there is one.

Senator Dasko: Thank you to our witnesses for being here. My questions are for Ms. Quaid and Ms. Robertson.

You've each expressed some criticisms of the bill. Ms. Quaid, you were calling for a broader approach — safe harbour laws going, as you said, below the threshold in some ways. Ms. Robertson, you seem to be suggesting something different. I think you're saying that the bill perhaps doesn't go quite far enough, but, Ms. Robertson, you're saying it perhaps goes too far because it has powers that place privacy at risk through the powers in the bill.

I don't think I've ever asked a question quite this way, but I would like to ask Ms. Quaid this: What do you think about the concerns that Ms. Robertson has? Please stick with substantive issues as opposed to — do you share any of the concerns that she has expressed?

Justice, des comités parlementaires et du commissaire à la protection de la vie privée, qui ont tous dit que la Loi sur la protection des renseignements personnels était terriblement désuète.

C'est précisément pour cette raison que les organismes fédéraux qui ont actuellement le pouvoir de recueillir des données auprès d'entreprises de télécommunications ne tirent pas ce pouvoir de la Loi sur la protection des renseignements personnels. Ils se conforment à des lois spécialisées qui exigent que, pour un pouvoir de collecte d'une telle ampleur — les renseignements les plus privés que notre système juridique reconnaît —, les tribunaux examinent les demandes et puissent imposer des restrictions concernant la conservation, la portée de l'utilisation et le partage.

C'est la lacune la plus importante de ce projet de loi : même la Cour fédérale a été essentiellement écartée de l'examen du pouvoir de collecte. C'est ce que nous avons inclus dans la recommandation 6, dont vous finirez par prendre connaissance, qui fait référence à la nécessité d'un contrôle par la Cour fédérale. Cependant, la recommandation 7 du mémoire recommande également que ces pouvoirs ne se transforment pas en pouvoirs liés à la surveillance ou à la sécurité nationale. On a dit au comité que ce projet de loi concerne la cybersécurité et non la sécurité nationale. Cependant, nous savons, d'après les positions prises par des organismes de sécurité nationale comme le CST, que les données reçues à des fins de cybersécurité seront utilisées dans le cadre de leur mandat. Cet effet devrait être restreint par ce qui est compris dans la recommandation 7, c'est-à-dire limiter l'utilisation de ces données aux seuls mandats de cybersécurité.

La sénatrice Batters : Merci. Je poursuivrai mes questions au deuxième tour, s'il y en a un.

La sénatrice Dasko : Je remercie nos témoins de leur présence. Mes questions s'adressent à Mme Quaid et à Me Robertson.

Vous avez toutes les deux formulé des critiques à l'égard du projet de loi. Madame Quaid, vous demandiez une approche plus large, c'est-à-dire des lois d'exonération s'appliquant, comme vous l'avez dit, aux situations qui dépassent les seuils à certains égards. Maître Robertson, vous semblez proposer quelque chose de différent. Je pense que vous dites que le projet de loi ne va peut-être pas assez loin, mais vous dites aussi qu'il va peut-être trop loin parce qu'il comporte des pouvoirs qui présentent des risques au chapitre de la protection de la vie privée.

Je ne crois pas avoir déjà posé une telle question, mais j'aimerais demander à Mme Quaid ce qu'elle pense des préoccupations de Me Robertson. Veuillez vous en tenir à des questions de fond plutôt qu'à... Partagez-vous les préoccupations qu'elle a exprimées?

Ms. Quaid: Of course I do, but I'm not a privacy expert, and I am certainly not a privacy lawyer with that depth and breadth of understanding and knowledge.

Senator Dasko: But calling for changes, as I understand them, that might actually lower the threshold for privacy considerations.

Ms. Quaid: No. Let me clarify that. The change that I am calling for is the addition of enabling safe harbour protection for the six sectors that have been impacted by this legislation. Safe harbour protection would simply enable those companies to talk about things with the greater public without fear of legal reprisals. In other words, it enables them to share information about things they are seeing, doing and experiencing without fear of lawsuits.

That's all I'm asking for. It has nothing to do with the privacy piece that Ms. Robertson has so eloquently spoken to.

Senator Dasko: It wouldn't jeopardize any privacy if companies were in a position to share more information? It certainly sounds as if it could go in that direction.

Ms. Quaid: The types of information they would share would be information about their cybersecurity systems and their policies and procedures — no personal information.

Senator Dasko: Would you care to comment? Perhaps I would ask you what you think about Ms. Quaid's suggestions.

Ms. Robertson: The coincidence is that we had —

Senator Dasko: You both make a great deal of sense, so I'm trying to see if there might be some sort of common ground between you in what you're saying. Even though you're speaking about different aspects of it, I see similarities in the areas you're addressing. I'm just trying to see if there is a common ground at all.

Ms. Robertson: Yes. I don't believe there is a misalignment between the recommendations and the topics that we are addressing this committee on. There are different aspects of the effects of this legislation.

I agree with Ms. Quaid's comments. They resonate because we have — and I have in my brief — ultimately talked about the importance of the public's right to understand their own cybersecurity and that there have been legacy deficiencies that have exposed people around the world to pervasive insecurity and historical telecommunication networks that were never designed to be secure in the first place; that wasn't their originating purpose. However, there has been excessive secrecy

Mme Quaid : Bien sûr que oui, mais je ne suis pas une experte de la protection de la vie privée, et je ne suis certainement pas une avocate spécialisée dans ce domaine, qui possède des connaissances aussi approfondies.

La sénatrice Dasko : Si j'ai bien compris, demander des changements pourrait en fait abaisser le seuil de protection de la vie privée.

Mme Quaid : Non. Permettez-moi de clarifier cela. Le changement que je demande, c'est l'ajout d'une disposition d'exonération pour les six secteurs touchés par ce projet de loi. Cela permettrait simplement aux entreprises visées d'avoir des discussions publiques sur certaines choses, sans crainte de représailles légales. Autrement dit, cela leur permettrait de partager des informations sur des choses qu'elles voient, font et vivent sans craindre des poursuites.

C'est tout ce que je demande. Cela n'a rien à voir avec les aspects de la protection de la vie privée dont Me Robertson a parlé avec tant d'éloquence.

La sénatrice Dasko : Si des entreprises étaient en mesure de partager plus de renseignements, cela ne compromettrait-il pas la protection de la vie privée? Il semble certainement que les choses pourraient aller dans cette direction.

Mme Quaid : Les types de renseignements qu'elles partageraient concerneraient leurs systèmes de cybersécurité et leurs politiques et procédures; il ne s'agirait pas de renseignements personnels.

La sénatrice Dasko : Avez-vous quelque chose à dire à ce sujet? J'aimerais vous demander ce que vous pensez des suggestions de Mme Quaid.

Me Robertson : Ce qui coïncide, c'est que nous avions...

La sénatrice Dasko : Ce que vous dites toutes les deux a beaucoup de sens, alors j'essaie de voir s'il y aurait des éléments communs entre ce que vous dites chacune de votre côté. Même si vous en parlez sous des angles différents, je vois des similitudes dans les domaines que vous abordez. J'essaie simplement de voir s'il y a des éléments communs.

Me Robertson : Oui. Je ne vois pas de décalage entre les recommandations et les sujets que nous abordons devant ce comité. Il y a différents aspects aux effets de ce projet de loi.

Je suis d'accord avec les observations de Mme Quaid. Elles font écho aux nôtres, parce que ce dont nous parlons — et je l'ai mentionné dans mon mémoire —, en fin de compte, c'est de l'importance du droit du public de comprendre la cybersécurité de son point de vue, ainsi que du fait que des lacunes se sont perpétuées et ont exposé les gens du monde entier à une insécurité généralisée et à des réseaux de télécommunications qui n'ont jamais été conçus pour être sécuritaires, car ce n'était

in how telecommunication providers operate, intermediate and are regulated in, essentially, a self-regulated way. That has meant that individuals and external, independent cybersecurity experts have not had access to the type of information to fully understand the extent of those threats.

That's why we have recommended in what you will ultimately see as recommendations 1 to 5, I believe, of my brief. They are textual changes to make this bill less excessive in terms of its potential secrecy, because as cybersecurity is a team sport, the public have a right to know. No one's suggesting there should be mandatory reporting on unpatched vulnerabilities, which was a reason offered for why the orders have nondisclosure provisions attached to them. However, that specific reason for secrecy is much narrower than the potential secrecy that we may see in whether the government ultimately requires our networks to be secure at a network level. That's why we say that if there is secrecy, it should be narrowly constrained. Specifically, we've agreed with the civil society recommendation that if there is going to be a nondisclosure order beyond, let's say, a period of three months, Federal Courts should have to approve any extension of that secrecy or nondisclosure.

Senator Richards: My question has been answered a dozen times. That's what I get for being last. Thanks very much for being here.

I have a quick question: How big a divide do you see between security and individual privacy, and how can your recommendation be integrated into the bill without losing what the actual bill intends? If there are amendments on these recommendations, how will they ever get passed in the other place?

I'm asking Ms. Robertson that.

Ms. Robertson: I see. I will have to, unfortunately, leave the political analysis to political experts. I'm here as a constitutional law expert who has very talented colleagues who have expertise in cybersecurity and technology. This should be a non-partisan issue because, as we're seeing unfolding in the United States at present, there are systemic vulnerabilities that this bill should be focused on ameliorating. However, right now, this bill carries powers that will potentially compromise the very solutions to these problems, and so we are asking for targeted, specific amendments to ensure that, as I indicated earlier today, our compass is pointed in the right direction. I have a number of specific amendments that are included in our brief that provide specific textual language as to how to accomplish these goals.

pas leur but à l'origine. Cependant, il y a eu une discrétion excessive quant à la façon dont les fournisseurs de services de télécommunications fonctionnent, agissent comme intermédiaires et sont réglementés, à savoir qu'ils s'autoréglementent essentiellement. Cela signifie que des personnes et des experts externes et indépendants en cybersécurité n'ont pas eu accès au type d'information qui leur aurait permis de comprendre pleinement l'ampleur de ces menaces.

C'est la raison de la teneur des recommandations 1 à 5, je crois, de mon mémoire. Il s'agit de changements de libellé visant à rendre le projet de loi moins excessif en ce qui concerne la confidentialité potentielle, car comme la cybersécurité est un sport d'équipe, le public a le droit de savoir. Personne ne laisse entendre qu'il devrait y avoir une obligation de rendre compte des vulnérabilités non corrigées, ce qui explique pourquoi les décrets sont assortis de dispositions de non-divulgation. Cependant, cette motivation précise au chapitre de la confidentialité est beaucoup plus étroite que ne le justifie la situation, à savoir que le gouvernement exige en fin de compte que nos réseaux soient entièrement sécurisés. C'est pourquoi nous disons qu'il devrait y avoir des restrictions étroites en matière de confidentialité. Plus précisément, nous avons accepté la recommandation de la société civile, selon laquelle si un décret de non-divulgation devait s'étendre au-delà, disons, d'une période de trois mois, cela devrait être approuvé par des cours fédérales.

Le sénateur Richards : On a déjà répondu à la question que j'avais une dizaine de fois. C'est ce qui arrive lorsque l'on est le dernier à intervenir. Merci beaucoup d'être ici.

J'ai une brève question à vous poser. Selon vous, quelle est la largeur du fossé entre la sécurité et la protection des renseignements personnels, et comment votre recommandation peut-elle être intégrée dans le projet de loi sans perdre de vue l'objectif réel de ce dernier? S'il y a des amendements découlant de ces recommandations, comment seront-ils adoptés à l'autre endroit?

Je pose la question à Me Robertson.

Me Robertson : Je comprends. Malheureusement, je vais devoir laisser l'analyse politique aux experts de ce domaine. Je suis ici en tant qu'experte en droit constitutionnel, et j'ai des collègues très talentueux qui ont une expertise en cybersécurité et en technologie. Cette question devrait être non partisane parce que, comme nous le voyons actuellement aux États-Unis, il y a des vulnérabilités systémiques que ce projet de loi devrait viser à régler. Cependant, à l'heure actuelle, ce projet de loi confère des pouvoirs qui pourraient aller jusqu'à compromettre les solutions à ces problèmes. Nous demandons donc des amendements ciblés et précis pour nous assurer, comme je l'ai dit plus tôt aujourd'hui, que nos repères vont dans la bonne direction. J'ai un certain nombre d'amendements précis qui figurent dans notre

Senator Richards: I wasn't asking you how they would get past — I was referring to that for myself, but thank you very much.

The Chair: This brings us to the end of our time with this panel, but many of you would like to continue. Thank you, Ms. Quaid, Ms. Robertson, and Mr. Shull, for sharing your insights and taking the time to meet with us today. It's relatively rare that as many senators as we saw today want to hear answers from all three witness, so that is very much a commendation toward your knowledge, skills and insightful contributions, so thank you for helping us today with this important piece of legislation.

Colleagues, we're meeting to continue our consideration of Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.

Next hour, we have the pleasure of welcoming from the Canadian Chamber of Commerce, Ulrike Bahr-Gedalia, Senior Director, Digital Economy, Technology and Innovation, and from IBM Canada, Tiéoulé Traoré, Executive, Government and Regulatory Affairs, and Daina Proctor, Executive, Cybersecurity Services, and from the Canadian Telecommunications Association, Eric Smith, Senior Vice-President. Thank you very much for meeting with us today.

We now invite you to make your opening remarks to be followed by questions from our members. And we will begin this evening with Ulrike Bahr-Gedalia from the Canadian Chamber of Commerce. Please begin when you're ready.

Ulrike Bahr-Gedalia, Senior Director, Digital Economy, Technology and Innovation, Canadian Chamber of Commerce: Mr. Chair, members of the Senate, good evening, my name is Ulrike Bahr-Gedalia and I'm the Canadian Chamber's policy lead for the Digital Economy Committee, Future of Artificial Intelligence Council and Cyber. Right. Now. Council.

As Canada's largest and most activated business network representing over 400 chambers of commerce and boards of trade, as well as more than 100 associations and over 200,000 businesses of every size from all regions and economic sectors of Canada, the Canadian Chamber is pleased to once again provide feedback on Bill C-26 following our appearance before the

mémoire et qui fournissent un libellé précis sur la façon d'atteindre ces objectifs.

Le sénateur Richards : Je ne vous demandais pas comment ils pourraient être adoptés. Ce n'était qu'une réflexion que je me faisais à moi-même, mais merci beaucoup.

Le président : Nous arrivons à la fin de la séance avec ce groupe de témoins, même si bon nombre d'entre vous aimeraient continuer. Merci, madame Quaid, maître Robertson et maître Shull, de nous avoir fait part de vos réflexions et d'avoir pris le temps de nous rencontrer aujourd'hui. Il est relativement rare qu'autant de sénateurs veuillent entendre les réponses des trois témoins, comme cela a été le cas aujourd'hui. Je vous félicite donc de vos connaissances, de vos compétences, ainsi que de votre contribution éclairée. Je vous remercie également de nous avoir aidés aujourd'hui à étudier cette importante mesure législative.

Chers collègues, nous poursuivons notre étude du projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois.

Au cours de la prochaine heure, nous avons le plaisir d'accueillir Ulrike Bahr-Gedalia, directrice principale, Économie numérique, technologie et innovation, de la Chambre de commerce du Canada, ainsi que Tiéoulé Traoré, directeur, Affaires gouvernementales et réglementaires, et Daina Proctor, directrice, Services de cybersécurité, chez IBM Canada, de même qu'Eric Smith, vice-président principal de l'Association canadienne des télécommunications. Merci beaucoup d'être venus nous rencontrer aujourd'hui.

Nous vous invitons maintenant à faire votre déclaration préliminaire, après quoi les membres du comité vous poseront des questions. Nous allons d'abord donner la parole à Ulrike Bahr-Gedalia, de la Chambre de commerce du Canada. Veuillez commencer lorsque vous serez prête.

Ulrike Bahr-Gedalia, directrice principale, Économie numérique, technologie et innovation, Chambre de commerce du Canada : Monsieur le président, membres du Sénat, bonsoir. Je me nomme Ulrike Bahr-Gedalia, et je suis directrice principale de l'économie numérique à la Chambre de commerce du Canada. Je suis également responsable des politiques pour le Comité de l'économie numérique, le Conseil sur l'avenir de l'intelligence artificielle et le programme La Cybersécurité. Dès. Maintenant.

En tant que réseau d'affaires le plus important et le plus dynamique au Canada, représentant plus de 400 chambres de commerce, une centaine d'associations et plus de 200 000 entreprises de toutes tailles et de tous les secteurs économiques du Canada, la Chambre de commerce du Canada est honorée d'être à nouveau invitée à vous faire part de ses commentaires

House of Commons Standing Committee on Public Safety and National Security, or SECU, in February.

I'd like to start off by acknowledging the adoption of some changes the Canadian Chamber had put forward during the bill's committee study, the deletion of clause 10, thereby restoring due diligence defence, removal of the requirement for immediate reporting of cybersecurity incidents and harmonization with existing obligations.

I'd also liked to acknowledge the recent appointment of Sami Khoury as a senior government official for cyber security, a role and responsibility the Canadian Chamber's Cyber. Right. Now. Council had been advocating for over the past two years, with a goal to ensure policy coherence, coordination of cybersecurity activities and initiatives, and alignment of resources across the government, all while increasing and improving two-way information sharing, which was also a concern we had expressed during our previous appearance.

While we are pleased to see the House SECU committee conclude their study on Bill C-26 and support the bill overall, certain amendments are still needed at this stage to ensure the bill reaches its full potential.

More specifically, with respect to the Telecommunications Act, while we applaud the House for making important changes to the bill, including a due diligence defence for administrative monetary penalties, we remain concerned that the bill suggests companies can be compensated for changes they may have to make under this regime. We believe the Senate should amend the legislation to allow the minister or Governor in Council to award compensation on a case-by-case basis.

With respect to the Critical Cyber Systems Protection Act, or CCSPA, our members continue to seek the following improvements: Two-way information sharing; as currently drafted, the CCSPA only contemplates one-way information sharing from designated operators to the government. We believe this is a missed opportunity and a potential weakness; a clearer definition of a reportable cybersecurity incident. This will ensure industry is not forced to report events that do not pose a material threat to a vital system. Failure to clearly define the parameters for a reportable incident will undermine the purpose of the bill and overwhelm government authorities who will have to process each cyber incident reported.

sur le projet de loi C-26, à la suite de notre intervention devant le Comité permanent de la sécurité publique et nationale en février dernier.

J'aimerais commencer par saluer l'adoption de certains changements proposés par la Chambre de commerce lors de l'étude du projet de loi en comité, la suppression de l'article 10, rétablissant ainsi la défense de diligence raisonnable; le retrait de l'obligation de signaler immédiatement les incidents de cybersécurité; l'harmonisation avec les obligations existantes.

J'aimerais également faire mention de la récente nomination de Sami Khoury en tant qu'agent supérieur pour la cybersécurité, un rôle et une responsabilité pour laquelle la Chambre de commerce du Canada a plaidé dans le cadre du programme La Cybersécurité. Dès. Maintenant., au cours des deux dernières années, dans le but d'assurer la cohérence des politiques, la coordination des activités et des initiatives en matière de cybersécurité et l'alignement des ressources au sein du gouvernement, tout en augmentant et en améliorant le partage bilatéral d'informations, ce qui était également une préoccupation que nous avions exprimée lors de notre précédent témoignage.

Bien que nous soyons heureux de voir le Comité permanent de la sécurité publique et nationale de la Chambre des communes conclure son étude sur le projet de loi C-26, et que nous soutenions le projet de loi dans son ensemble, certains amendements sont encore nécessaires à ce stade pour s'assurer que le projet de loi atteigne son plein potentiel.

Plus précisément, en ce qui concerne la Loi sur les télécommunications : bien que nous applaudissions la Chambre d'avoir apporté des modifications importantes au projet de loi, y compris en ce qui concerne la défense de diligence raisonnable pour les sanctions administratives pécuniaires, nous demeurons préoccupés par le fait que le projet de loi laisse entendre que les sociétés ne peuvent pas être indemnisées pour les changements qu'elles pourraient devoir apporter dans le cadre de ce régime. Nous pensons que le Sénat devrait amender la législation pour permettre au ministre ou au gouverneur en conseil d'accorder des compensations au cas par cas.

En ce qui concerne la Loi sur la protection des cybersystèmes essentiels, ou LPCE, nos membres continuent à demander les améliorations suivantes, à savoir, le partage bilatéral de l'information. Dans sa version actuelle, la LPCE envisage seulement un partage d'information à sens unique entre les opérateurs désignés et le gouvernement. Nous pensons qu'il s'agit là à la fois d'une erreur et d'une faille potentielle; une définition plus claire de ce qu'est un incident de cybersécurité devant faire l'objet d'un rapport. Ainsi, l'industrie ne serait pas obligée de faire des rapports sur des événements qui ne représentent pas une menace sérieuse pour un système vital. L'absence de définition claire des paramètres d'un incident à

Another area of concern is the continued rise of ransomware incidents. In this context, we commend Canada in its involvement in the International Counter Ransomware Initiative, or CRI, which includes the development of a CRI public-private sector advisory panel.

The following facts emphasize the severity and urgency for more action on this issue. The RCMP states that almost 60% of cyber incidents reported to its national cyber crime coordination centre are ransomware attacks. The Canadian Centre for Cyber Security calls ransomware the most disruptive form of cyber crime facing Canada, and the most recent national cyber threat assessment report notes that ransomware is the top cyber threat facing Canada's critical infrastructure, and Bill C-26 is about protecting Canada's critical infrastructure.

While this bill has increased visibility of ransomware and other cyber-threats, we believe the issue of ransomware requires more public discussion and study and would encourage the Senate to look into how this scourge is affecting our country beyond the critical infrastructure sectors that the federal government focused on in this bill.

As more collective action and coordination to combat this growing challenge is required, the Canadian Chamber, together with the Cyber. Right. Now. Council, will be hosting their second cyber security and ransomware Hill Day later this month to discuss these challenges and opportunities with senior government officials from across government departments, ministries and agencies.

To conclude, we would like to stress the urgency to pass the bill so we can move on to developing the regulations and implementation framework. The clock is ticking, and the geopolitical environment continues to get worse, as does cyber crime.

Thank you for listening and for the continued opportunity to participate in the study of Bill C-26.

The Chair: Thank you.

signaler nuit à l'objectif du projet de loi et submergera les autorités gouvernementales, qui devront traiter et évaluer chaque cyberincident signalé.

Une autre source de préoccupation majeure est la hausse continue des incidents liés aux rançongiciels. Dans ce contexte, nous félicitons le Canada pour sa participation à l'Initiative de lutte contre les rançongiciels — ou ILR — internationale, qui comprend la mise en place d'un groupe consultatif du secteur public-privé.

Les faits suivants illustrent la gravité de la situation et l'urgence d'agir dans ce domaine. La GRC affirme que près de 60 % des cyberincidents signalés à son Centre national de coordination en cybercriminalité sont des attaques par rançongiciel. Le Centre canadien pour la cybersécurité qualifie les rançongiciels de « forme de cybercriminalité la plus perturbatrice à laquelle le Canada est confronté ». Sa plus récente Évaluation des cybermenaces nationales indique que le rançongiciel est la principale menace cybercriminelle à laquelle sont confrontées les infrastructures essentielles du Canada. Or, le projet de loi C-26 vise à protéger les infrastructures essentielles du Canada.

Bien que le projet de loi contribue à accroître la vigilance à l'égard des rançongiciels et d'autres cybermenaces, nous pensons que la problématique des rançongiciels nécessite davantage de discussions et d'études sur la place publique et nous encourageons le Sénat à examiner la manière dont ce fléau affecte notre pays au-delà des infrastructures essentielles sur lesquelles le gouvernement fédéral a concentré ses efforts dans le cadre du projet de loi.

Comme il faut davantage de mesures collectives et une meilleure coordination pour lutter contre ce défi croissant, la Chambre de commerce, en collaboration avec son programme La Cybersécurité. Dès. Maintenant., organisera sa deuxième Journée sur la Colline sur la cybersécurité et le rançongiciel à la fin du mois au cours de laquelle nous discuterons avec de hauts fonctionnaires de l'ensemble des ministères, services et organismes gouvernementaux.

Pour terminer, nous souhaitons insister sur l'urgence d'adopter le projet de loi, afin que nous puissions passer à l'élaboration des réglementations et du cadre de mise en œuvre. Le temps presse et l'environnement géopolitique continue de se dégrader, parallèlement à la cybercriminalité qui ne cesse de s'aggraver.

Je vous remercie de m'avoir écoutée et de m'avoir donné l'occasion de participer à l'étude du projet de loi C-26.

Le président : Merci.

[*Translation*]

Tiéoulé Traoré, Executive, Government and Regulatory Affairs, IBM Canada: Thank you, Mr. Chair. On behalf of IBM Canada, thank you for the opportunity to appear before the committee regarding Bill C-26.

[*English*]

This testimony — focused on Part 2 of the bill — will largely repeat the points initially made before the House of Commons Standing Committee on Public Safety and National Security last winter,

IBM continues to support the essence of this bill, an initiative made necessary in the wake of the digitization of the global economy, and the subsequent rise of cybercrimes. Cybersecurity protocols are not "nice to haves": they are essential components of the foundations of business and governments.

Critical infrastructure is the number one target of cyber breaches, with each instance costing on average $9 million. Canada being a G7 country, it should indeed lead by example in this crucial file.

Last winter, we highlighted what we saw as issues that could prevent the government from truly fulfilling the bold mission embedded in Bill C-26. Months later, we are still of the belief that Bill C-26 should strive to clean up definitions, seek broader alignments with more mature cyber systems and avoid the excessive and unfair targeting of individuals.

Having discussed these topics with the House of Commons Standing Committee on Public Safety and National Security in February, my colleague, Ms. Proctor, will now provide additional points for each recommendation.

Daina Proctor, Executive, Cyber Security Services, IBM Canada: Thank you for the opportunity to discuss this important bill. My name is Daina Proctor, I'm a security executive with IBM.

Having had the opportunity to listen to last week's testimony, I resonate with much of the commentary and also share many of the same concerns expressed.

The recent CRA breach highlighted the concern for existing government bodies to effectively consume and communicate the breach and breach awareness. It highlighted the challenges with our private and public partnerships, which we all recognize are essential if we are to collectively raise the bar for securing our nation's critical infrastructure, which is ultimately the goal of Bill C-26.

[*Français*]

Tiéoulé Traoré, directeur, Affaires gouvernementales et réglementaires, IBM Canada : Merci, monsieur le président. IBM Canada remercie ce comité de l'occasion de témoigner sur le projet de loi C-26.

[*Traduction*]

Ce témoignage — qui est axé sur la partie 2 du projet de loi — reprendra pour une large part les points soulevés initialement devant le Comité permanent de la sécurité publique et nationale de la Chambre des communes, l'hiver dernier.

IBM continue d'appuyer l'essence de ce projet de loi, lequel a été rendu nécessaire dans la foulée de la numérisation de l'économie mondiale et de l'augmentation subséquente des cybercrimes. Les protocoles de cybersécurité ne sont pas « bons à avoir » : ils sont des éléments essentiels des fondements des entreprises et des gouvernements.

Les infrastructures essentielles sont la cible numéro un des cyberatteintes, et chaque cas coûte en moyenne 9 millions de dollars. Comme le Canada est un pays du G7, il devrait effectivement donner l'exemple dans ce dossier crucial.

L'hiver dernier, nous avons souligné ce que nous considérions comme des problèmes qui pourraient empêcher le gouvernement de vraiment remplir la mission audacieuse inscrite dans le projet de loi C-26. Des mois plus tard, nous croyons toujours que le projet de loi C-26 devrait viser à épurer les définitions, à s'aligner davantage avec des systèmes cybernétiques plus matures et à éviter le ciblage excessif et injuste de personnes.

Comme elle a discuté de ces sujets avec le Comité permanent de la sécurité publique et nationale de la Chambre des communes en février, ma collègue, Mme Proctor, présentera maintenant des points supplémentaires pour chaque recommandation.

Daina Proctor, directrice, Services de cybersécurité, IBM Canada : Je vous remercie de me donner l'occasion de discuter de cet important projet de loi. Je m'appelle Daina Proctor, et je suis directrice de la sécurité chez IBM.

J'ai eu l'occasion d'écouter les témoignages de la semaine dernière, et je suis d'accord avec une bonne partie des commentaires et des préoccupations exprimés.

La récente atteinte à la vie privée à l'Agence du revenu du Canada a mis en évidence la préoccupation des organismes gouvernementaux actuels en ce qui a trait aux atteintes à la sécurité et à la sensibilisation à ce chapitre. Elle a fait ressortir les défis que posent les partenariats entre les secteurs public et privé, qui, nous le reconnaissons tous, sont essentiels si nous voulons collectivement rehausser la barre en matière de protection des infrastructures essentielles de notre pays, ce qui est l'objectif ultime du projet de loi C-26.

Contrary to some of the testimony from last week, however, I would offer that there remain concerning misalignments with international standards and overreach of government that collectively are counter to the private and public partnership we are all seeking and are equally causing a chilling effect on our cybersecurity professionals.

It's well documented and known that skilled and experienced cybersecurity professionals are in short supply. Statistics indicate that at the moment there are over 28,000 rules open right now in Canada, however, chief security officers, or CSOs, are equally leaving the industry more now than ever due to the burn out they're experiencing.

I have found in my personal discussions with chief information officers CIOs and CSOs across the country, that Bill C-26 has inspired many to prepare resignation letters. There are a number of reasons why this chilling effect, as expressed in my appearance earlier this year, is occurring, but with time in my mind I just want to talk about two of them.

First is misalignment with international standards. The legislation penalizes victims of cybersecurity incidents through overly punitive compounding fines. This unfairly assumes the cyber security threat is the result of negligence. A criminal conviction can be imposed, a criminal conviction that can impose up to two years' imprisonment. An uncapped fine, a personal liability on the part of an individual, despite the absence of prosecution or a conviction.

Respectfully, the enforcement actions that may be taken against individuals should be removed. At a minimum, we offer that there should be a defined standard to demonstrate objective and substantiated culpability and that scope be expanded to apply equally to our federal government agencies.

The next concern is with overreach of government. While IBM recognizes the need for compliance oversight, we suggest the government's involvement be clearly articulated and limited to what is needed to enforce the provisions of Bill C-26. IBM recommends specifying and limiting the powers of regulatory authorities and related individuals. The power to impose remedial actions, for example, should be strictly restricted to critical situations meeting specific non-compliance thresholds. IBM suggests incorporating clear language outlining the steps that must be taken to mitigate cyber risks while ensuring that responsibility is appropriate but also proportionate to the risks involved.

Contrairement à certains témoignages de la semaine dernière, cependant, je dirais qu'il continue d'y avoir des manques d'harmonisation préoccupants par rapport aux normes internationales et de trop grands pouvoirs pour le gouvernement, ce qui, collectivement, va à l'encontre du partenariat privé et public que nous recherchons tous, et ce qui a également un effet paralysant sur nos professionnels de la cybersécurité.

Il est bien documenté et bien connu que les professionnels de la cybersécurité qualifiés et expérimentés sont rares. Les statistiques indiquent qu'à l'heure actuelle, on compte plus de 28 000 règles ouverte au Canada, mais les dirigeants principaux de la sécurité, ou DPS, quittent l'industrie plus que jamais, à cause de l'épuisement professionnel qu'ils subissent.

Au cours de mes entretiens personnels avec des dirigeants principaux de l'information et des DPS de partout au pays, j'ai constaté que le projet de loi C-26 en a incité beaucoup à rédiger des lettres de démission. Il y a un certain nombre de raisons qui expliquent cet effet paralysant, comme je l'ai dit lors de ma comparution plus tôt cette année, mais compte tenu du temps dont je dispose, je vais simplement en aborder deux.

Premièrement, il y a un manque d'harmonisation avec les normes internationales. Le projet de loi pénalise les victimes d'incidents de cybersécurité en imposant des amendes cumulatives excessivement punitives, ce qui suppose injustement que la menace à la cybersécurité est le résultat d'une négligence. Cela peut entraîner une condamnation au criminel, laquelle peut se traduire par une peine d'emprisonnement pouvant aller jusqu'à deux ans, une amende non plafonnée, ainsi qu'une responsabilité personnelle pour quelqu'un, malgré l'absence de poursuite ou de condamnation.

Avec tout le respect que je vous dois, les mesures d'application de la loi qui peuvent être prises contre des personnes devraient être retirées. À tout le moins, nous proposons qu'il y ait une norme définie pour démontrer la culpabilité de façon objective et corroborée, et que cette norme soit élargie pour s'appliquer également à nos organismes du gouvernement fédéral.

La deuxième préoccupation concerne les pouvoirs trop grands du gouvernement. Bien qu'IBM reconnaisse la nécessité d'une surveillance de la conformité, nous suggérons que la participation du gouvernement soit clairement définie et limitée à ce qui est nécessaire pour appliquer les dispositions du projet de loi C-26. IBM recommande de préciser et de limiter les pouvoirs des organismes de réglementation et de leurs responsables. Le pouvoir d'imposer des mesures correctives, par exemple, devrait être strictement limité aux situations critiques répondant à des seuils de non-conformité précis. IBM suggère d'intégrer un libellé clair décrivant les mesures à prendre pour atténuer les risques cybernétiques, tout en veillant à ce que la responsabilité soit appropriée, mais qu'elle soit aussi proportionnelle aux risques en cause.

In conclusion, we believe that enhanced harmonization with international standards, revision away from the punitive elements, and clear safeguards from potential government overreach would strengthen Bill C-26's mandate to protect our critical infrastructure and encourage further private and public partnerships.

Thank you so much for your time. I look forward to your questions.

The Chair: Thank you very much, Mr. Traoré and Ms. Proctor. Finally, Mr. Eric Smith from the Canadian Telecommunications Association. Welcome. Please commence whenever you're ready.

Eric Smith, Senior Vice-President, Canadian Telecommunications Association: Thank you. 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.

I appreciated the opportunity to appear before you today to present our perspective on Bill C-26.

The security of Canada's telecommunications system is of the utmost importance. Accordingly, our members invest significant resources to safeguard their systems and infrastructure from cyberattacks and other threats. Members also actively participate in the Canadian Security Telecommunications Advisory Committee, or CSTAC, 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 telecommunication systems, including cybersecurity threats.

In addition to providing connectivity services, many of our telecommunications service providers also deliver cybersecurity solutions to businesses across the country, helping them protect against cyberattacks. In other words, our industry takes security seriously and is committed to the security of the Canadian telecommunications system.

In our submission to the House of Commons Standing Committee on Public Safety and National Security, we raised several concerns with the initial version of Bill C-26 as it relates to the proposed amendments to the Telecommunications Act. We're pleased to see that the amendments to the bill put forward by the House committee reflect many of our recommendations, including placing additional safeguards around order-making powers, adding a list of factors that must be considered before an

En conclusion, nous croyons qu'une meilleure harmonisation avec les normes internationales, une révision qui s'éloignerait des éléments punitifs et des mesures de protection claires contre une intervention excessive du gouvernement renforceraient le mandat du projet de loi C-26, qui est de protéger nos infrastructures essentielles et d'encourager la création de nouveaux partenariats entre les secteurs public et privé.

Merci beaucoup de votre temps. Je serai heureuse de répondre à vos questions.

Le président : Merci beaucoup, monsieur Traoré et madame Proctor. Enfin, c'est au tour de M. Eric Smith, de l'Association canadienne des télécommunications. Soyez le bienvenu. Veuillez commencer dès que vous serez prêt.

Eric Smith, vice-président principal, Association canadienne des télécommunications : Merci. Bonsoir. L'Association canadienne des télécommunications est déterminée 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 calibre mondial du Canada, les construisent, les entretiennent et les exploitent.

Je suis heureux d'avoir l'occasion de comparaître devant vous aujourd'hui pour vous présenter notre point de vue sur le projet de loi C-26.

La sécurité du système de télécommunications du Canada est de la plus haute importance. Par conséquent, nos membres investissent des ressources considérables pour protéger leurs systèmes et leurs infrastructures contre les cyberattaques et d'autres menaces. Ils participent également activement au Comité consultatif canadien pour la sécurité des télécommunications, ou CCCST, qui facilite l'échange d'information entre les secteurs privé et public, ainsi que la collaboration stratégique sur les enjeux actuels et en évolution qui peuvent avoir une incidence sur les systèmes de télécommunications, y compris les menaces à la cybersécurité.

En plus de fournir des services de connectivité, bon nombre de nos fournisseurs de services de télécommunications offrent également des solutions de cybersécurité aux entreprises partout au pays, ce qui les aide à se protéger contre les cyberattaques. Autrement dit, notre industrie prend la sécurité au sérieux et s'engage à assurer la sécurité du système canadien de télécommunications.

Dans le mémoire que nous avons présenté au Comité permanent de la sécurité publique et nationale de la Chambre des communes, nous avons soulevé plusieurs préoccupations au sujet de la version initiale du projet de loi C-26 en ce qui concerne les modifications proposées à la Loi sur les télécommunications. Nous sommes heureux de constater que les amendements au projet de loi proposés par le comité de la Chambre reflètent bon nombre de nos recommandations, y compris l'ajout de mesures

order is made, requiring that orders must be proportional to the gravity of the perceived threat, expanding the definition of "confidential information" to include personal information and de-identified information, and reinstating the due diligence defence for violations of orders.

de protection supplémentaires concernant le pouvoir de prendre des décrets, l'inclusion d'une liste de facteurs qui doivent être pris en considération avant qu'un décret soit pris, l'obligation que les décrets soient proportionnels à la gravité de la menace perçue, l'élargissement de la définition de « renseignements confidentiels » pour inclure les renseignements personnels et les renseignements anonymisés, et le rétablissement de la défense de diligence raisonnable pour les violations des décrets.

However, we have some remaining concerns. First, the proposed changes to the Telecommunications Act provide that:

> No one is entitled to any compensation from Her Majesty in right of Canada for any financial losses resulting from the making of an order . . . .

Cependant, nous avons encore des préoccupations. Premièrement, les modifications proposées à la Loi sur les télécommunications prévoient que :

> Nul ne peut obtenir d'indemnité contre Sa Majesté du chef du Canada pour les pertes financières subies par suite de la prise du décret.

We already know from real-life examples around the world that removing and replacing telecommunications equipment can be extremely expensive, hinder the expansion of telecommunications services to underserved communities, and in the case of smaller network operators, even threaten their ability to continue operations. Precluding compensation in all cases is unnecessary and unwise.

Nous savons déjà, à la lumière d'exemples concrets dans le monde entier, que l'enlèvement et le remplacement d'équipement de télécommunications peuvent être extrêmement coûteux, nuire à l'expansion des services de télécommunications dans les collectivités mal desservies et, dans le cas des petits exploitants de réseaux, menacer leur capacité même de poursuivre leurs activités. Il est inutile et malavisé d'exclure le versement d'une indemnité dans tous les cas.

We propose a simple fix. These subsections should be replaced with the following:

> An order may provide for compensation for financial losses and other costs if, in the circumstances, the minister [or Governor-in-Counsel, as applicable] considers it reasonable to so provide.

Nous proposons une solution simple. Ces paragraphes devraient être remplacés par ce qui suit :

> Tout décret peut prévoir une indemnité pour les pertes financières et autres coûts si, dans les circonstances, le ministre [ou le gouverneur en conseil, selon le cas] estime que cela est raisonnable.

Second, although the bill provides that orders are subject to judicial review, the legislation provides that a judge can base his or her decision on evidence that the appellant is not allowed to see, and therefore, cannot challenge. This process robs appellants of procedural fairness and makes no effort to provide for alternative means of testing the government's evidence, such as the appointment of a special advocate with the appropriate level of security clearance.

Deuxièmement, même si le projet de loi prévoit que les décrets peuvent faire l'objet d'un contrôle judiciaire, un juge peut fonder sa décision sur des éléments de preuve que l'appelant n'est pas autorisé à voir et, par conséquent, ne peut pas contester. Ce processus prive les appelants de l'équité procédurale et ne fournit pas d'autres moyens de vérifier la preuve du gouvernement, comme la nomination d'un avocat spécial ayant le niveau approprié d'habilitation de sécurité.

Third, while the House standing committee has put forward an amendment requiring the minister to report on an annual basis the number of times that an order supersedes a decision by the Canadian Radio-television and Telecommunications Commission, or CRTC, there remains no obligation for the commission to promptly notify the public as to which of its decisions have been amended or rendered unenforceable by an order. Overturning CRTC decisions without notice can erode public trust in regulatory bodies and create market uncertainty in regulatory decisions. They can be overturned without notice or explanation.

Troisièmement, bien que le comité permanent de la Chambre ait proposé un amendement exigeant que le ministre fasse rapport chaque année du nombre de fois qu'un décret a préséance sur une décision du Conseil de la radiodiffusion et des télécommunications canadiennes, ou CRTC, ce dernier n'est toujours pas tenu d'aviser rapidement le public de la modification ou du caractère inexécutable de ses décisions en raison d'un décret. L'annulation sans préavis des décisions du CRTC peut miner la confiance du public à l'égard des organismes de réglementation et créer une incertitude sur le marché concernant les décisions réglementaires. Ces dernières peuvent être renversées sans préavis ni explication.

Thank you for the opportunity to express our views on these important issues. I'm happy to answer any questions you have.

The Chair: Thank you very much, Mr. Smith. We will now proceed to questions. As usual, four minutes for each question, including the answer. Please keep your questions as short as possible.

We begin the questions with our deputy chair, Senator Dagenais.

[*Translation*]

Senator Dagenais: My first question is for Mr. Smith. Mr. Smith, Bill C-26 comes as no surprise. Have people in your industry been able to be proactive in developing their facilities in anticipation of the restrictions that could come along with such a bill? Have contracts with suppliers had to be cancelled? Given that these things must be negotiated, are new technologies from abroad being verified?

[*English*]

Mr. Smith: Thank you for the question. Yes. Even without Bill C-26, our industry has been very proactive in implementing security protocols, working, as I said, through CSTAC, the public-private sector committee, to look at best practices to protect telecommunications systems. That has been an ongoing activity.

With respect to particular vendors, we know that a couple of years ago, the government requested that telecommunications providers cease using equipment from certain foreign vendors, and industry participants voluntarily agreed to do so and have been taking action to implement those changes.

[*Translation*]

Senator Dagenais: Could the development of our telecommunications networks be jeopardized because certain equipment suppliers pose a security risk? If so, can you provide some examples?

[*English*]

Mr. Smith: Certainly, as we've heard from other witnesses, telecommunications and other critical systems are made up of many different components. That's no exception for telecommunications. There's a supply chain that supplies equipment to operators around the world.

Je vous remercie de nous donner l'occasion d'exprimer notre point de vue sur ces questions importantes. Je serai heureux de répondre à vos questions.

Le président : Merci beaucoup, monsieur Smith. Nous allons maintenant passer aux questions. Comme d'habitude, vous disposez de quatre minutes pour chaque question, y compris la réponse. Veuillez poser des questions aussi brèves que possible.

Nous allons commencer les questions avec notre vice-président, le sénateur Dagenais.

[*Français*]

Le sénateur Dagenais : Ma première question s'adresse à M. Smith. Monsieur Smith, le projet de loi C-26 n'est pas une surprise. Les membres de votre industrie ont-ils pu être proactifs dans le développement de leurs installations en prévision des restrictions qu'un tel projet de loi peut instaurer? Des contrats avec des fournisseurs ont-ils dû être annulés? Comme cela se passe-t-il sur le plan des négociations, les nouvelles technologies qui viennent de l'étranger sont-elles vérifiées?

[*Traduction*]

M. Smith : Je vous remercie de la question. Oui. Même sans le projet de loi C-26, notre industrie a été très proactive dans la mise en œuvre de protocoles de sécurité, en travaillant, comme je l'ai dit, par l'entremise du Comité consultatif canadien pour la sécurité des télécommunications, un comité réunissant les secteurs public et privé, pour examiner les pratiques exemplaires, afin de protéger les systèmes de télécommunications. C'est une activité continue.

En ce qui concerne certains fournisseurs, nous savons qu'il y a quelques années, le gouvernement a demandé aux fournisseurs de services de télécommunications de cesser d'utiliser l'équipement de certains fournisseurs étrangers, et les participants de l'industrie ont volontairement accepté de le faire et ont pris des mesures pour mettre en œuvre ces changements.

[*Français*]

Le sénateur Dagenais : Est-ce que le développement de nos réseaux de télécommunication peut être compromis, car certains équipementiers représenteraient des risques pour notre sécurité? Dans l'affirmative, pouvez-vous nous donner des exemples?

[*Traduction*]

M. Smith : Certainement. Comme d'autres témoins l'ont dit, les systèmes de télécommunications et d'autres systèmes essentiels sont composés de nombreux éléments différents. Les télécommunications ne font pas exception à ce chapitre. Il y a une chaîne d'approvisionnement qui fournit de l'équipement aux exploitants partout dans le monde.

Governments work together and the industry works together to take measures to ensure they are using reliable equipment that is both resilient and safe. If an issue does arise, that's really what this bill is targeted toward. The industry obviously does not knowingly implement security risks into their systems, but they work with government to identify potential risks and ameliorate those. This is really a backstop that would allow the government greater powers to make orders if they feel there's something that needed to be done that was not being done.

[*Translation*]

Senator Dagenais: Ms. Bahr-Gedalia, you mentioned your recommendations regarding compensation that could be paid to companies forced to comply with regulations enacted for security reasons. Do you have a rough estimate of what such compensation measures could cost the government?

[*English*]

Ms. Bahr-Gedalia: I don't have any specific amount or evaluation in mind, but in conversations with our telco members, of which we have all in our membership, it has become very clear that they have spent billions building their networks. Those networks come with enormous complexities, so they would be looking for some kind of compensation on a case-by-case basis. Mr. Smith had also mentioned the rationale of a reasonable judgment. Just modifying those networks could be incredibly costly and could also impact the services Canadians receive.

I want to comment that when a company may be required to make a change to the network, they should be able to make representations to the government to request that compensation if that change is required due to their previous investments.

We can't envision all scenarios where the government may use this legislation. Therefore, outright banning of compensation is felt by members to be slightly heavy-handed, so they appreciate some flexibility to be allowed within the act.

Senator Cardozo: I have a couple of questions. Ms. Bahr-Gedalia, I'll start with you. I tend to agree with Senator Batters's point that our role is that of sober second thought. This is a very important bill, and if we feel we should amend it, we should. On your point about ransomware, you have concerns about it in this bill, but if we don't make changes here, what other means would you see that issue being dealt with?

Les gouvernements travaillent ensemble et les entreprises font de même pour prendre des mesures, afin de s'assurer qu'elles utilisent un équipement fiable, à la fois résilient et sécuritaire. Ce que vise le projet de loi, ce sont les cas où un problème survient. De toute évidence, l'industrie n'intègre pas sciemment les risques pour la sécurité dans ses systèmes, mais elle travaille avec le gouvernement pour cerner les risques potentiels et les atténuer. Il s'agit en fait d'un filet de sécurité qui permettrait au gouvernement de prendre des décrets s'il estimait qu'il faut faire quelque chose qui n'a pas été fait.

[*Français*]

Le sénateur Dagenais : Madame Bahr-Gedalia, vous avez évoqué vos recommandations sur les compensations qui pourraient être versées aux entreprises qui seront obligées de se conformer à certaines règles édictées pour des raisons de sécurité. Avez-vous une évaluation sommaire de ce qu'une telle mesure de compensation pourrait coûter au gouvernement?

[*Traduction*]

Mme Bahr-Gedalia : Je n'ai pas de montant précis à l'esprit ni d'évaluation en tête, mais d'après les conversations que nous avons eues avec nos membres du secteur des télécommunications, il est devenu très clair qu'ils ont dépensé des milliards de dollars pour bâtir leurs réseaux. Ces réseaux présentent d'énormes complexités, alors ils demanderaient une indemnisation au cas par cas. M. Smith a également mentionné le motif de jugement raisonnable. Le simple fait de modifier ces réseaux pourrait être extrêmement coûteux et avoir une incidence sur les services que les Canadiens reçoivent.

Je tiens à dire que lorsqu'une entreprise est tenue d'apporter un changement à un réseau, elle devrait être en mesure de faire des représentations auprès du gouvernement pour demander une indemnisation si ce changement est nécessaire en raison de ses investissements antérieurs.

Nous ne pouvons pas imaginer tous les scénarios où le gouvernement pourrait appliquer cette loi. Par conséquent, l'interdiction pure et simple du versement d'une indemnisation est perçue par les membres comme étant un peu trop sévère, de sorte qu'ils aimeraient une certaine souplesse dans la loi.

Le sénateur Cardozo : J'ai quelques questions. Madame Bahr-Gedalia, je vais commencer par vous. J'ai tendance à être d'accord avec la sénatrice Batters lorsqu'elle dit que notre rôle consiste à procéder à un second examen objectif. C'est un projet de loi très important, et si nous estimons que nous devrions l'amender, nous devrions le faire. Pour ce qui est des rançongiciels, vous avez des préoccupations à ce sujet dans le cadre de ce projet de loi, mais si nous n'y apportons pas de changements, quels autres moyens envisageriez-vous pour régler ce problème?

I'll ask my second question now, if you don't mind. Mr. Traoré, you and your colleague Ms. Proctor talked about overreach, and a feeling that you want us to move away from punitive measures in this bill. If you want to limit abuse and the misuse of information, isn't it the norm to have punitive measures to guide behaviour in that direction?

I'll start with Ms. Bahr-Gedalia, please.

Ms. Bahr-Gedalia: In terms of ransomware and to address this issue any further, I mentioned the Cyber. Right. Now. Council a few times, which is a group of experts that would kindly offer to the Senate and to the government at large to provide solutions and insight on how this could probably be solved or addressed. Members of the council have also agreed, and one member in particular, if the Senate is interested, to appear, testify and have conversations with the Senate about these particular issues.

The Cyber. Right. Now. Council, which I established for the Canadian centre, is a hub of experts. We've been around for four years now and going into our fifth year. If you wish to look further for recommendations into this particular topic of ransomware, ransom payments and such issues, we would offer our expertise to meet with us at any given moment.

Senator Cardozo: When you have that forum you mentioned on ransomware, if you can send us a report once you have a report, that would be helpful.

Ms. Bahr-Gedalia: Which forum?

Senator Cardozo: Did you mention a forum?

Ms. Bahr-Gedalia: Yes, absolutely. The Canadian Chamber of Commerce will be holding a Hill Day on cybersecurity and ransomware on November 18. Absolutely.

Mr. Traoré: We have to look at the underlying assumption behind these punitive financial sanctions. The idea that a cyber incident is the result of gross negligence, which, thankfully, isn't always the case, or mostly the case. We are dealing with threats that are more elaborated, using technology that is very complex and very new against actors that are always on their back foot because you're preparing for something that you don't know is coming and in what form. Knowing that, more often than not, the victim of a cyber incident is a victim and was hit by something they never saw coming and knowing that we believe, as written, Bill C-26 doesn't identify these scenarios as possibilities and paints a picture that isn't always rooted, like the very serious nature of a cyber incident.

Je vais tout de suite poser ma deuxième question, si vous n'y voyez pas d'inconvénient. Monsieur Traoré, vous et votre collègue, Mme Proctor, avez parlé de trop grands pouvoirs et de votre impression que nous devrions nous éloigner des mesures punitives dans ce projet de loi. Si vous voulez limiter les abus et l'utilisation de l'information à mauvais escient, n'est-il pas normal d'avoir des mesures punitives pour guider les comportements dans cette direction?

Je vais commencer par Mme Bahr-Gedalia. Je vous en prie.

Mme Bahr-Gedalia : Pour ce qui est des rançongiciels et pour régler ce problème, j'ai mentionné le programme La Cybersécurité. Dès. Maintenant., à quelques reprises. Il s'agit d'un groupe d'experts qui aurait l'amabilité d'offrir au Sénat et au gouvernement en général des solutions et des idées sur la façon dont cela pourrait probablement être réglé. Si le Sénat est intéressé, les membres du conseil, et un membre en particulier, ont également accepté de comparaître, de témoigner et d'avoir des conversations avec vous sur ces questions particulières.

Le programme La Cybersécurité. Dès. Maintenant., que j'ai créé pour le centre canadien, est un carrefour d'experts. Nous existons depuis quatre ans maintenant et nous entreprenons notre cinquième année d'activité. Si vous souhaitez obtenir des recommandations sur les rançongiciels, les paiements de rançons et d'autres questions de ce genre, nous sommes prêts à vous rencontrer à tout moment.

Le sénateur Cardozo : Lorsque vous tiendrez ce forum au sujet des rançongiciels dont vous avez parlé, si vous pouvez nous envoyer un rapport, ce serait utile.

Mme Bahr-Gedalia : Quel forum?

Le sénateur Cardozo : Vous n'avez pas mentionné un forum?

Mme Bahr-Gedalia : Oui, absolument. La Chambre de commerce du Canada tiendra une Journée de la Colline sur la cybersécurité et les rançongiciels le 18 novembre. Vous avez raison.

M. Traoré : Nous devons examiner l'hypothèse sous-jacente à ces sanctions financières punitives. La perception selon laquelle un cyberincident est le résultat d'une négligence grave ne se confirme heureusement pas toujours, ni la plupart du temps. Nous faisons face à des menaces qui sont plus élaborées et qui utilisent une technologie très complexe et très nouvelle, et elles prennent souvent les responsables par surprise par ce qu'ils ne savent quand elles se produiront et quelle forme elles prendront. Il faut savoir que, la plupart du temps, la victime d'un cyberincident est une victime et qu'elle a été frappée par quelque chose qu'elle n'a jamais vu venir. Selon nous, tel qu'il est rédigé, le projet de loi C-26 ne considère pas ces scénarios comme des possibilités et brosse un tableau qui n'est pas toujours fondé,

Senator Cardozo: Would you think there is some level of due process in that people wouldn't get fined before there was due process? People could make the case that it wasn't their fault.

Ms. Proctor: Indeed and as they should. To your point of having a punitive nature to guide behaviour is exceedingly fair, and that is found in other international regulations. Where this deviates, however, is the individual. An individual who often does not have decision-making power nor had culpability that has been proven. Our suggestion is to define a standard, which, if they're not being demonstrated against it in an objective way or with a substantiated culpability, then they not face that.

When we look at other international organizations and standards such as General Data Protection Regulation, or GDPR, the California Consumer Privacy Act, or CCPA, or even SOCC, it's an organization. Only when there is intentional malice proven against an individual is there penalty against an individual. That would be our suggestion: to guide without penalizing an individual.

Senator M. Deacon: Thank you for being here today. I'm going to direct this question first to the Canadian Chamber of Commerce, but if we have time, others are certainly welcome to respond.

We've read that a large number of Canada's small- and medium-sized enterprises, or SMEs, struggle with cybersecurity. A 2021 KPMG report found that while 95% of the Canadian SMEs do surveillance for potential cyberattacks, only 56% test the effectiveness of these cyber defences.

My question is this: We know that not all SMEs would fall under the umbrella of this legislation, but their cybersecurity is still very important, especially when it comes to data breaches and personal information for their customers. From your perspective, and that of the people you represent, is there a hope of a trickle-down effect? Could this legislation be the tide that lifts all boats when it comes to cybersecurity in our private sector?

Ms. Bahr-Gedalia: Thanks for the question. SMEs are very important to the Canadian Chamber of Commerce, and the groups I mentioned are all comprised of many SMEs across different industries and sectors.

One of the goals of the Canadian Chamber of Commerce is to create greater public awareness and education around certification for SMEs. I'm bringing this down to a point. At a higher level, we have Bill C-26. We are waiting for the national cybersecurity strategy, which we hope will launch soon, in order

notamment en ce qui a trait à la nature très grave d'un cyberincident.

Le sénateur Cardozo : Au chapitre de l'application régulière de la loi, ne pensez-vous pas qu'il n'y aurait pas d'amende imposée avant que la preuve soit faite? Les gens pourraient faire valoir que ce n'est pas leur faute.

Mme Proctor : En effet, et ils seraient justifiés de le faire. Pour ce qui est du caractère punitif pour orienter les comportements, c'est extrêmement juste, et c'est ce que l'on retrouve dans d'autres règlements internationaux. Toutefois, c'est l'individu qui est visé; une personne qui, souvent, n'a pas de pouvoir décisionnel et dont la culpabilité n'a pas été prouvée. Nous suggérons de définir une norme qui, si elle n'est pas démontrée de façon objective ou par une culpabilité manifeste, ne sera pas appliquée.

Dans d'autres organisations et normes internationales comme la General Data Protection Regulation, ou GDPR, la California Consumer Privacy Act, ou CCPA, ou même la SOCC, qui est une organisation, ce n'est que lorsque la malice intentionnelle est démontrée concernant une personne que cette dernière est punie. C'est ce que nous suggérons : guider sans pénaliser une personne.

La sénatrice M. Deacon : Merci d'être ici aujourd'hui. Je vais d'abord adresser ma question à la Chambre de commerce du Canada, mais si nous avons le temps, les autres témoins pourront certainement y répondre.

Nous avons lu qu'un grand nombre de petites et moyennes entreprises, ou PME, du Canada sont aux prises avec des problèmes de cybersécurité. Selon un rapport de 2021 de KPMG, alors que 95 % des PME canadiennes surveillent les cyberattaques potentielles, seulement 56 % vérifient l'efficacité de ces cyberdéfenses.

Ma question est la suivante : on sait que ce ne sont pas toutes les PME qui seraient visées par cette loi, mais leur cybersécurité est quand même très importante, surtout en ce qui a trait aux atteintes à la protection des données et aux renseignements personnels de leurs clients. De votre point de vue et de celui des gens que vous représentez, y a-t-il un espoir d'effet de retombée? Ce projet de loi pourrait-il favoriser la cybersécurité dans l'ensemble du secteur privé?

Mme Bahr-Gedalia : Merci de la question. Les PME sont très importantes pour la Chambre de commerce du Canada, et les groupes que j'ai mentionnés sont tous composés de nombreuses PME de différents secteurs et industries.

L'un des objectifs de la Chambre de commerce du Canada est de sensibiliser davantage le public à la certification des PME. Je ramène cela à un élément. À un niveau plus élevé, nous avons le projet de loi C-26. Nous attendons la stratégie nationale en matière de cybersécurité, qui, nous l'espérons, sera lancée

to have the overarching strategy, which, I hope, will also include an outlook on SMEs. The Canadian Chamber of Commerce has been asking — and this is publicly known — for an SME cyberdefence fund to help SMEs protect themselves better.

How we have suggested to go about it is to reallocate funding from already-existing programs, which have been untapped or have been under-resourced in terms of funding available, and reallocate this funding toward that fund to help SMEs. The Canadian Chamber of Commerce has been advocating for this for at least the last two years, and we have had conversations with government on this level. We think this is one way to address it and help SMEs as well. This is a publicly known initiative that the Canadian Chamber of Commerce has been driving. We are not asking government for more money. We are asking the government to reallocate funding of programs that may have been underutilized.

Senator M. Deacon: Thank you. Would anyone else care to respond to my question?

Mr. Traoré: At IBM, we compile a Cost of a Data Breach Report every year, and the cost on average of a cyber breach instance is $6.32 million, which is a figure associated to companies. This is in Canada. It's a figure that's associated with big business here in Canada, but also to SMEs. Obviously, in the context of being victims of cyber incidents, that is a sizeable amount of money. If you factor in the cost of compliance and punitive sanctions being bestowed upon an actor who was a victim, that is a cost that is ballooning up. That is definitely something worth keeping in mind.

Different actors won't have the same capabilities in terms of making sure their systems are adequate and they can effortlessly comply with this framework.

Senator M. Deacon: Thank you.

Senator Boehm: Thank you, witnesses, for being here. My first question is for Ulrike Bahr-Gedalia. I heard you speak about compensation for SMEs, about funds that would be set up, contingency-type funds.

But there is another element there of technical assistance, and that is the ease with which some might be able to fill out their applications. We're talking bureaucracy here. For a small- and medium-sized company, that could be difficult and too involved. Are you contemplating technical assistance? If so — and I know you have international experience — have you looked at what other jurisdictions might have done to facilitate what small- and medium-sized enterprises could undertake?

bientôt, une stratégie globale qui, je l'espère, comprendra également une perspective sur les PME. La Chambre de commerce du Canada demande — et c'est connu du public — un fonds de cyberdéfense pour les PME, afin de les aider à mieux se protéger.

Nous avons proposé de réaffecter des fonds provenant de programmes déjà existants, qui n'ont pas été exploités ou qui ont été sous-financés, à ce fonds pour aider les PME. La Chambre de commerce du Canada défend cette cause depuis au moins deux ans, et nous avons eu des discussions avec le gouvernement à ce sujet. Nous pensons que c'est une façon de régler le problème et d'aider les PME également. Il s'agit d'une initiative publique que la Chambre de commerce du Canada a pilotée. Nous ne demandons pas plus d'argent au gouvernement. Nous demandons au gouvernement de réaffecter les fonds de programmes qui ont peut-être été sous-utilisés.

La sénatrice M. Deacon : Merci. Quelqu'un d'autre veut-il répondre à ma question?

M. Traoré : Chez IBM, nous produisons le Rapport sur le coût d'une violation de données chaque année, et nous avons déterminé que le coût moyen d'une telle violation est de 6,32 millions de dollars dans le cas des entreprises. Cela concerne le Canada. C'est un chiffre qui est associé aux grandes entreprises ici au Canada, mais aussi aux PME. Évidemment, dans le contexte des cyberincidents, il s'agit d'une somme considérable. Si l'on tient compte du coût de la conformité et des sanctions punitives imposées à un acteur qui a été victime, ce coût augmente encore plus. C'est certainement quelque chose qu'il faut garder à l'esprit.

Les différents acteurs n'auront pas les mêmes capacités pour s'assurer que leurs systèmes sont adéquats et qu'ils peuvent se conformer sans effort à ce cadre.

La sénatrice M. Deacon : Merci.

Le sénateur Boehm : Je remercie les témoins de leur présence. Ma première question s'adresse à Ulrike Bahr-Gedalia. Je vous ai entendu parler d'indemnisation pour les PME, de fonds qui seraient mis sur pied, de fonds de prévoyance.

Mais il y a un autre élément au chapitre de l'aide technique, et c'est la facilité avec laquelle certains peuvent remplir leurs demandes. Nous parlons ici de bureaucratie. Pour une petite et moyenne entreprise, cela pourrait être difficile et trop complexe. Envisagez-vous une aide technique? Dans l'affirmative — et je sais que vous avez de l'expérience à l'échelle internationale —, avez-vous examiné ce que d'autres pays ont pu faire pour faciliter la tâche des petites et moyennes entreprises?

Ms. Bahr-Gedalia: Thank you for the question. First, I am well aware of the complexity of a lot of programs government has put out there for SMEs to complete the application, sometimes only to find out at the end they might not be eligible.

We would set up the SME cyber defence fund. We would have to structure the format — it is still a work-in-progress — learning from exactly these programs that have been too complicated and cumbersome to complete.

We have looked at one example from the United States, and there happened to be an example from Malta as well. I know it is a small jurisdiction, but how they implemented a cyber fund for SMEs is something we could possibly look at in terms of access, ease of use and the application. I'm fully aware of that. We would not, at the Canadian chamber, add more burden to SMEs in terms of completing applications and applying for funds. Our goal is to make it easy. Providing assistance means getting it right from the beginning, so you don't need assistance to complete these applications.

Senator Boehm: Thank you very much. I have a question for Mr. Smith as well. In your testimony, you frequently referred to your concerns about operational flexibility in terms of dealing with and balancing the security mandates that are implicit or explicit in Bill C-26. If this bill is passed without major amendment, would you see that being addressed in the implementation phase?

Mr. Smith: In terms of balance, there have been good amendments proposed in different areas of the act in terms of the proportionality of orders, for example. Orders have to take into account the differences of the companies that are impacted by those, their size, the operations of that company and their ability. I think there are some good protections that are being proposed in there. We're on the right track in that respect.

Senator Boehm: Thank you.

Senator Batters: Thank you to all of you for being here today and helping us with this complex bill.

First of all, to the Canadian Chamber of Commerce, with these brand new requirements on such complex measures in Bill C-26, I know that small- and medium-sized businesses will be reaching out to you to express their concerns, as your members are concerned about their ability to comply with this bill once it comes into effect.

Mme Bahr-Gedalia : Je vous remercie de la question. Tout d'abord, je suis bien consciente de la complexité de beaucoup de programmes que le gouvernement a mis en place et pour lesquels les petites et moyennes entreprises, les PME, doivent remplir une demande, pour parfois découvrir à la fin qu'elles pourraient ne pas y être admissibles.

Nous mettrions sur pied le Fonds de cyberdéfense pour les PME. Il faudrait structurer le format — cela demeure un travail en cours — en tirant des leçons justement de ces programmes qui sont trop compliqués et trop fastidieux à réaliser.

Nous avons examiné un exemple des États-Unis, et il y en a eu un de Malte également. Je sais qu'il s'agit d'une petite administration, mais nous pourrions nous pencher sur la façon dont elle a mis en place un fonds de cybersécurité pour les PME en ce qui concerne l'accès, la facilité d'utilisation et le processus de demande. J'en suis pleinement consciente. À la Chambre de commerce du Canada, nous n'alourdirions pas le fardeau des PME pour ce qui est de remplir des demandes et de demander des fonds. Nous voulons faciliter les choses. Fournir de l'aide consiste à bien faire les choses dès le début, de sorte qu'il ne soit pas nécessaire de demander de l'aide pour remplir ces demandes.

Le sénateur Boehm : Merci beaucoup. J'ai aussi une question pour M. Smith. Dans votre témoignage, vous avez souvent fait allusion à vos préoccupations au sujet de la souplesse opérationnelle requise pour gérer et équilibrer les mandats de sécurité qui sont implicites ou explicites dans le projet de loi C-26. Si ce projet de loi est adopté sans amendement majeur, croyez-vous que cela pourrait se régler à l'étape de la mise en œuvre?

M. Smith : Pour ce qui est de l'équilibre, de bons amendements ont été proposés dans différentes parties de la loi en ce qui concerne la proportionnalité des décrets, par exemple. Les décrets doivent tenir compte des différences entre les personnes morales qu'ils touchent, de leur taille, de leurs activités et de leur capacité. Je pense qu'il y a de bonnes mesures de protection qui sont proposées. Nous sommes sur la bonne voie à cet égard.

Le sénateur Boehm : Merci.

La sénatrice Batters : Merci à vous tous de votre participation ici aujourd'hui et de nous aider à améliorer ce projet de loi complexe.

Tout d'abord, je m'adresse à la Chambre de commerce du Canada. Je sais que les petites et moyennes entreprises vont communiquer avec vous pour vous faire part de leurs préoccupations au sujet des nouvelles exigences relatives aux mesures si complexes contenues dans le projet de loi C-26, puisque vos membres s'inquiètent de leur capacité de se conformer à ce projet de loi lorsqu'il entrera en vigueur.

Maybe you could tell us what those major concerns are. Do you believe the government should assist with some dedicated funds to help smaller businesses meet cybersecurity standards?

Ms. Bahr-Gedalia: I'll start with your last question. I'm always in favour of helping SMEs, but I'm also aware of not asking for new money in order to implement any funds. Of course, it would be helpful if there were a navigator program or any help and assistance, as we've seen with other programs in the past around immigration processes and so forth. There are already models that could probably work.

Again, back to my earlier point, if we could reallocate funds, as the Canadian chamber wouldn't ask for new funding, that would be helpful to SMEs.

Anything that is a new bill and new legislation impacts small businesses in that new burdensome regulations might be coming their way. It is the nature of any new legislation and regulation, and I think small businesses do understand that. There is a community of support that the Canadian chamber provides where we would also be in a position to support small- and medium-sized businesses. To your point, they will come with us to ask questions and we will make ourselves available to help as we see fit.

Senator Batters: Thank you. One of the major things that I've noticed about this bill is the fact that it has no breakdown, as some of you have mentioned, as far as small- and medium-sized businesses have a certain level of potential maximum fine. It just says that for a corporation, the maximum penalty is $10 million or $15 million for subsequent violations. If there's no breakdown, then it deals with individuals to just say $25,000 or $50,000 for subsequent violations. Obviously, that will come with precedent, but there should be some kind of indication right away.

Ms. Proctor, from IBM, during your intervention in the House and also here today, you mentioned that certain parts of Bill C-26 go well beyond very well-established international cybersecurity standards, particularly in relation to regimes of our allies. Could you tell us more about the aspects of Bill C-26, which, in your view, go beyond those international standards? Which elements, in your opinion, risk imposing unnecessary constraints or complicating the practices of Canadian industry compared to international standards?

Ms. Proctor: Thank you very much. Wonderful question.

Vous pourriez peut-être nous dire quelles sont ces principales préoccupations. Croyez-vous que le gouvernement devrait fournir une aide financière pour aider les plus petites entreprises à respecter les normes en matière de cybersécurité?

Mme Bahr-Gedalia : Je vais commencer par répondre à votre dernière question. Je suis toujours en faveur d'aider les PME, mais je sais aussi qu'il ne faut pas demander d'argent neuf pour mettre en place des fonds. Bien sûr, il serait utile d'avoir un programme de navigation ou de l'aide, comme dans le cas de programmes antérieurs concernant les processus d'immigration et ainsi de suite. Il existe déjà des modèles qui pourraient probablement fonctionner.

Encore une fois, pour revenir à ce que je disais plus tôt, si nous pouvions réaffecter des fonds, puisque la Chambre de commerce du Canada ne demanderait pas d'argent neuf, cela aiderait les PME.

Tout nouveau projet de loi et toute nouvelle mesure législative a des répercussions sur les petites entreprises, en ce sens qu'une nouvelle réglementation fastidieuse pourrait alourdir leur fardeau. C'est dans la nature de toute nouvelle mesure législative et de tout nouveau règlement, et je pense que les petites entreprises le comprennent. La Chambre de commerce du Canada offre une communauté de soutien grâce à laquelle nous serions également en mesure d'appuyer les petites et moyennes entreprises. Pour répondre à votre question, les PME viendront avec nous afin de poser des questions et nous serons disponibles pour aider comme bon nous semble.

La sénatrice Batters : Merci. L'un des principaux points que j'ai remarqués au sujet de ce projet de loi, c'est qu'il n'y a pas de ventilation, comme certains d'entre vous l'ont mentionné, en ce qui concerne les petites et moyennes entreprises qui s'exposent à un certain niveau d'amende maximale potentielle. On précise simplement que pour une personne morale, la pénalité maximale est de 10 millions de dollars, ou 15 millions de dollars en cas de récidive. S'il n'y a pas de ventilation, cette pénalité pour une personne physique est de 25 000 $, ou de 50 000 $ en cas de récidive. De toute évidence, il y aura des précédents, mais on devrait tout de suite fournir une indication de quelque sorte.

Madame Proctor, d'IBM, pendant votre intervention à la Chambre et ici aujourd'hui, vous avez dit que certaines parties du projet de loi C-26 vont bien au-delà des normes internationales très bien établies en matière de cybersécurité, particulièrement par rapport aux régimes de nos alliés. Pourriez-vous nous parler davantage des aspects du projet de loi C-26 qui, selon vous, vont au-delà de ces normes internationales? Quels éléments, selon vous, risquent d'imposer des contraintes inutiles ou de compliquer les pratiques de l'industrie canadienne par rapport aux normes internationales?

Mme Proctor : Merci beaucoup. Excellente question.

Certainly, the international standards are broad. Starting with some of the overreach that you mentioned and asked about, the overreach relative to sharing of information but also allowing a government organization, specifically, having a minister have the ability to go on site, audit documents, dictate remedial actions are all further than many of our allies have gone. Balance that against the individual punitive natures goes just a little bit further as mentioned in our earlier conversation and earlier questioning. It's usually stuck more directly to the corporation and only when found to have malicious intent or individual culpability, knowing culpability, does it go toward an individual.

Les normes internationales sont certainement très générales. En commençant par certaines des contraintes dont vous venez de parler et au sujet desquelles vous me posez la question, la portée excessive touche la communication de renseignements, mais aussi le fait de permettre à un organisme gouvernemental, et plus précisément d'autoriser un ministre à se rendre sur place, à auditer des documents et à dicter les mesures de redressement à adopter sont toutes des mesures qui vont plus loin que celles de bon nombre de nos alliés. Le fait d'équilibrer ces mesures par la nature punitive de celles qui sont prises contre les personnes physiques va un peu plus loin, comme nous l'avons dit dans notre échange antérieur et en réponse aux questions précédentes. Habituellement, les mesures sont plus directement liées à la personne morale et ce n'est que lorsqu'on constate qu'il y a eu intention malveillante ou culpabilité individuelle, et que l'on sait qu'il y a culpabilité, qu'elles sont liées à une personne physique.

Senator Batters: Exactly. When you have these types of sanctions, such as potential jail time, and I know the government is saying if it doesn't go beyond negligence, there isn't jail time, but that's maybe cold comfort dealing with some of the things we're dealing with here as your colleague said earlier. We're not dealing with potentially gross negligence, and there doesn't seem to be a requirement for that. It could be simply not adhering to the standards, perhaps.

La sénatrice Batters : Exactement. Lorsqu'il y a ce genre de sanctions, comme des peines d'emprisonnement potentielles, et je sais que le gouvernement dit que si l'infraction ne dépasse pas la négligence, il n'y a pas de peine d'emprisonnement, mais c'est peut-être une bien piètre consolation pour ce qui est de certaines des mesures dont nous parlons ici, comme votre collègue l'a dit plus tôt. Nous ne traitons pas de négligence grave, et il ne semble pas y avoir d'exigence à cet égard. Il est peut-être simplement question d'un non-respect des normes.

Ms. Proctor: If I may, supplemental to that, cyber-threats — and I feel a little trite in saying this — are evolving every day. It's a sophisticated business wherein there is recruitment, job advancement and exceedingly lucrative terms. Our ability to thwart that at every pass isn't just because someone didn't do something right; it's that they did. I'm mindful to this bill of being guiding and informing, while also not having a chilling effect so that people don't want to work in this industry and help us protect our critical infrastructure.

Mme Proctor : Si vous me le permettez, j'aimerais ajouter que les cybermenaces — et il peut sembler un peu superflu de le préciser — évoluent chaque jour. C'est une activité de pointe où il y a du recrutement, de l'avancement et des conditions extrêmement lucratives. Si nous réussissons à contrecarrer les plans des auteurs à chaque étape, ce n'est pas parce que quelqu'un a échoué auparavant, bien au contraire. Je suis consciente du fait que ce projet de loi sert de guide et d'information, mais qu'il n'a pas non plus un effet paralysant qui dissuaderait les gens de travailler dans cette industrie et de nous aider à protéger notre infrastructure essentielle.

Senator Batters: Thank you very much.

La sénatrice Batters : Merci beaucoup.

Senator McNair: Thank you for the testimony you're giving today. I think all of you touched on the fact that the bill specifically says, "no compensation." No one is entitled to compensation. When officials were asked that last week, their response was that doesn't mean that the minister or government in special circumstances or appropriate circumstances can't give compensation. Maybe you could each comment in the order you presented. I assume that doesn't give you enough comfort from your perspective.

Le sénateur McNair : Je vous remercie de votre témoignage d'aujourd'hui. Je pense que vous avez tous parlé du fait que le projet de loi précise qu'« aucune indemnité » n'est accordée. Personne n'a droit à une indemnité. Lorsqu'on a posé la question aux fonctionnaires la semaine dernière, ils ont répondu que cela ne voulait pas dire que le ministre ou le gouvernement, dans des circonstances particulières ou lorsque cela est justifié, ne pourrait pas accorder d'indemnité. Peut-être pourriez-vous répondre chacun dans l'ordre où vous avez présenté votre déclaration. Je suppose que cela ne vous rassure pas assez, de votre point de vue.

Ms. Bahr-Gedalia: I speak, of course, on behalf of my members. It would be nice to see it in writing then. I would like to think as part of the bill, not as a verbal confirmation, but as

Mme Bahr-Gedalia : Je parle, bien sûr, au nom de mes membres. Ce serait bien que ces circonstances soient précisées par écrit. J'aimerais qu'elles fassent partie du projet de loi, et ne

written confirmation, and laid out so it can be referenced as needed.

Mr. Smith: We've heard that before and not just last week but in other discussions with government officials. I don't think there's any reason why we should set up a debate over what the word "entitled" means. We've seen some very good amendments proposed to this legislation. We proposed what I think would be a very simple one. We're not asking to say there is a right to compensation. It's just that it may be ordered, and as my colleague beside me said, there should be a mechanism that allows companies to make representations as to why they believe compensation is appropriate. I think it is an easy fix. I don't think this is backing government into the corner by making this change. It's just clearing up something that could cause unnecessary disputes in the future.

Senator McNair: This is for IBM. You already have a very effective and good cybersecurity program in place. From your perspective, if this bill passes, how will this practically affect how you deal with it on an everyday basis?

Ms. Proctor: The good news is it allows us to continue to work with our critical infrastructure, or CI, partners and our entire ecosystem. It will not substantively change, however. We do an awful lot of work internationally intentionally to align our clients from a regulatory-control perspective to make sure they are aware. If I lean this out a little further and say that as we all lean toward adopting generative AI and preparing for post-quantum cryptography, the topic of data governance is on all of our minds and in all our conversations.

That topic of data governance is predicated on knowing where your data is, who has access to it and the security controls around it, which this regulation would become part of. This regulation would be swirled into that ecosystem of how we maintain our organizations and ensure that data governance to ensure we can lean forward into those new advancements in a very positive manner, just as many of the advancements like the CCPA did just not too long ago.

Senator LaBoucane-Benson: This is for the Canadian Chamber of Commerce. Ms. Bahr-Gedalia, you called for clear definition of reportable incidents. Last week, the government officials told us these would be developed in regulation rather than law because the tech and the threat landscape changes so fast and so quickly. I think Ms. Proctor mentioned that as well. I imagine you're eager to be consulted on those regulations. Do you have any thoughts about what the definition should be?

pas devoir croire ces fonctionnaires sur parole. J'aimerais que cette disposition soit confirmée par écrit, et qu'on puisse s'y référer au besoin.

M. Smith : Nous avons déjà entendu cela, et pas seulement la semaine dernière, mais lors d'autres discussions avec des fonctionnaires. Je ne vois pas pourquoi nous devrions lancer un débat sur le sens de l'expression « ne peut obtenir ». De très bons amendements ont été proposés relativement à ce projet de loi. Nous en avons proposé un qui, à mon avis, serait très simple. Nous ne demandons pas de dire qu'il y a un droit à une indemnité. C'est simplement que cela peut être décrété et, comme ma collègue à mes côtés l'a dit, il devrait y avoir un mécanisme qui permette aux personnes morales de faire des représentations pour expliquer pourquoi elles estiment qu'il y a lieu qu'une indemnité soit accordée. Je pense que ce serait un amendement facile à mettre en œuvre. Je ne pense pas que ce changement ait pour effet d'acculer le gouvernement au pied du mur. Il s'agit simplement d'éclaircir un point qui pourrait causer des différends inutiles à l'avenir.

Le sénateur McNair : Ma prochaine question est pour IBM. Vous avez déjà un très bon programme de cybersécurité. De votre point de vue, si ce projet de loi est adopté, en quoi cela changera-t-il votre fonctionnement quotidien?

Mme Proctor : La bonne nouvelle, c'est qu'il nous permet de continuer à travailler avec nos partenaires des infrastructures essentielles et avec l'ensemble de notre écosystème. Il ne changera pas de façon substantielle notre fonctionnement au quotidien. Nous travaillons beaucoup à l'échelle internationale pour assurer l'harmonisation avec nos clients du point de vue du contrôle réglementaire afin de nous assurer qu'ils le connaissent. Si je vais un peu plus loin et si je dis que nous tendons tous vers l'adoption de l'IA générative et la préparation à la cryptographie post-quantique, le sujet de la gouvernance des données est dans notre esprit à tous et dans toutes nos discussions.

Ce sujet de la gouvernance des données consiste à savoir où se trouvent vos données, qui y a accès et quels contrôles de sécurité s'y rattachent, et ce règlement en ferait partie. Ce règlement s'immiscerait dans cet écosystème qui régit comment nous administrons nos organisations et comment nous assurons cette gouvernance des données de manière à profiter de ces nouvelles avancées de façon très positive, tout comme bon nombre d'avancées comme la California Consumer Privacy Act, la CCPA, l'ont fait il n'y a pas si longtemps.

La sénatrice LaBoucane-Benson : Ma question s'adresse à la Chambre de commerce du Canada. Madame Bahr-Gedalia, vous avez demandé une définition claire des incidents devant être signalés. La semaine dernière, les fonctionnaires nous ont dit que ces incidents seraient définis par voie réglementaire plutôt que par voie législative parce que la technologie et la menace évoluent si rapidement. Je pense que Mme Proctor en a parlé également. J'imagine que vous avez hâte d'être consultés au

Ms. Bahr-Gedalia: First, I entirely agree that it would be timely to leave it up to the regulations because of, as I mentioned at the end of my remarks, the urgency of passing this legislation with the discussions we had here today and considerations, of course, of leaving it up to regulation.

I was prepared for this question because if I ask for a definition, I should be prepared myself. We were looking at the Department of Homeland Security in the United States. I remember that the White House had commissioned a study. They haven't landed yet on a "cybersecurity incident" definition. I wanted to lean my definition on that outcome and product, again, to talk to our alliances, key trading partners and international harmonization. At this point in time, it hasn't been really approved, and it is actually a comment I made during my February 5 appearance as well. I brought this forward and there hasn't been any definition concurred, but I would strongly encourage that we look at those definitions to ensure Canada aligns with its international counterparts.

Senator LaBoucane-Benson: This question is for Mr. Smith, but I know that Ms. Proctor also weighed in on it. It is around the entitlement to compensation just to further clarify or talk about it. It doesn't say that the government can't choose to provide compensation. What it says is that the companies just don't have an inherent right to it. My brain says, "Well that means the companies can't sue for compensation because it clearly says they're not entitled to it." Nothing precludes the government from entering into a negotiation or a conversation if something really blows up and money has to be spent. It's something that the government should wade into. Nothing stops them from doing that. Mr. Smith, am I reading that wrong, or is that a reasonable way to read that clause?

Mr. Smith: It's a reasonable way to read it, but I think the fact there has been so much discussion around it means the language as it rests today it is uncertain and there is a difference of opinion. I think this is the time to add clarity to it.

Senator LaBoucane-Benson: Thank you.

Senator Yussuff: Thank you, witnesses, for being here. I think we would all agree that cybersecurity attacks are increasing on a daily basis. They are an incredible cost to companies and individuals because individuals don't have any control when their personal information has been compromised and used against them. Standards are going to be critical, and holding

sujet de ces règlements. Quelle devrait être cette définition selon vous?

Mme Bahr-Gedalia : Tout d'abord, je suis entièrement d'accord pour dire qu'il serait opportun de s'en remettre à la réglementation parce que, comme je l'ai dit à la fin de mon intervention, il est urgent d'adopter ce projet de loi, compte tenu de nos discussions ici aujourd'hui et du caractère opportun de suivre cette voie.

J'étais prête à répondre à cette question parce que si je demande une définition, je dois moi-même en avoir une à proposer. Nous avons examiné le département de la Sécurité intérieure des États-Unis. Je me souviens que la Maison-Blanche avait commandé une étude. Ils n'ont pas encore établi la définition d'un « incident de cybersécurité ». Je voulais fonder ma définition sur ce résultat et ce produit, encore une fois, pour me baser sur nos alliances, sur nos principaux partenaires commerciaux et pour assurer une harmonisation à l'échelle internationale. À l'heure actuelle, cette définition n'a pas vraiment été approuvée, et c'est ce que j'ai dit lors de ma comparution du 5 février. J'ai soulevé cette question et aucune définition n'a été adoptée, mais j'encourage fortement le Canada à examiner ces définitions pour veiller à ce que la sienne soit harmonisée avec celles de ses homologues internationaux.

La sénatrice LaBoucane-Benson : Ma question s'adresse à M. Smith, mais je sais que Mme Proctor y a aussi réfléchi. Elle concerne le droit à une indemnité, simplement à titre de précision. On ne dit pas que le gouvernement ne peut pas choisir d'accorder des indemnités, mais plutôt que les personnes morales n'ont tout simplement pas de droit intrinsèque à une telle indemnité. Ma raison me dit que cela signifie que les personnes morales ne peuvent pas intenter de poursuites pour obtenir une indemnité parce qu'il est clairement indiqué qu'elles n'y ont pas droit, mais rien n'empêche le gouvernement de s'engager dans une négociation ou une discussion s'il y a un incident vraiment grave et s'il faut dépenser de l'argent pour le régler. C'est une avenue que le gouvernement devrait envisager. Rien ne l'en empêche. Monsieur Smith, est-ce que je me trompe ou est-ce une interprétation raisonnable de cette disposition?

M. Smith : C'est une interprétation raisonnable, mais je pense que le fait qu'il y ait eu tellement de discussions à ce sujet signifie que le libellé actuel est imprécis et qu'il y a une divergence d'opinions. Je pense que le moment est venu d'apporter des précisions.

La sénatrice LaBoucane-Benson : Merci.

Le sénateur Yussuff : Je remercie les témoins de leur présence. Je pense que nous sommes tous d'accord pour dire que les attaques contre la cybersécurité augmentent chaque jour. Elles imposent d'énormes coûts aux personnes morales et aux personnes physiques, parce que ces dernières n'ont aucun contrôle lorsque leurs renseignements personnels ont été

those that are responsible for maintaining a standard is, going forward, fundamental.

Ms. Proctor, I think I heard you say that obviously you have some worry about individuals being held accountable. In the same vein, as we try to elevate whatever the standard might be, obviously, there are global standards that our companies are following, but we don't want to remain there because everybody is evaluating what somebody is doing and they're raising their standard.

What would you say is fair in the context of what we're dealing with? Because the reality is today you can't do anything without putting your information in a device, and somebody is going to get it. Given the degree of trust with which we're relying on companies to protect that information, how does the public become more politically aware, not only as to what's at stake for us as a country, but also to what's at stake in general for all of us when we put our faith in businesses, in government and in, of course, the practices they're going to tell us when something is truly compromised, so we're not going to spend the rest of our lives worrying that somebody has our information and when they're going to use it against us?

Ms. Proctor: I think that's a brilliant question, and it speaks a little bit to a level of breach fatigue we all have where there is almost a little bit of apathy to it because it's already been breached or people think my information is already out there or my credit card is already known. There is a level of apathy that I'm mindful about.

My colleague mentioned IBM's *Cost of a Data Breach Report 2024* certainly leans into a lot of the challenges we're seeing. What we encourage and what we're seeing benefit from, however, is recognizing the number of breaches, while increasing, are also shifting. We, as consumers, municipal governments, provincial governments, and federal governments are wiser. We are setting controls and regulations that are improving and benefiting ourselves.

The point that I really want to lean into that I would wholeheartedly agree with is that awareness. I think individuals who testified last week also leaned into this: that the awareness is key to this. Private-public partnership and the respect within it, I believe, are foundationally based on sharing of information and how we share that.

Earlier testimony was speaking of safe harbour. I would encourage us to go almost a little bit further than that, meaning that during breach response, we're learning from each other

compromis et utilisés contre eux. Des normes seront essentielles, et il sera fondamental, à l'avenir, d'assurer la vigilance de ceux qui sont responsables de les faire observer.

Madame Proctor, je crois vous avoir entendue dire que vous vous inquiétez évidemment du fait que des personnes physiques soient tenues responsables. Dans le même ordre d'idées, lorsque nous essayons d'élever la norme, quelle qu'elle soit, évidemment, il y a aussi des normes mondiales auxquelles nos personnes morales sont astreintes, mais nous ne voulons pas en rester là parce que tous nos homologues évaluent ce que font les autres et rehaussent leurs normes.

Selon vous, qu'est-ce qui est approprié dans le contexte actuel? La réalité aujourd'hui, c'est qu'on ne peut rien faire sans devoir divulguer nos renseignements personnels. Compte tenu de la confiance que nous accordons aux personnes morales pour qu'elles protègent ces renseignements, comment le public devient-il plus conscient sur le plan politique, non seulement de ce qui est en jeu pour nous comme pays, mais aussi en général pour nous tous lorsque nous faisons confiance aux personnes morales, au gouvernement et, bien sûr, aux pratiques qu'ils nous conseillent d'adopter lorsque nos renseignements sont effectivement compromis, pour que nous ne passions pas le reste de notre vie à nous inquiéter parce que quelqu'un détient nos renseignements, et à nous demander à quel moment il les utilisera contre nous?

Mme Proctor : Je pense que c'est une excellente question, qui en dit long sur le degré de lassitude que nous ressentons tous à l'égard des atteintes à la vie privée. Il y a même presque une certaine apathie, parce que des gens ont déjà été victimes d'une atteinte à la vie privée, ou parce qu'ils pensent que leurs renseignements ou leur carte de crédit sont déjà compromis. Il y a un certain degré d'apathie dont je suis consciente.

Mon collègue a parlé plus tôt du rapport d'IBM intitulé *Rapport 2024 sur le coût d'une violation de données*, qui porte sur bon nombre des difficultés auxquelles nous sommes confrontés. Ce que nous encourageons et ce dont nous voyons l'avantage, cependant, c'est de reconnaître que ces atteintes, si leur nombre augmente, se transforment également. Nous, c'est-à-dire les consommateurs, les administrations municipales, les gouvernements provinciaux et le gouvernement fédéral agissons plus intelligemment. Nous établissons des contrôles et des règlements qui s'améliorent et qui nous avantagent.

Je suis tout à fait d'accord avec ce que vous dites au sujet de la prise de conscience. Je pense que les personnes qui ont témoigné la semaine dernière ont également insisté sur le fait que la prise de conscience est essentielle. Je crois que le partenariat public-privé et le respect qui y est associé reposent sur le partage de renseignements et sur la façon dont il se pratique.

Un témoin précédent a parlé d'un refuge sûr. Je nous encouragerais à aller un peu plus loin, c'est-à-dire que lors de l'intervention en cas d'atteinte, nous apprenons les uns des autres

without punitive measures. The *Cost of a Data Breach Report 2024* had over 600 companies that were reporting breaches. One of the biggest findings was over 50% do not report because of fear of a punitive nature.

Senator Yussuff: But isn't that a problem? If I trust you with my information and you don't tell me or you don't tell the government, how do we have any confidence in the system that we operate in, because we don't have a choice? I can't go back to where I dial a telephone so somebody wouldn't hack my device.

The world is evolving at a much faster pace, and we need to keep up. The businesses that are utilizing whatever system, we don't get to tell them what system to use. Don't they have an obligation and a responsibility to recognize that they have a large degree of obligation to the people who are trusting them with their information?

Ms. Proctor: They do indeed, and the regulations go a long way to ensuring that their duty of care is aligned to a standard that is recognized as the right level of care. That goes back to malicious intent versus unknowing attempt versus a threat actor or being compromised by a savvy professional — all very different aspects. To your colleague's comments earlier, that would be ideal: Just shift the regulations and Bill C-26 to have further levels of definition, if not also remove the individual culpability where malice or mistreatment isn't intended.

Senator Yussuff: Individual culpability — in terms of drafting the regulations, you could put clarity to the regulation —

The Chair: We have to keep going.

Senator Richards: Thank you for being here. I asked this question of the last panel, and I wasn't clear about the answer, if I got one.

What I asked was this: Is there a way to integrate the concerns of your individual rights with the needed security aspect of this important bill unless the bill is quite seriously amended — and that this bill is vitally needed, but is this the actual bill that is needed, or do we need some kind of compromise for the people involved? I ask any of you to maybe answer that.

sans qu'il y ait de mesures punitives. Dans le *Rapport 2024 sur le coût d'une violation de données*, plus de 600 entreprises ont signalé des violations. L'une des constatations les plus étonnantes, c'est que plus de 50 % des entreprises ne signalent pas les incidents par crainte d'être punies.

Le sénateur Yussuff : Mais n'est-ce pas un problème? Si je vous fais assez confiance pour vous fournir mes renseignements et que vous ne me le dites pas ou que vous ne le dites pas au gouvernement quand ils sont compromis, comment pouvons-nous continuer de faire confiance à notre système? Est-ce parce que nous n'avons pas le choix? Je ne peux pas retourner à l'époque du téléphone à cadran pour que personne ne puisse pirater mon appareil.

Le monde évolue beaucoup plus rapidement qu'autrefois, et nous devons suivre le rythme. Nous ne pouvons dicter aux entreprises quel système utiliser, quel que soit celui qu'elles utilisent. Ne sont-elles pas tenues et responsables de reconnaître qu'elles ont un grand degré d'obligation envers les gens qui leur font confiance en leur fournissant leurs renseignements?

Mme Proctor : En effet, et les règlements contribuent dans une grande mesure à faire en sorte que leur devoir de diligence soit conforme à une norme qui est reconnue comme le bon niveau de service. Cela nous ramène à la question de l'intention malveillante par opposition à la tentative inconsciente par rapport à un auteur de menaces ou au fait que nos renseignements soient compromis par un professionnel avisé, et tous ces aspects sont très différents. Pour revenir à ce que disait votre collègue tout à l'heure, l'idéal serait de modifier le règlement et le projet de loi C-26 pour qu'il y ait davantage de niveaux de définitions, voire supprimer la culpabilité individuelle lorsque la malveillance ou la mauvaise gestion ne sont pas intentionnelles.

Le sénateur Yussuff : En ce qui concerne la culpabilité individuelle, pour ce qui est de la rédaction du règlement, celui-ci pourrait être clarifié...

Le président : Nous devons continuer.

Le sénateur Richards : Merci de votre présence. J'ai posé cette question au dernier groupe de témoins, mais je n'ai pas bien compris la réponse, si tant est qu'il y en ait eu une.

J'ai demandé s'il y avait moyen d'intégrer les préoccupations relatives aux droits individuels à l'aspect nécessaire de cet important projet de loi qui porte sur la sécurité, à moins que le projet de loi ne soit assez sérieusement amendé, et j'ai voulu savoir, attendu que ce projet de loi est absolument nécessaire, s'il s'agit vraiment du projet de loi dont nous avons besoin? Avons-nous plutôt besoin d'une sorte de compromis pour les personnes concernées? J'aimerais que l'un d'entre vous réponde à cette question.

Mr. Traoré: We understand the government's intent to ensure the regulations can clear up some of the definitions and carve outs that are necessary to really fulfill the mission of the legislation. As we said at the onset, we do share the essence of this bill; we were aligned with the government in the sense that we need to act, and act now. When we're looking at the cost of an average cyber threat that is majorly touching critical systems, there's a need to act now. We need to ensure that Canada's infrastructure is on par. This bill is trying to do just that.

We do believe, however, that the devil is in the details. A few definitions could be amended right now, before the regulations, to bring some certainty into the government's resolve.

Ms. Proctor: I would agree with my colleague, Mr. Traoré.

Senator Richards: My second question is this: Do you know how many cyberattacks Canadians face on a daily or weekly basis, or are there just too many to count? How would you answer that?

Ms. Proctor: I have a view to the number of cyber attacks that IBM is assisting our clients and partners on a daily basis, but I would not begin to make a statement of how many in Canada are being encountered.

Last year, the number of records breached — and a record would be an individual's credit card or an individual's personal identifiable information, or PII, data — there were over 24,000 breaches of records last year.

Senator Richards: Thank you.

The Chair: We have time for two more questions.

Senator M. Deacon: Back to the chamber again, a number of amendments we know were adopted in the House, and I'm trying to sort through all these specific concerns raised by witnesses in those hearings. The Chamber of Commerce — I knew there was concern expressed around duplication and onerous reporting standards of the term "reportable cyber security instance" was not better defined. For its part, the Business Council of Canada was also concerned about the lack of a risk-based methodology — the blanket reporting standards that would catch up low-risk operations when looked at through the lens of national security.

M. Traoré : Nous comprenons l'intention du gouvernement de veiller à ce que les règlements puissent mettre au clair certaines des définitions et des exclusions qui sont nécessaires pour vraiment réaliser l'objectif visé au moyen de la mesure législative. Comme nous l'avons dit au début, nous souscrivons à l'essence de ce projet de loi; nous étions d'accord avec le gouvernement pour dire que nous devons agir, et agir maintenant. Compte tenu du coût d'une cybermenace moyenne qui touche principalement les systèmes essentiels, il faut agir maintenant. Nous devons nous assurer que l'infrastructure du Canada est au bon niveau. C'est exactement ce que vise ce projet de loi.

Cependant, nous croyons que les détails feront foi de tout. Quelques définitions pourraient être modifiées dès maintenant, avant les règlements, pour donner plus de certitude à l'intention du gouvernement.

Mme Proctor : Je suis d'accord avec mon collègue, M. Traoré.

Le sénateur Richards : Ma deuxième question est la suivante : savez-vous combien de Canadiens sont victimes de cyberattaques chaque jour ou chaque semaine, ou y en a-t-il tout simplement trop pour les compter? Que pouvez-vous répondre à cela?

Mme Proctor : J'ai une idée du nombre de cyberattaques relativement auxquelles IBM aide quotidiennement ses clients et ses partenaires, mais je ne peux pas vous dire combien il y en a au Canada.

Il y a eu plus de 24 000 cas d'atteinte à la protection des renseignements personnels — on parle ici d'une carte de crédit ou de renseignements personnels identifiables — l'an dernier.

Le sénateur Richards : Merci.

Le président : Il nous reste du temps pour deux autres questions.

La sénatrice M. Deacon : Je reviens à la Chambre de commerce. Nous savons qu'un certain nombre d'amendements ont été adoptés à la Chambre des communes, et j'essaie de comprendre toutes les préoccupations précises soulevées par les témoins lors de ces audiences. Pour ce qui est de la Chambre de commerce, je savais que des préoccupations avaient été exprimées au sujet du dédoublement et du fait que les normes de déclaration onéreuses d'un incident de cybersécurité à signaler n'étaient pas mieux définies. Pour sa part, le Conseil canadien des affaires était également préoccupé par l'absence d'une méthodologie fondée sur le risque, à savoir les normes générales de signalement qui permettraient de rattraper les opérations à faible risque lorsqu'on les examine sous l'angle de la sécurité nationale.

Did the amendments that were made to address those concerns?

I'm just going to add something about high- and low-risk operations, but, first, with the concerns that were addressed — here is what we're concerned about — do you believe the amendments that were offered to the House addressed those concerns?

Ms. Bahr-Gedalia: The concern of the definition of a "cyber incident" is still outstanding. I think this is why I was earlier asked the question to which I would hopefully look forward to being able to answer one of these days in order to give you a definition — so that wasn't addressed, which is why I was referencing it again and pointing out that we were pleased that the changes were made that the Canadian Chamber of Commerce had been asking about, which was the one you just pointed out.

From that perspective, I would think our members would be looking for more clarification, but as noted earlier, that could probably also be addressed in the regulatory process in the regulations.

Senator M. Deacon: So how would you suggest we define "high-risk" and "low-risk" operations? What recourse would a business have if they disagreed with the designation they were given? Is there any thought that any of you have given to that?

It's at our table, which is fair. I think about that, because that is going to be a question. That's why I wondered if it was something that you had given any thought to.

Ms. Bahr-Gedalia: We could perhaps briefly say high and low risk reminds me of a conversation on another bill looking at those systems. These conversations have been happening at the Canadian chamber table, and with members but not pertaining to this bill. However, we have had discussions and are aware of the importance of the differences. We would have to look, probably, at more definitions pertaining to Bill C-26.

Senator M. Deacon: Thank you. Fair enough.

Senator Batters: Going back to the Chamber of Commerce on this, with respect to this reportable cybersecurity incident — that it remains undefined and the government is saying it will be defined in regulations — what are the potential consequences to an individual and to a corporation for offending that provision of Bill C-26? What could they be facing if their conduct, which is still undefined in the bill and potentially just left to regulations — what sorts of consequences could they potentially face under Bill C-26?

Les amendements qui ont été apportés répondent-ils à ces préoccupations?

J'aimerais simplement ajouter quelque chose au sujet des opérations à haut et à faible risque, mais tout d'abord, compte tenu des préoccupations qui ont été soulevées — et c'est ce qui nous préoccupe —, croyez-vous que les amendements qui ont été proposés à la Chambre ont répondu à ces préoccupations?

Mme Bahr-Gedalia : La question de la définition d'un cyberincident n'est toujours pas réglée. Je pense que c'est la raison pour laquelle on m'a posé la question plus tôt, et j'ai hâte de pouvoir y répondre un de ces jours afin de vous donner une définition. Donc, la question n'est toujours pas réglée, et c'est la raison pour laquelle j'en ai reparlé et c'est pourquoi j'ai souligné que nous étions heureux que les changements qui avaient été demandés par la Chambre de commerce du Canada, notamment celui que vous venez de souligner, ont été apportés.

De ce point de vue, je pense que nos membres aimeraient obtenir plus de précisions, mais comme on l'a vu plus tôt, cela pourrait probablement être réglé au cours du processus de réglementation, dans le règlement.

La sénatrice M. Deacon : Comment devrions-nous définir les opérations à haut risque et à faible risque? Quel recours une entreprise aurait-elle si elle n'était pas d'accord avec la désignation qui leur a été accordée? L'un d'entre vous y a-t-il réfléchi?

Cela relève de nous, à juste titre, et j'y ai réfléchi, parce que la question sera posée. C'est pourquoi je me demandais si vous y aviez réfléchi.

Mme Bahr-Gedalia : Nous pourrions peut-être dire brièvement que la question du risque élevé ou faible me rappelle une discussion sur un autre projet de loi portant sur ces systèmes. Il en a été question à la Chambre de commerce du Canada avec les membres, mais pas dans le contexte de ce projet de loi. Cependant, nous en avons discuté et nous sommes conscients de l'importance de la distinction. Il faudrait probablement envisager d'autres définitions dans le cas du projet de loi C-26.

La sénatrice M. Deacon : Merci. D'accord.

La sénatrice Batters : Pour revenir à la Chambre de commerce, en ce qui concerne cet incident de cybersécurité à signaler — qui n'est toujours pas défini et au sujet duquel le gouvernement dit qu'il sera défini dans le règlement —, quelles sont les conséquences possibles pour une personne physique et une personne morale qui contreviennent à cette disposition du projet de loi C-26? À quelles pénalités pourraient-elles s'exposer en raison de leur conduite, qui n'est toujours pas définie dans le projet de loi et qui pourrait être simplement assujettie à la réglementation, et quelles sortes de conséquences pourraient-elles subir en vertu du projet de loi C-26?

Ms. Bahr-Gedalia: I'll answer this question by saying I would have to look at our bills or regulations in place where such consequences have been implemented and if it is comparable. But what particular consequences for not reporting, what kinds of penalties or what kinds of consequences, I wouldn't be able to be lay them out, nor would I want to suggest any.

Mme Bahr-Gedalia : Je répondrai à cette question en disant qu'il faudrait que je regarde les projets de loi ou les règlements en place où de telles conséquences ont été mises en œuvre, et voir si une comparaison est possible. Je ne pourrais toutefois pas vous dire quelles seraient les conséquences particulières en l'absence d'un signalement, quels types de sanctions ou quels types de conséquences, et je ne voudrais pas non plus vous en suggérer.

Senator Batters: To IBM, are these the type of things that could potentially fall within the very punitive penalties that are provided in this bill, either potential jail or very huge fines?

La sénatrice Batters : Pour IBM, est-ce le genre de choses qui pourraient être visées par les sanctions très punitives prévues dans le projet de loi, soit une peine d'emprisonnement ou des amendes très lourdes?

Ms. Proctor: Yes, is the easy answer. The definitions from designated operator to the incident response or the incident itself and the response mechanism are all collectively part of the challenge of what that means for how we operate.

Mme Proctor : La réponse facile est oui. Les définitions de l'exploitant désigné, de l'intervention en cas d'incident ou de l'incident lui-même et du mécanisme d'intervention font toutes partie du défi que cela représente pour notre mode de fonctionnement.

To your earlier question of how are we operating this? This will guide. So the interest is not simply on certain terms; it is relative to how each one of those terms is going to impact the other. An organization's ability to change their organizations shift and implement the technology needed for it will not be immediate, so I daresay there would need to be a burn-in or normalization period to it as well to ensure alignment with them after the regulations have been further defined.

J'aimerais répondre à votre question précédente sur la façon dont nous nous adapterons à la situation, et cela vous guidera. Donc, notre intérêt ne se limite pas à certaines expressions; il dépend de l'incidence de chacune de ces expressions sur l'autre. Puisque la capacité d'une organisation de modifier son orientation et de mettre en œuvre la technologie nécessaire pour cela ne sera pas immédiatement disponible, j'oserais donc dire qu'il faudra prévoir une période de transition ou de normalisation pour assurer l'harmonisation avec la réglementation, une fois que celle-ci sera mieux définie.

The Chair: Thank you very much. This brings us to the end of our time with the panel. It's my privilege to thank Mr. Smith, Ms. Bahr-Gedalia, Ms. Proctor and Mr. Traoré for being with us this evening and for your very clear answers to a number of tough questions. You could tell from the interest around the room how much thought your presentations provoked. We're grateful for you being here and for helping us with this important legislation. Beyond that, you have jobs that I'm sure keep you awake at night and on some weekends. We thank you for that and for the very positive impact that this has on your clients and Canadians across the country. On behalf of the committee, thank you very much for doing that. It's very much appreciated.

Le président : Merci beaucoup. Cela nous amène à la fin de la séance. J'ai le privilège de remercier M. Smith, Mme Bahr-Gedalia, Mme Proctor et M. Traoré d'être venus ce soir et d'avoir répondu très clairement à un certain nombre de questions difficiles. Vous avez pu constater, d'après l'intérêt manifesté dans la salle, à quel point vos exposés ont suscité une réflexion. Nous vous sommes reconnaissants d'être venus ici et de nous avoir aidés dans notre étude de cet important projet de loi. De plus, vous avez des emplois qui, j'en suis persuadé, vous gardent éveillé la nuit et certains week-ends. Nous vous sommes donc doublement reconnaissants et nous vous remercions de l'incidence très positive de votre travail sur vos clients et sur les Canadiens partout au pays. Au nom du Comité, je vous remercie beaucoup. Nous vous sommes très reconnaissants.

For our final panel of the evening, I welcome, from the Canadian Internet Registration Authority, Byron Holland, President and Chief Executive Officer; and Matt Malone, Balsillie Scholar at the Balsillie School of International Affairs. I thank you both for joining us today.

Pour notre dernier groupe de la soirée, je souhaite la bienvenue à Byron Holland, président et chef de la direction de l'Autorité canadienne pour les enregistrements Internet, et à Matt Malone, chercheur-boursier Balsillie à la Balsillie School of International Affairs. Je vous remercie tous les deux de vous joindre à nous aujourd'hui.

I invite our panellists to now provide their opening remarks. You have five minutes each for this testimony, and we will begin

J'invite maintenant nos témoins à faire leur déclaration préliminaire. Vous avez cinq minutes chacun, et nous allons

with Mr. Byron Holland of the Canadian Internet Registration Authority. Whenever you're ready, please go ahead.

Byron Holland, President and Chief Executive Officer, Canadian Internet Registration Authority: Thank you very much. Mr. Chair, members of the committee, my name is Byron Holland, and I'm the President and Chief Executive Officer of the Canadian Internet Registration Authority, or CIRA. Thank you for the invitation to share our views and recommendations on Bill C-26.

The Canadian Internet Registration Authority is the not-for-profit organization best known for operating the .ca domain registry. In simple terms, this means that CIRA manages all 3.4 million .ca domain names, ensuring all websites and emails ending in .ca connect to the global internet and vice versa.

We maintain a global network that ensures the .ca domain is quickly available no matter where you are in the world, and we have a broader mission to promote a trusted internet, which we work toward by providing high-quality registry, domain name system and cybersecurity services, and by investing in the internet community. The Canadian Internet Registration Authority participates in numerous fora to provide and promote the security and resilience of the internet.

We're long-time leaders in global internet governance, and this includes extensive engagement with the Internet Corporation for Assigned Names and Numbers, or ICANN, the global coordinator of the domain name system that ensures your web browser can reach websites like Canada.ca. We also contribute to the Internet Engineering Task Force, where the technical standards that underpin the internet are developed.

The Canadian Internet Registration Authority also provides cybersecurity services that keep over 8 million Canadians safe online, including CIRA Canadian Shield, our free cybersecurity service that protects Canadian households from online threats; DNS Firewall, our enterprise-level DNS protection used by over a thousand Canadian organizations, including many cybersystems; and Anycast DNS, our global infrastructure that increases the performance and resiliency of top-level domains like .ca and helps mitigate malicious activity, such as distributed denial of service attacks from foreign actors.

We collaborate with several institutions to keep these services up to date, including the Canadian Centre for Cyber Security, the Canadian Centre for Child Protection and the Internet Watch Foundation. CIRA strongly supports the government's objective

commencer par M. Byron Holland, de l'Autorité canadienne pour les enregistrements Internet. Quand vous serez prêt, c'est à vous.

Byron Holland, président et chef de la direction, Autorité canadienne pour les enregistrements Internet : Merci beaucoup. Monsieur le président, sénateurs et sénatrices, je m'appelle Byron Holland. Je suis président et chef de la direction de la CIRA ou, en français, l'Autorité canadienne pour les enregistrements Internet. Je vous remercie de nous avoir invités à vous faire part de notre point de vue et de nos recommandations sur le projet de loi C-26.

La CIRA est l'organisme sans but lucratif mieux connu pour exploiter le registre de domaines .ca. En termes simples, cela signifie qu'elle gère les 3,4 millions de noms de domaine .ca, en veillant à ce que tous les sites Web et courriels se terminant par .ca soient reliés à l'Internet global et vice versa.

Nous entretenons un réseau mondial garantissant que le domaine .ca soit rapidement accessible partout dans le monde, et, plus généralement, nous avons pour mission de promouvoir un Internet fiable. C'est ce à quoi nous travaillons en fournissant un registre de haute qualité, un système de noms de domaine et des services de cybersécurité et en investissant dans la communauté Internet. La CIRA participe à de nombreuses tribunes pour assurer et promouvoir la sûreté et la résilience d'Internet.

Nous sommes à l'avant-garde depuis longtemps en matière de gouvernance de l'Internet à l'échelle mondiale, et cela comprend une collaboration approfondie avec l'ICANN, l'Internet Corporation for Assigned Names and Numbers, coordonnateur mondial du système de noms de domaine qui veille à ce que votre navigateur Web puisse atteindre des sites comme Canada.ca. Nous contribuons également aux travaux du Groupe de travail sur l'ingénierie d'Internet, qui élabore les normes techniques d'Internet.

Nous offrons également des services de cybersécurité qui protègent plus de 8 millions de Canadiens en ligne, notamment sous la forme du Bouclier canadien de la CIRA, notre service gratuit de cybersécurité, qui protège les ménages canadiens contre les menaces en ligne, mais aussi du pare-feu DNS, qui protège les entreprises et qui est utilisé par plus d'un millier d'organisations canadiennes, dont de nombreux cybersystèmes, et, enfin, d'Anycast DNS, notre infrastructure mondiale, qui permet d'améliorer le rendement et la résilience de domaines de haut niveau comme .ca et contribue à atténuer les activités malveillantes, comme les attaques par déni de service distribué en provenance de l'étranger.

Pour garder ces services à jour, nous collaborons avec plusieurs entités, dont le Centre canadien pour la cybersécurité, le Centre canadien de protection de l'enfance et la Fondation Internet Watch. La CIRA appuie vigoureusement l'objectif du

to raise the baseline level of cybersecurity across critical infrastructure through Bill C-26.

As I mentioned earlier, CIRA has a mission to promote a trusted internet. To achieve this, Canadians will need to trust the cybersecurity framework meant to protect them. With this in mind, I'll now share our recommendations to strengthen Bill C-26 and promote trust in the legislation.

During the House's study of Bill C-26, CIRA, alongside other witnesses, advocated for enhanced transparency provisions, which we are pleased to see reflected in the current draft of the legislation.

Today, we offer two recommendations to Part 2 of the bill, or the Critical Cyber Systems Protection Act, to better balance the bill's cybersecurity objectives with well-established best practices in oversight and in information sharing.

First, to protect more effective oversight, the issuance of cybersecurity directions under Part 2 of the bill should be subject to section 3 of the Statutory Instruments Act. This would ensure the cybersecurity directions are examined by the Clerk of the Privy Council in consultation with the Deputy Minister of Justice.

Second, conditions on the use of information should be strengthened to increase confidence in the CCSPA's information-sharing provisions. Currently, the bill does not explicitly limit how government entities can use information collected under certain sections. The additional guardrails proposed in our written brief would help ensure that collected information can only be used for the purposes set out in section 5 of the bill and mitigate concerns that CSE could use data collection under section 15 to pursue aspects of its mandate other than cybersecurity and information assurance.

In conclusion, CIRA recognizes the need to protect sources and methods in matters of national security and public safety. However, confidentiality and expedience must be balanced with due process and oversight. Through added provisions, we believe the Senate can enhance Canadians' trust and confidence in this framework.

gouvernement d'augmenter le niveau de base de la cybersécurité dans l'ensemble des infrastructures essentielles au moyen du projet de loi C-26.

Comme je l'ai dit tout à l'heure, la CIRA a pour mission de promouvoir un Internet fiable. Il faut pour cela que les Canadiens puissent faire confiance au cadre de cybersécurité conçu pour les protéger. Permettez-moi maintenant de vous faire part des mesures que nous recommandons pour renforcer le projet de loi C-26 et pour promouvoir la confiance de la population dans la réglementation.

Au cours de l'étude du projet de loi C-26 à la Chambre, la CIRA, en parallèle avec d'autres témoins, a préconisé l'amélioration des dispositions relatives à la transparence, et nous sommes heureux de constater que cela figure dans la version actuelle du projet de loi.

Aujourd'hui, nous vous présentons deux recommandations concernant la partie 2 du projet de loi, à savoir la Loi sur la protection des cybersystèmes essentiels, pour mieux aligner les objectifs du projet de loi en matière de cybersécurité sur les pratiques exemplaires reconnues en matière de surveillance et d'échange d'information.

Premièrement, pour améliorer la surveillance, les directives de cybersécurité proposées en vertu de la partie 2 du projet de loi devraient être assujetties à l'article 3 de la Loi sur les textes réglementaires. Elles devraient donc être examinées par le greffier du Conseil privé en consultation avec le sous-ministre de la Justice.

Deuxièmement, les conditions relatives à l'utilisation de l'information devraient être renforcées afin d'accroître la confiance à l'égard des dispositions de la LPCE sur l'échange d'information. À l'heure actuelle, le projet de loi ne limite pas explicitement la façon dont des entités gouvernementales peuvent utiliser les renseignements recueillis en vertu de certains articles. Les garanties supplémentaires proposées dans notre mémoire contribueraient à garantir que les renseignements recueillis ne puissent être utilisés qu'aux fins énoncées à l'article 5 du projet de loi et atténueraient le risque que le CST puisse recueillir des données en vertu de l'article 15 pour donner suite à des volets de son mandat autres que la cybersécurité et l'assurance de l'information.

En conclusion, la CIRA est consciente de la nécessité de protéger les sources et les méthodes en matière de sécurité nationale et de sécurité publique. Mais la confidentialité et la rapidité doivent être conciliées avec l'application régulière de la loi et la surveillance. Grâce à des dispositions supplémentaires, le Sénat pourrait, selon nous, accroître la confiance des Canadiens à l'égard de ce cadre de réglementation.

Thank you for the invitation to share our views and recommendations on Bill C-26 and for the Senate's time and consideration. Thank you.

The Chair: Thank you very much. Mr. Malone, please take it away.

Matt Malone, Balsillie Scholar, Balsillie School of International Affairs, as an individual: Thank you. My name is Matt Malone. I'm currently a Balsillie scholar at the Balsillie School of International Affairs in Waterloo, and I'm also the founder of the Open By Default database, which is the largest public database of records released under the federal Access to Information Act. You can access that database right now at openbydefault.ca.

Before commencing, I just want to note that it's a real pleasure to present with many incredible folks, including Mr. Holland, whose organization has contributed generously to the organization that hosts the Open By Default database. It's quite the honour and privilege to present with subject-matter experts like him who show a real commitment to accountable and transparent government.

Turning to Bill C-26, I want to applaud the work of the committee for taking on the review. Thank you for the unexpected invitation. I stress that I'm just appearing in an individual capacity representing only my own views.

To summarize my views, while I see Bill C-26 as a well-intentioned bill that has necessary components, I personally view it as a measure that also entrenches government surveillance power, undermines Canadian privacy rights and further erodes our transparency frameworks. I believe there are better ways to achieve the bill's stated goals.

My thoughts can basically be distilled into the following statement: Secrecy is not security. As government officials push a narrative that this bill is vital to protecting Canadians online, I ask you to consider that we are still waiting — quite some time now — for meaningful privacy reform to protect Canadians' privacy rights online.

I also ask you to consider that if we had meaningful privacy legislation, this would be beneficial to our cybersecurity. Privacy legislation with teeth would help address all different kinds of situations, such as data breaches of companies, collecting fitness tracker data, data breaches of health care companies like LifeLabs or 23andMe by giving Canadians recourse to meaningful privacy rights.

Je vous remercie de nous avoir invités à vous faire part de notre point de vue et de nos recommandations sur le projet de loi C-26, ainsi que du temps et de l'attention que vous nous accordez. Merci.

Le président : Merci beaucoup. Monsieur Malone, c'est à vous.

Matt Malone, chercheur-boursier Balsillie, Balsillie School of International Affairs, à titre personnel : Merci. Je m'appelle Matt Malone. Je suis actuellement boursier à la Balsillie School of International Affairs de Waterloo, et je suis également le fondateur de la base de données Open By Default, qui est la plus grande base publique de documents publiés en vertu de la Loi sur l'accès à l'information du gouvernement fédéral. Vous pouvez accéder en tout temps à openbydefault.ca.

Permettez-moi, avant de commencer, de vous dire que c'est un réel plaisir de comparaître en compagnie de nombreuses personnes remarquables, dont M. Holland, dont l'entreprise a généreusement contribué à l'organisation qui héberge la base de données Open By Default. C'est tout un honneur et tout un privilège de comparaître avec des experts comme lui, qui font preuve d'un véritable engagement à l'égard d'un gouvernement responsable et transparent.

Concernant le projet de loi C-26, je tiens à féliciter le comité d'avoir entrepris cet examen. Merci de cette invitation inattendue. J'insiste sur le fait que je comparais à titre personnel et que je n'exprime que mes propres opinions.

Pour résumer mon point de vue, et bien que je considère le projet de loi C-26 comme un texte législatif bien intentionné comportant des éléments nécessaires, j'estime personnellement que c'est une mesure qui consacre également le pouvoir de surveillance du gouvernement, qui compromet le droit à la vie privée des Canadiens et qui érode davantage nos normes de transparence. Il existe, à mon avis, de meilleurs moyens d'atteindre les objectifs énoncés dans le projet de loi.

Mes réflexions se résument essentiellement à l'énoncé suivant : le secret n'est pas synonyme de sécurité. Les représentants du gouvernement veulent nous convaincre que ce projet de loi est essentiel pour protéger les Canadiens en ligne, mais je vous demande de tenir compte du fait que nous attendons encore — et depuis déjà un certain temps — une vraie réforme pour protéger le droit à la vie privée des Canadiens en ligne.

Je vous demande également de tenir compte du fait que, si nous avions une loi sur la protection des renseignements personnels efficace, elle contribuerait à notre cybersécurité. Une loi sur la protection des renseignements personnels qui aurait du mordant aiderait à régler toutes sortes de situations, comme les atteintes à la protection des données des entreprises, la collecte de données de suivi de la condition physique, les atteintes à la

This reform with privacy legislation would actually establish better incident protocols, enhanced data protection and do many of the things that this bill is seeking to do. This bill does many good things, but it also entrenches an approach to cybersecurity that significantly expands state control with secret order-making power that lacks adequate review.

Secrecy is not security. This bill endows very great powers to an agency, CSE, that is clearly struggling to get oversight right. For example, CSE will not answer basic questions about its respect of human rights, including whether it has used or is actively using spyware. As many have noted, CSE has refused to give documents to its oversight bodies like NSIRA.

I understand that the committee doesn't have The Citizen Lab's brief, but I direct you to paragraph 26 of Kate Robertson's excellent brief for a history of how CSE has not given documents to NSIRA when requested.

What happens when the CSE doesn't give documents to its oversight bodies, as it has failed to do in the past? We go through the Access to Information Act. The CSE has one of the slowest and worst response rates for access to information requests. It regularly fails to issue acknowledging letters, which is a procedural tactic to delay answering requests and to stymie reviews.

The government claims that we need this law to meet the challenges of the digital moment that we are in, but this is the same government — and CSE is a federal institution among many — that responds to access to information requests using CDs, USBs and paper mail, even when requesters ask for electronic records. This has happened to me many times.

There is also systematic document destruction happening on the front end and the back end. There was an article today in the *Toronto Star* concerning the Ford government. It has a direct analogy with things that are happening in the federal government. I'm happy to talk about that.

This brings me to, perhaps, the central issue in this legislation. While the bill before you is well intentioned and has some necessary components, it does not address shortcomings in the government's own posture when it comes to cybersecurity.

protection des données des entreprises de soins de santé comme LifeLabs ou 23andMe, en permettant aux Canadiens de faire valoir leur droit à la protection des renseignements personnels.

Cette réforme de la Loi sur la protection des renseignements personnels permettrait d'établir de meilleurs protocoles d'intervention, d'améliorer la protection des données et de faire beaucoup de ce que le projet de loi vise à faire. Il y a beaucoup de bonnes choses dans ce projet de loi, mais il consacre aussi une approche de la cybersécurité qui élargit considérablement le contrôle de l'État, dont le pouvoir de rendre des décrets secrets ne ferait pas l'objet d'un examen suffisant.

Le secret n'est pas synonyme de sécurité. Ce projet de loi confère de très grands pouvoirs à un organisme, le CST, qui a manifestement de la difficulté à assurer une surveillance suffisante. À titre d'exemple, il ne répondra pas aux questions fondamentales concernant son respect des droits de la personne, notamment s'il a utilisé ou utilise activement des logiciels espions. Comme beaucoup l'ont fait remarquer, il a refusé de fournir des documents à l'OSSNR, l'un de ses organismes de surveillance.

Je crois savoir que le comité n'a pas reçu le mémoire du Citizen Lab, mais je vous renvoie au paragraphe 26 de l'excellent mémoire de Kate Robertson, qui explique que le CST n'a pas fourni de documents à l'OSSNR lorsqu'on le lui a demandé.

Que se passe-t-il quand le CST ne remet pas de documents à ses organismes de surveillance, comme c'est déjà arrivé? On invoque la Loi sur l'accès à l'information. Le CST affiche l'un des plus lents et des pires taux de réponse aux demandes d'accès à l'information. Il omet régulièrement d'envoyer des accusés de réception, une tactique procédurale visant à retarder les réponses et à entraver les examens.

Selon le gouvernement, nous avons besoin de cette loi pour relever les défis du numérique, mais c'est le même gouvernement — et le CST est un organisme fédéral parmi beaucoup d'autres — qui répond aux demandes d'accès à l'information au moyen de CD, de clés USB et de courrier imprimé, même lorsque les demandeurs demandent des documents électroniques. Cela m'est arrivé très souvent.

Il y a aussi la destruction systématique des documents au début et à la fin du processus. Un article a été publié aujourd'hui dans le *Toronto Star* au sujet du gouvernement Ford. On y fait une analogie directe avec ce qui se passe au gouvernement fédéral. Je suis heureux d'en parler.

Voilà qui m'amène peut-être à la question centrale. Bien que le projet de loi dont vous êtes saisis soit bien intentionné et comporte des éléments nécessaires, il ne corrige pas les lacunes relatives à la position du gouvernement en matière de cybersécurité.

Last Monday, members of Public Safety, ISED and CSE came before you to emphasize that they need these powers over the private sector. However, two days later, CSE admitted that China had compromised and infiltrated at least 20 networks associated with the federal government. The government has not installed the CSE sensors on all of the federal government institutions, as NSICOP — again, one of the oversight bodies in this legislation — has recommended.

The same week, CIRA discovered that hackers had obtained confidential information, pocketing more than $6 million. These are disclosures of government cybersecurity shortcomings from just last week, but there are many more we could discuss.

Rather than lead by example, the government is pushing through a bill for the private sector with order-making power that not many people truly understand. This resembles the problem currently in the state of affairs in Canada where when folks experience a cyberincident, they don't necessarily know which body to report to in the first place. You could report to many different bodies in Canada.

While I believe that the best parts of the law are well intentioned, and the law is needed, I personally believe the worst parts will set terrible new norms for Canada, in particular, clause 15 of Part 1 and clauses 20 to 25 of Part 2. Thank you for your invitation today, and I'm happy to answer any questions.

The Chair: Thank you very much. We'll go to questions and answers, starting with Senator Dagenais.

[*Translation*]

Senator Dagenais: My first question is for Mr. Holland.

Mr. Holland, correct me if I'm wrong, but you're responsible for Internet domains ending in ".ca," as opposed to the more prominent and more international ".com." To what extent can cybercriminals from abroad obtain ".ca" domains from their place of operation or by using aliases living in Canada? Finally, how can those domains be used for criminal purposes?

[*English*]

Mr. Holland: Thank you for the question. If I could just take a moment, my colleague here Mr. Malone mentioned that CIRA had a $6 million breach. I think you meant CRA. CIRA has not had any breaches, no $6 million breaches — just for clarification.

Lundi dernier, des représentants de Sécurité publique Canada, d'ISDE et du CST sont venus vous dire qu'ils avaient besoin de ces pouvoirs sur le secteur privé. Pourtant, deux jours plus tard, le CST a admis que la Chine avait compromis et infiltré au moins 20 réseaux associés au gouvernement fédéral. Le gouvernement n'a pas installé les capteurs du CST dans toutes les organismes du gouvernement fédéral, comme l'avait recommandé le Comité des parlementaires sur la sécurité nationale et le renseignement — je rappelle que c'est l'un des organismes de surveillance prévus dans le projet de loi.

La même semaine, la CIRA a découvert que des pirates avaient obtenu des renseignements confidentiels et empoché plus de 6 millions de dollars. Ces lacunes du gouvernement en matière de cybersécurité ont été révélées la semaine dernière, mais il y en a beaucoup d'autres à discuter.

Plutôt que de prêcher par l'exemple, le gouvernement veut faire adopter à toute vapeur un projet de loi sur le secteur privé et se doter d'un pouvoir de rendre des décrets que peu de gens comprennent vraiment. On pense à la situation actuelle au Canada, où des victimes de cyberincident ne savent pas nécessairement à quel organisme s'adresser. On peut s'adresser à toutes sortes d'organismes.

Je reste convaincu que les meilleures parties du projet de loi sont bien intentionnées et que la loi est nécessaire, mais j'estime personnellement que d'autres parties, bien pires, permettront d'adopter de nouvelles normes terribles pour le Canada, notamment l'article 15 de la partie 1 et les articles 20 à 25 de la partie 2. Merci de votre invitation aujourd'hui. Je me ferai un plaisir de répondre à vos questions.

Le président : Merci beaucoup. Nous allons passer aux questions, en commençant par le sénateur Dagenais.

[*Français*]

Le sénateur Dagenais : Ma première question s'adresse à M. Holland.

Monsieur Holland, excusez mon ignorance; vous êtes le registraire des domaines Internet qui se terminent par « .ca », en comparaison avec le « .com », qui est plus connu et plus international. Dans quelle mesure des cybercriminels de l'étranger peuvent-ils se procurer des domaines « .ca » à partir de leur lieu d'opération ou en utilisant des prête-noms qui vivent au Canada? Enfin, quel usage criminel peuvent-ils principalement en faire?

[*Traduction*]

M. Holland : Je vous remercie de la question. Permettez que je prenne un instant pour corriger mon collègue ici présent, M. Malone, qui a dit que la CIRA avait été victime d'un incident ayant coûté 6 millions de dollars. Je pense qu'il voulait parler de l'ARC. Je tiens à préciser que la CIRA n'a pas été victime

Mr. Malone: Total misinformation.

Mr. Holland: To your question, thank you for the question. I think the good news story here is that CIRA runs what we in the industry call a very clean zone. The .ca top-level domain is among the top handful — when I say "top handful," I mean two or three, the number varies month to month, but second or third cleanest zone of all the top-level domains in the world, including .com, .org, .uk, .net and all the rest of them. Fortunately, we have very few cyberbreaches or cybersecurity incidents emanating from a .ca domain name. To be clear, that means in the low single digits of .ca domain names where cybersecurity incidents are emanating from, which puts us as one of the cleanest top-level domains in the world.

[*Translation*]

Senator Dagenais: Do you have any idea how many ".ca" domains are currently in the hands of groups, countries or individuals who are using them to commit cybercrime?

[*English*]

Mr. Holland: Thank you for the question. By policy, only Canadian entities or individuals are allowed to register a .ca domain name. Whether you're a permanent resident, citizen, corporation or institution, you must have a formal legal tie to Canada. By design, foreign nationals or foreign entities cannot get .ca domain names. From time to time, they try. We have both proactive audit and complaint-based mechanisms by which we try to unearth .ca domain names registered inappropriately by foreign actors and foreign nationals. It's a tiny percentage where that happens, and we root them out as fast as we can.

[*Translation*]

Senator Dagenais: When sensitive information is being shared, what are your real concerns about the use of the information you possess? What sort of safeguards need to be put in place to ensure better protection?

[*English*]

Mr. Holland: Certainly, from CIRA's perspective, as we look at Bill C-26, we've already made some recommendations to the House. Fortunately, one of them seems to have been taken up. We continue to make recommendations around oversight and the sharing of information as it pertains to CSE, and we certainly believe there are opportunities, as we've said in our submission,

d'atteinte à la sécurité et qu'elle n'a pas perdu 6 millions de dollars.

M. Malone : C'est de la désinformation intégrale.

M. Holland : Pour revenir à la question, je vous en remercie. Je pense que la bonne nouvelle, c'est que la CIRA gère ce que, dans notre secteur, on appelle une zone très sûre. Le domaine de haut niveau .ca figure parmi les meilleurs — quelques deux ou trois, dont le nombre varie d'un mois à l'autre, mais c'est la deuxième ou troisième zone la plus sûre de tous les domaines de haut niveau dans le monde, en comptant .com, .org, .uk, .net, etc. Heureusement, il y a très peu d'atteintes à la cybersécurité ou d'incidents de cybersécurité provenant d'un nom de domaine .ca. Autrement dit, les incidents de cybersécurité provenant de noms de domaine .ca sont dans les plus faibles des nombres à un chiffre, ce qui en fait l'un des domaines les plus sûrs au monde.

[*Français*]

Le sénateur Dagenais : Est-ce que vous avez une idée du nombre de domaines « .ca » qui sont actuellement entre les mains de groupes, de pays ou d'individus qui les utilisent à des fins de cybercriminalité?

[*Traduction*]

M. Holland : Je vous remercie de la question. En vertu de la réglementation, seules des entités canadiennes ou des particuliers canadiens sont autorisés à enregistrer un nom de domaine .ca. Que vous soyez un résident permanent, un citoyen, une société ou un organisme, vous devez avoir un lien juridique officiel avec le Canada. Par définition, les ressortissants étrangers ou les entités étrangères ne peuvent pas obtenir de nom de domaine .ca. Ils s'y essaient de temps à autre. Des mécanismes de vérification proactive et des mécanismes fondés sur les plaintes nous permettent de découvrir des noms de domaine .ca enregistrés frauduleusement par des entités et des ressortissants étrangers. Ils sont très peu nombreux et sont éliminés le plus rapidement possible.

[*Français*]

Le sénateur Dagenais : Dans l'échange d'informations sensibles, quelles sont vos craintes réelles au sujet de l'utilisation des informations que vous possédez? Où sont les balises à mettre en place pour assurer une meilleure protection?

[*Traduction*]

M. Holland : La CIRA a déjà recommandé certaines mesures à la Chambre au sujet du projet de loi C-26. Heureusement, l'une d'elles semble avoir été adoptée. Nous continuons de formuler des recommandations au sujet de la surveillance et du partage d'information concernant le CST, et nous sommes effectivement convaincus qu'il y a moyen, comme nous l'avons indiqué dans

to tighten up the language and to put guardrails on how shared information is used and disseminated by CSE.

[*Translation*]

Senator Dagenais: Thank you very much.

[*English*]

Senator M. Deacon: Thank you to our witnesses for being here, and thank you for correcting misinformation.

A question for you, and thinking about this, Canada is the last G7 country to implement a robust regulatory framework for cybersecurity, something this legislation hopes to address.

I heard a little bit about the privacy legislation in some comments earlier. In your opinion, what took so long? What is taking so long? Is there something different or unique in Canada's institutions that make us a little bit slow on the uptake? Is there an opinion you would like to offer based on the line of work that you do? I'll ask you, Mr. Malone, first, and if you want to respond, Mr. Holland, that would be great.

Mr. Malone: Thank you for the question. I can opine a little bit. The Canada-United States-Mexico Agreement, or CUSMA, had some provisions on cybersecurity that favoured taking a risk-based approach as opposed to a prescriptive approach under the Trump administration, when such legislation was not in force. That didn't come in until Biden came along when you saw a bunch of prescriptive legislation start to come. Perhaps we were more wed to that provision in CUSMA; we were following that. That is possibly one answer.

The other is when you look at peer states when it comes to this type of legislation, cybersecurity for critical infrastructure, there has been a series of updates to the legislation. Australia introduced its legislation in 2018, but it already went through revisions, and now there is a second version.

The Europeans did the same thing in 2016 when they introduced their version of cybersecurity legislation for critical infrastructure, NIS 1, which is now replaced with NIS 2.

There is also some defence of the approach of "we need to get it right," and we shouldn't rush.

Mr. Holland: Thank you for the question. I share some of the sentiments in that often we tend to look at what our peers around the world are doing, and I think there was an opportunity here for Canadian legislators to look at what some of the earliest

notre mémoire, de renforcer le libellé et de prévoir des garanties concernant l'utilisation et la diffusion de l'information partagée par le CST.

[*Français*]

Le sénateur Dagenais : Merci beaucoup.

[*Traduction*]

La sénatrice M. Deacon : Merci aux témoins de leur présence ici aujourd'hui, et merci d'avoir corrigé l'erreur.

J'ai une question. À bien y penser, le Canada est le dernier pays du G7 à se doter d'un cadre de réglementation solide en matière de cybersécurité, et c'est ce que le projet de loi vise à corriger.

Certains témoins ont un peu parlé de la Loi sur la protection des renseignements personnels. Selon vous, qu'est-ce qui a pris autant de temps? Qu'est-ce qui prend autant de temps? Les organismes canadiens ont-ils quelque chose différent ou d'unique qui expliquerait cette lenteur? Avez-vous une opinion à formuler compte tenu de votre expérience professionnelle? Je vais m'adresser d'abord à vous, monsieur Malone, et j'aimerais aussi connaître l'avis de M. Holland, s'il veut bien répondre aussi.

M. Malone : Je vous remercie de la question. J'ai ma petite opinion. L'ACEUM, c'est-à-dire l'Accord Canada-États-Unis-Mexique, comportait des dispositions sur la cybersécurité privilégiant une approche axée sur le risque plutôt qu'une approche prescriptive sous l'administration Trump, quand ce genre de loi n'était pas en vigueur. Ce n'est qu'après l'arrivée de M. Biden qu'on a vu apparaître toute une série de lois prescriptives. Nous étions peut-être plus attachés à cette disposition de l'ACEUM et nous l'appliquions. C'est peut-être un élément de réponse à votre question.

D'autre part, quand on s'intéresse aux États comparables en matière de réglementation, les mesures de cybersécurité concernant les infrastructures essentielles ont fait l'objet d'une série de mises à jour. L'Australie a adopté sa loi en 2018, mais celle-ci a déjà fait l'objet de révisions, et il y a maintenant une deuxième version.

Les Européens ont fait la même chose en 2016 quand ils ont adopté leur réglementation de la cybersécurité pour les infrastructures essentielles, à savoir la directive NIS 1, maintenant remplacée par la directive NIS 2.

Certains défendent aussi l'idée qu'il « faut bien faire les choses » et qu'il ne faut pas se précipiter.

M. Holland : Je vous remercie de la question. Je partage certains des sentiments que nous avons souvent à l'égard de ce que font nos homologues partout dans le monde, et je crois que les législateurs canadiens ont eu l'occasion d'examiner certaines

legislation in the space was and learn from some of the challenges and mistakes, NIS 1 and NIS 2, for example.

I also think that we've had the benefit of being able to consider some of the supply chain challenges that impact cybersecurity in a way that some of our peer nations around the world didn't have the opportunity to do because they got out of the gate more quickly than we did. On the other hand, we've had an opportunity to think about some of the issues that weren't in the initial rounds of legislation.

Senator M. Deacon: Thank you. It is something with the chicken and egg, cause and effect.

Canada remains one of the most targeted countries by ransomware or cybercriminal groups. Is this the result of being cautious, thorough and taking your time, or is it that Canada might not be perceived as being as cyber wise as other comparable societies? That is the push-pull I'm thinking about. I'm not sure if there is anything else you would like to comment on.

Mr. Malone: I think one issue which has been highlighted by government officials who talked about the bill is the division of powers. There has been a big preoccupation with areas like health care, and government officials from the federal government emphasized we can't really regulate in this area. There is some concern about where the problem is and who has leverage to effect the solution.

I still think there is space for the federal government to set norms and to learn best practices from peer jurisdictions. I think that's important. I think this bill mirrors a lot of things we saw in NIS 1 in Europe that didn't work and have been since rendered obsolete and replaced by NIS 2, but the division of powers definitely plays a part in this as well.

Senator M. Deacon: Thank you.

Senator Batters: Thank you to both of you for being here personally and for your work on this.

Professor Malone, thanks very much for your testimony today. I'm also very concerned about the secretive court proceedings that will occur under Bill C-26. I referenced that in my Senate second reading speech where I quoted some of your work on this as critic for the bill. This is especially so because there are some very onerous penalties that exist under this bill.

One of the things I quoted from your work is where you were talking about the office of the intelligence commissioner and the work they do with respect to the communications security establishment. Could you tell us a bit more about what you see as

des premières lois dans ce domaine et de tirer des leçons de certaines difficultés et erreurs, comme les directives NIS 1 et NIS 2, par exemple.

Nous avons également eu l'avantage de pouvoir examiner certaines difficultés liées à la chaîne d'approvisionnement qui ont une incidence sur la cybersécurité, contrairement à certains de nos homologues dans le monde parce qu'ils ont agi plus rapidement que nous. Par ailleurs, nous avons eu la possibilité de réfléchir à certains enjeux qui n'étaient pas abordés dans les premières versions législatives.

La sénatrice M. Deacon : Merci. C'est une histoire d'œuf et de poule, de cause et d'effet.

Le Canada reste l'un des pays les plus ciblés par les rançongiciels ou les groupes de cybercriminels. Est-ce parce que vous avez été prudents, minutieux, et que vous avez pris votre temps, ou est-ce parce que le Canada n'est peut-être pas perçu comme étant aussi avisé en matière de cybersécurité que d'autres sociétés comparables? C'est ce que je me demande. Auriez-vous quelque chose à ajouter?

M. Malone : Des fonctionnaires ont soulevé la question de la division des pouvoirs au sujet du projet de loi. On se préoccupe beaucoup de domaines comme la santé, et les représentants du gouvernement fédéral ont insisté sur le fait qu'on ne peut pas vraiment réglementer ce domaine. On se demande où est le problème et qui a le pouvoir de trouver une solution.

Je pense quand même que le gouvernement fédéral peut fixer des normes des normes et s'inspirer des pratiques exemplaires de ses homologues. C'est important. Ce projet de loi contient beaucoup de dispositions semblables à celles de la direction européenne NIS 1 qui n'ont pas fonctionné et qui sont désormais obsolètes et remplacées par la directive NIS 2, mais le partage des pouvoirs est aussi un enjeu.

La sénatrice M. Deacon : Merci.

La sénatrice Batters : Je vous remercie tous les deux de votre présence et de votre travail dans ce dossier.

Monsieur Malone, merci beaucoup de votre témoignage d'aujourd'hui. Je suis également très préoccupée par les poursuites judiciaires secrètes qui seraient intentées en vertu du projet de loi C-26. J'en ai parlé dans mon discours à l'étape de la deuxième lecture, dans lequel, comme porte-parole pour le projet de loi, j'ai cité une partie de votre travail. C'est d'autant plus important que le projet de loi prévoit des sanctions très lourdes.

J'ai cité ce que vous avez dit au sujet du bureau du commissaire au renseignement et du travail qu'il fait concernant le Centre de la sécurité des télécommunications. Pourriez-vous nous préciser un peu les modifications qu'il serait crucial

some crucial amendments that could be made to Bill C-26 to improve those provisions of the bill?

Mr. Malone: Thank you. I think one of the real shortcomings with the bill is that there is no oversight on the front end, when it comes to the issuance of the orders we're talking about under clause 15 of Part 1 and clause 20 and onward in Part 2.

I should add that there were amendments that were made during the life of the bill in the House of Commons where in response to vocal concern from many folks, including open media, including The Citizen Lab, there were changes where notification requirements were put in to the National Security and Intelligence Review Agency, and the National Security and Intelligence Committee of Parliamentarians. But those were after the fact. What you have a problem with here is that there is no preapproval process that this is in fact an appropriate or considered measure. That markedly diverges from what the Communications Security Establishment Act passed in 2019 foresees as some of the mandates of Communications Security Establishment Canada. Many folks here have been emphasizing their concern about information collection under the act and the possibility of repurposing information that is collected.

One of the real concerns that the Communications Security Establishment Act addresses is that concern by specifically having the intelligence commissioner at the outset authorize, or not, certain types of actions, especially when it comes to breaking Canadian law where they might be collecting foreign intelligence or breaking Canadian law where they might be engaging in their cybersecurity assurance mandate. They have five mandates.

That is one of the issues: When you look at this law, you don't see an equivalent. You see an after-the-fact obligation to notify NSIRA or NSICOP that an order has been made. There are many problems with this approach. One, CSE has a demonstrated history — and I refer you to the Citizen Lab's incredible brief on this — of not providing information to NSIRA. That's a big issue. It might be a valid concern because NSIRA itself has been the subject of a major cybersecurity incident, which they didn't announce until 4 p.m. on a Friday, at one point. Those are real concerns that CSE might have. What you need to do is have some kind of preapproval, not just after the fact.

Of course, there is the issue of how those bodies are composed and the ability to muzzle the reports that those bodies might be producing, especially with NSICOP, which is not protected with parliamentarian privilege, so they are muzzled in terms of their work.

d'apporter, selon vous, au projet de loi C-26 pour améliorer ces dispositions?

M. Malone : Merci. À mon avis, l'une des grandes lacunes du projet de loi est le manque de surveillance au départ concernant les décrets dont nous parlons aux termes de l'article 15 de la partie 1 et des articles 20 et suivants de la partie 2.

Je dois ajouter que des amendements ont été apportés pendant l'étude du projet de loi à la Chambre des communes et que, en réponse aux préoccupations exprimées par beaucoup de gens, dont des médias ouverts comme le Citizen Lab, des exigences de notification ont été imposées à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement et au Comité des parlementaires sur la sécurité nationale et le renseignement. Mais c'était après coup. Votre problème aujourd'hui est qu'il n'y a pas de processus de préapprobation confirmant qu'il s'agit effectivement d'une mesure appropriée ou envisagée. Cela diffère considérablement de ce que la Loi sur le Centre de la sécurité des télécommunications adoptée en 2019 prévoit comme étant certains des mandats du Centre. Beaucoup de gens ici ont exprimé leur inquiétude au sujet de la collecte de renseignements en vertu de la loi et de la possibilité que ces renseignements soient utilisés à d'autres fins.

La Loi sur le Centre de la sécurité des télécommunications répond à l'une des préoccupations réelles que soulève le fait que le commissaire au renseignement autorise ou non au départ certains types de mesures, surtout quand il y a infraction au droit canadien dans le cadre de la collecte de renseignement étranger ou dans le cadre de son mandat d'assurance de la cybersécurité. Le Centre a cinq mandats.

C'est l'un des enjeux : on ne voit pas d'équivalent dans cette loi. On voit l'obligation a posteriori d'informer l'OSSNR ou le CPSNR qu'un décret a été rendu. Cette approche soulève beaucoup de problèmes. Premièrement, le CST a des antécédents — et je vous renvoie au mémoire incroyable du Citizen Lab à ce sujet — indiquant qu'il ne fournit pas d'information à l'OSSNR. C'est un gros problème. Il y a peut-être lieu de s'inquiéter quand on sait que l'OSSNR a fait l'objet d'un incident majeur de cybersécurité qui n'a pas été signalé avant 16 heures un vendredi. Ce sont des sujets d'inquiétude valables que pourrait avoir le CST. Ce qu'il faut, c'est obtenir une sorte d'approbation préalable, et pas seulement après coup.

Il y a, bien sûr, la question de la composition de ces organismes et de la capacité de museler les auteurs des rapports que ces organismes pourraient produire, surtout dans le cas du Comité des parlementaires sur la sécurité nationale et le renseignement, dont les membres ne sont pas protégés par le privilège parlementaire et qui sont donc muselés dans le cadre de leur travail.

Senator Batters: Exactly. That was where I was going to go with my second question. For both NSICOP and NSIRA, the members of those bodies are all appointed by the Prime Minister, and they report directly to the Prime Minister. As you noted now, and in your opening remarks, there have been significant occasions over recent years when the federal government has refused to comply with NSIRA and NSICOP directives. How would you suggest that Bill C-26 be amended to improve the concerning situation about oversight?

Mr. Malone: Where preapproval or pre-authorization is necessitated under the Communications Security Establishment Act, you can see that it is not always given. That might be the reason, in the drafting of this bill, it is not provided. CSE's annual report noted last year that, of the six times they had to go to the intelligence commissioner, they were only granted full approval half of those times. Some sort of preapproval from a truly independent body — I would consider Justice Noel truly independent — would be helpful.

The other problem the bill is going to have is that because it has been rendered obsolete by Bill C-70, in part, the judicial review provisions also introduce or inject these secured administrative review proceedings that have not been tested in law. As a law professor, I have a lot of concern about this provision because it doesn't provide a lawyer role for the person who's engaged in the judicial review. So they're just defending their interests; they are not actually serving with ethical, deontological obligations toward the client in those contexts.

If you look at Part 2 of the bill — specifically in the context of cybersecurity directives — it is not clear to me how a party will know that those directives have been issued and will be able to engage in the judicial review or proceedings. It makes more sense if your internet gets cut off under the order-making powers of Part 1, but under Part 2, if those directives have been made, it is not clear how a party will know they have been made. This starts to resemble a warrant list kind of FISA proceeding. This will create problems for Canada when it comes to how the EU, under its much more protective approach to privacy and its more robust data protection measures, views the Canadian legal regime when it comes to safeguarding personal information.

This could ultimately represent a bigger problem for us in terms of the Europeans deeming our data-protection regimes adequate in terms of protecting personal information. The moment Bill C-26 is passed, I'm going to go to a European privacy activist, tell them about this, point them to these proceedings and say, "Do you feel that this adequately protects your privacy?" Adequacy agreements made by the European Commission about the United States have consistently been

La sénatrice Batters : Exactement. C'était le sens de ma deuxième question. Les membres du CPSNR et du OSSNR sont tous nommés par le 4 ministre et en relèvent directement. Comme vous l'avez rappelé dans votre exposé préliminaire, il est arrivé à certains moments importants des dernières années que le gouvernement fédéral refuse de se conformer aux directives de l'OSSNR et du CPSNR. Comment pourrait-on, selon vous, modifier le projet de loi C-26 pour améliorer cette situation préoccupante en matière de surveillance?

M. Malone : On peut constater que les préapprobations et les préautorisations requises en vertu de la Loi sur le Centre de la sécurité des télécommunications ne sont pas toujours accordées. C'est peut-être la raison pour laquelle ce n'est pas prévu dans le texte de ce projet de loi. Dans son rapport annuel de l'an dernier, le CST a indiqué que, sur les six fois où il a dû s'adresser au commissaire au renseignement, il n'a obtenu d'approbation complète que la moitié du temps. Il serait utile d'obtenir l'approbation préalable d'un organisme vraiment indépendant, et je considère que le juge Noel est vraiment indépendant.

L'autre problème à venir est que, le projet de loi étant rendu en partie obsolète par le projet de loi C-70, les dispositions relatives au contrôle judiciaire introduisent ou injectent ces procédures de contrôle administratif sécurisées qui n'ont pas été testées en droit. Comme professeur de droit, je m'inquiète de cette disposition parce qu'elle ne prévoit pas un rôle d'avocat pour la personne participant au contrôle judiciaire. Chacun défend donc ses intérêts et ne remplit pas ses obligations éthiques et déontologiques envers le client dans ce cas.

Compte tenu des dispositions de la partie 2 du projet de loi — en particulier dans le contexte des directives en matière de cybersécurité —, je ne vois pas très bien comment une partie pourrait savoir que ces directives ont été adoptées et participer au contrôle judiciaire ou à la procédure. On comprend mieux si votre accès à Internet est interrompu en vertu des pouvoirs de rendre des décrets en vertu de la partie 1, mais, en vertu de la partie 2, si ces directives ont été adoptées, on ne voit pas bien comment une partie pourrait savoir qu'elles l'ont été. On dirait une sorte de liste de mandats à la FISA. Cela entraînera des problèmes pour le Canada compte tenu de la façon dont l'UE, qui a une perspective beaucoup plus protectrice de la vie privée et a adopté des mesures de protection des données plus robustes, perçoit le régime juridique canadien en matière de protection des renseignements personnels.

Au final, cela pourrait représenter un plus gros problème pour nous si les Européens estiment que nos systèmes de protection sont suffisants pour protéger des renseignements personnels. Dès que le projet de loi C-26 sera adopté, je vais m'adresser à un militant européen de la protection de la vie privée, lui en parler et porter son attention sur ces procédures en lui demandant : « Estimez-vous qu'elles protégeraient suffisamment votre vie privée? » Les ententes d'équivalence conclues par la

overturned on concerns that they don't adequately protect privacy and that they infringe all kinds of rule-of-law issues.

Senator Batters: Thank you so much.

Senator Dasko: My first question was going to be the same question as Senator Batters to Professor Malone about amendments. I read into what you've said. It sounds as if there aren't any amendments that would actually save this bill in terms of the issues that you've outlined. Would you start from scratch with a different bill? Would that be a better way to do it? It sounds like amendments wouldn't be helpful here. You outline other issues, such as the fact that we don't have privacy legislation. That puts this bill into a context in which it has a structural problem coming from elsewhere, and other issues that you outlined that seem to be part of this same context problem. Should we get rid of the bill and start from scratch with a different approach?

Mr. Malone: It's a great question. The bill contains many necessary components. It's laudable to require certain private-sector actors to have cybersecurity programs and to update those cybersecurity programs. There should be reporting obligations when certain breaches happen. Those could be expanded. We know that only 5% to 10% of cybercrimes are reported to a federal body. The Canadian Anti-Fraud Centre talks about that as a statistic. The CSE uses the same statistic. Anything that enhances reporting is good. It is salvageable by going toward lessons learned from the European Union. The NIS 2 is a good example, in my view, of how we might salvage it.

Senator Dasko: This one can be salvaged by looking at those opportunities.

Mr. Holland, I have a quick question. You've had such success with few cyberattacks on the .ca domains, and we had witnesses here earlier talking about best practices. Obviously, you must have something to share with the world about what you've done to be so successful. Would you share those with us?

Mr. Holland: Thank you for the question and the comment. We are definitely fortunate in that we have not suffered any kind of extreme or catastrophic cyberattacks. That doesn't happen by accident, of course. It is because of the programs, procedures, policies, technology that we have in place, and the focus of our organization is a trusted internet of which .ca is a key part of that.

Commission européenne à l'égard des États-Unis ont systématiquement été annulées parce qu'on craignait qu'elles ne protègent pas suffisamment la vie privée et qu'elles empiètent sur toutes sortes d'enjeux liés à la primauté du droit.

La sénatrice Batters : Merci beaucoup.

La sénatrice Dasko : Ma première question était la même que celle de la sénatrice Batters au professeur Malone au sujet des amendements. J'ai réfléchi à ce que vous avez dit. On dirait qu'aucun amendement ne pourrait sauver ce projet de loi du point de vue des enjeux que vous avez soulevés. Est-ce que vous reprendriez tout à zéro pour rédiger un projet de loi différent? Est-ce que ce serait une meilleure solution? On dirait que des amendements ne suffiraient pas. Vous soulevez d'autres questions, comme le fait que nous n'avons pas de loi sur la protection de la vie privée. Cela inscrit le projet de loi dans un contexte où il pose un problème structurel venant d'ailleurs, outre d'autres problèmes que vous avez soulignés et qui semblent faire partie du même contexte. Devrait-on se débarrasser du projet de loi et recommencer à zéro en adoptant une perspective différente?

M. Malone : Excellente question. Le projet de loi comporte de nombreux éléments nécessaires. Il est louable d'exiger que certains protagonistes du secteur privé aient des programmes de cybersécurité et les mettent à jour. On devrait prévoir des obligations de signalement dans certains cas d'atteinte à la sécurité. Ces dispositions pourraient être élargies. On sait que seulement 5 à 10 % des cybercrimes sont signalés à un organisme fédéral. Le Centre antifraude du Canada en parle comme d'une statistique. Le CST utilise la même statistique. Tout ce qui améliore les signalements est une bonne chose. Le projet de loi est récupérable si on s'inspire des leçons européennes. La directive NIS 2 est, à mon avis, un bon exemple de moyen de sauver le projet de loi.

La sénatrice Dasko : On peut le sauver en examinant ces possibilités.

J'ai une brève question pour vous, monsieur Holland. Vous avez eu beaucoup de succès dans votre entreprise et peu de cyberattaques contre les domaines .ca, et des témoins antérieurs nous ont parlé de pratiques exemplaires. Il est évident que vous devez avoir quelque chose à nous apprendre sur ce que vous avez fait pour réussir ainsi. Pourriez-vous nous en parler?

M. Holland : Je vous remercie de la question et du commentaire. Nous avons effectivement eu la chance de ne pas subir de cyberattaques extrêmes ou catastrophiques. Ce n'est pas un hasard, évidemment. C'est grâce à des programmes, des procédures, des politiques et une technologie, et l'objectif de notre organisation est un Internet fiable, dont le domaine .ca, est un élément déterminant.

We already do many of the things contemplated in Bill C-26 as best practices in terms of how we operationalize security at the network level, security by design, multi-layered security, which are things that the people who were here just before us know. They know those things. Then, there was the panellist from IBM. I'm sure that they're doing those things as well.

Those are lessons that we share. We share them in the Canadian context with our customers that we support. We share them in the international context in the industry that we're in so we can help top-level domain operators from other countries who don't necessarily have the benefit of all what we have to help lift them as well because cybersecurity, I'm sure you heard it here before, is a team sport, and we need to float all boats because inevitably it's the weakest link that suffers the attack, which then spreads out to the rest of us. So we have policies, programs, procedures and technology in place and are always monitoring. We run business continuity and disaster recovery on a regular basis, not just once in a while. Those are the things we do, and then, we share with others to bring them best practices. That has a tendency to lift all boats, which is actually in everybody's interest.

Senator Dasko: This is a playbook that's pretty well known. It is a set of rules that not everybody follows but that you follow?

Mr. Holland: Yes, I think that is a fair and accurate representation. There are always going to be zero-day attacks, things that have never been seen before. That is the unfortunate landscape that we operate in, but for the most part, most things are known. It is about remediation and diligence, and the playbook that you refer to is how you respond when you are attacked because it truly is not if, but when. Those playbooks will protect most organizations the vast majority of the times, with the exception of zero-day attacks that have never been seen before, which do happen, but they're not that common and they tend to be directed at only extremely high-value targets.

Senator Yussuff: I'll start with Mr. Malone. Spying is a pretty interesting field. I'm not involved in it, but the CSE's job is multi-layering responsibility for the nation's security. There are things that they do that I don't quite understand and maybe I don't want to understand, but I trust they are protecting the nation's interests. In terms of cyber breaches, both on the commercial and on the state side, this is happening at an alarming rate. There are a lot of things they share with other spy agencies around the world in terms of our friends.

Nous appliquons déjà beaucoup des mesures envisagées dans le projet de loi C-26 comme pratiques exemplaires dans l'opérationnalisation de la sécurité au niveau du réseau, de la sécurité dès la conception et de la sécurité à plusieurs volets, et ce sont des choses que savent les gens qui étaient ici, juste avant nous. Ils savent tout cela. Il y a eu ensuite le représentant d'IBM. Je suis sûr qu'IBM applique également ce genre de mesures.

Ce sont des leçons que nous partageons. Au Canada, nous les partageons avec les clients que nous soutenons. À l'étranger, nous les partageons avec les exploitants de domaines de haut niveau d'autres pays qui ne bénéficient pas nécessairement de tout ce que nous avons, parce que la cybersécurité, comme on vous l'a sûrement dit, est un sport d'équipe, et il faut garder tous les bateaux à flot parce que c'est inévitablement le maillon le plus faible qui subit l'attaque, et celle-ci se propage ensuite à tous les autres. Nous avons donc des politiques, des programmes, des procédures et une technologie, et nous surveillons toujours la situation de près. Nous assurons la continuité des activités et la reprise après sinistre de façon régulière, pas seulement de temps en temps. C'est ce que nous faisons et que nous partageons avec d'autres pour leur transmettre les pratiques exemplaires. C'est ainsi qu'on améliore la résistance de tous les bateaux, et c'est dans l'intérêt de tous.

La sénatrice Dasko : C'est un modèle assez connu. C'est un ensemble de règles que tout le monde ne suit pas nécessairement, mais que vous suivez, n'est-ce pas?

M. Holland : Oui, je dirais que c'est une représentation juste et exacte. Il y aura toujours des attaques du jour zéro, c'est-à-dire du jamais vu. C'est malheureusement le genre de contexte lequel nous évoluons, mais la plupart des éventualités sont connues. Il s'agit de prendre des mesures correctives et de faire preuve de diligence, et le modèle dont vous parlez est la façon de réagir en cas d'attaque, parce que la question n'est pas de savoir si, mais quand elle se produira. Ces modèles protégeront la plupart des organisations la plupart du temps, exception faite des attaques du jour zéro, du jamais vu, mais qui se produit effectivement. Cela dit, ces attaques ne sont pas très courantes et ne visent généralement que des cibles de très grande valeur.

Le sénateur Yussuff : Je vais commencer par M. Malone. L'espionnage est un domaine assez intéressant. Je n'y participe pas, mais le travail du CST comporte plusieurs niveaux de responsabilité pour la sécurité du pays. Il fait des choses que je ne comprends pas vraiment et que je ne veux peut-être pas comprendre, mais j'espère qu'il protège les intérêts de la nation. Les atteintes à la cybersécurité, du côté commercial comme du côté de l'État, se produisent à un rythme alarmant. Nous partageons beaucoup de choses avec d'autres agences d'espionnage dans le monde.

I understand some of the concerns you're raising, but I also think there is a fine line. How do we give them the authority or at least allow them the responsibility to do the things that are necessary to protect the nation's security while at the same time recognizing they should adhere to some standards that are fundamental to protect our fundamental rights under the Constitution?

That's a fine line. I always struggled with what the balance is because in the context of a crisis before us, I expect them to do the right thing and I'm not in their shoes, so I'm not there to assess what the right thing is, but I want to give them the latitude because they're protecting the nation's interests. Maybe you can elaborate a bit so I can understand you better.

Mr. Malone: That's a great question, and this is one of the needles we need to thread very carefully. You heard many recommendations from folks about repurposing information.

Mr. Holland opened by saying you should limit the ability to share information that's collected for the purpose of cybersecurity assurance, one of the mandates of CSE, but that's not what the bill is doing. The bill is compelling, under clause 15.4, the ability to collect any information. Once that information is collected, it can be repurposed to any of the five mandates that CSE has. That's very different from simply collecting information of a technical operation that you're going to deploy in a limited cybersecurity assurance context. It goes beyond that. It says they can mandate the collection of any information they need and they preserve the right to share that information with just about anyone they want.

I really do believe that European privacy activists will be very concerned when they learn about the scope of that type of data sharing, and it might spur some action toward Canada because I think it constitutes a significant overreach. There are ways to cabin that. Many folks have suggested — and I share these views — that you should limit the information-sharing purpose and repurposing once that information is collected.

The reality is that CSE is going to make mistakes. They're hyper competent, one of the most competent federal institutions we have. There's no question, but they have a mandate to not collect information about Canadians or people in Canada, and yet we know that that happens sometimes. They make mistakes. The CSE's annual report noted all kinds of privacy breaches, over 100 operational breaches involving privacy issues. I'll point out that those breaches are under CSE internal guidelines not the Privacy Act, and they won't release what the guidelines are. We don't have a window into how CSE is legally interpreting many of their obligations. There is incredible work done by Bill Robinson at the BC Civil Liberties Association, but we need to cabin this information collecting and information repurposing once it's collected. I think that would go very far in terms of addressing some of the issues there.

Je comprends certaines des préoccupations que vous soulevez, mais je pense aussi que la ligne est mince. Comment lui donner le pouvoir ou, à tout le moins, lui permettre de faire ce qui est nécessaire pour protéger la sécurité de la nation tout en reconnaissant qu'il doit respecter certaines normes fondamentales pour protéger nos droits fondamentaux en vertu de la Constitution?

La ligne est mince. L'équilibre est difficile à trouver, parce que, en cas de crise, je m'attends à ce que le Centre fasse ce qu'il faut, mais je ne suis pas à la place de ces gens et je ne suis pas là pour évaluer ce qu'il faut faire, mais je veux leur donner la latitude nécessaire pour qu'ils puissent protéger les intérêts de la nation. Peut-être pourriez-vous m'aider à comprendre.

M. Malone : C'est une excellente question et un enjeu très délicat. On vous a proposé de nombreuses recommandations au sujet de la réutilisation de l'information.

M. Holland a commencé en disant qu'il faudrait limiter la capacité de communiquer des renseignements recueillis aux fins de l'assurance de la cybersécurité, qui est l'un des mandats du CST, mais ce n'est pas ce que fait le projet de loi. Le projet de loi impose, en vertu de l'article 15.4, la capacité de recueillir des renseignements. Une fois ces renseignements recueillis, ils peuvent être réaffectés à l'un des cinq mandats du CST. C'est très différent de la simple collecte de renseignements pour une opération technique qu'on va déployer dans un contexte limité d'assurance de la cybersécurité. Cela va plus loin. On peut imposer la collecte de tous les renseignements jugés nécessaires et conserver le droit de communiquer ces renseignements à quiconque le Centre juge utile.

Je crois effectivement que les militants européens de la protection de la vie privée seront très inquiets d'apprendre la portée de ce type de partage de données, et cela pourrait déclencher des mesures à l'égard du Canada, car je crois que c'est excessif. Il y a des façons de limiter cela. Beaucoup de gens ont suggéré — et je suis d'accord avec eux — de limiter l'objectif de l'échange d'information et de sa réutilisation.

En réalité, le CST va commettre des erreurs. Il est extrêmement compétent, et c'est l'une des institutions fédérales les plus compétentes que nous ayons. Cela ne fait aucun doute, mais il a le mandat de ne pas recueillir de renseignements sur les Canadiens ou des gens au Canada, et pourtant, nous savons que cela arrive parfois. Il fait des erreurs. Son rapport annuel fait état de toutes sortes d'atteintes à la vie privée et de plus d'une centaine d'atteintes opérationnelles ayant trait à des renseignements personnels. Je tiens à souligner que ces atteintes relèvent des lignes directrices internes du Centre et non de la Loi sur la protection des renseignements personnels, et que ces lignes directrices ne sont pas divulguées. On ne sait pas comment le CST interprète légalement beaucoup de ses obligations. Bill Robinson fait un travail incroyable à l'Association des libertés civiles de la Colombie-Britannique, mais il faut limiter la

collecte de ces renseignements et leur réutilisation une fois qu'ils sont recueillis. Je pense que cela contribuerait grandement à régler certains problèmes.

Senator Yussuff: Is it possible, Mr. Malone, that we could limit that in the context that a regulation be more specific about — collecting is one thing but — what is then shared with CSE?

Le sénateur Yussuff : Monsieur Malone, serait-il possible de limiter cela dans le contexte où un règlement serait plus précis — la collecte est une chose, mais — reste à savoir ce qui est ensuite partagé avec le CST?

Mr. Malone: I would point you to clause 15 of part 1. Clause 15.4 says clearly any information can be collected, and I think it's 15.6 or onward that preserves the ability to share that information with just about anyone they want. There were assurances given to you last Monday in a committee that I saw talking about how this is just technical information, it's not personal information, but that's not what the law says. Kate Robertson, in one of the panels earlier, pointed out clearly that the language of the law, which is what is important, says any information can be collected, and I think we should take that at face value.

M. Malone : Je vous renvoie à l'article 15 de la partie 1. L'article 15.4 dit clairement qu'on peut recueillir n'importe quels renseignements jugés nécessaires, et je crois que ce sont l'article 15.6 ou les suivants qui préservent la possibilité de communiquer cette information à presque n'importe qui. Lundi dernier, dans le cadre d'une réunion du comité, on vous a donné l'assurance qu'il ne s'agissait, selon ce que j'avais entendu, que de renseignements techniques et non de renseignements personnels, mais ce n'est pas ce que dit la loi. Kate Robertson, dans le cadre d'auditions antérieures, a souligné clairement que le libellé de la loi, qui est ce qui importe, dit qu'on peut recueillir n'importe quels renseignements jugés nécessaires, et je pense qu'il faut le prendre au pied de la lettre.

Senator Boehm: This is a very interesting discussion. Thank you both for being here.

Le sénateur Boehm : C'est une discussion très intéressante. Merci à vous deux d'être avec nous.

I wanted to come at this from a little bit of a different angle. Mr. Holland, you said you have to float all boats. You were talking to people with similar responsibilities to your own in other jurisdictions. We always talk about the Five Eyes in this context, but it goes much broader than the Five Eyes as well. Dr. Malone, you have cited the European Commission a number of times and generally how that works.

Je voulais aborder la question sous un angle un peu différent. Monsieur Holland, vous avez dit que tous les bateaux devaient être à flot. Vous communiquez avec des gens ayant des responsabilités semblables aux vôtres dans d'autres pays. On parle toujours du Groupe des Cinq dans ce contexte, mais cela va beaucoup plus loin. Monsieur Malone, vous avez parlé de la Commission européenne à plusieurs reprises et de la façon dont cela fonctionne en général.

In my previous life before coming here, I often sat at negotiating tables, particularly with our G7 partners, and the discussion on cybersecurity has been going on for years. There is an exchange of views, and there is an exchange of best practices. Then, everyone agrees that the adversary is getting stronger and changing approaches, and the ball is moved down the field until we meet again as it were. There are committees of officials that feed into the ministerial meetings, and there is probably a need for some leadership.

Avant d'être sénateur, j'ai souvent participé à des négociations, en particulier avec nos partenaires du G7, et les discussions sur la cybersécurité durent depuis des années. Il y a échange de points de vue et échange de pratiques exemplaires. Ensuite, tout le monde s'entend pour dire que l'adversaire prend des forces et change d'approche, et la balle roule sur le terrain jusqu'à ce que nous nous rencontrions de nouveau. Des comités de fonctionnaires alimentent les discussions en réunions ministérielles, et on aurait probablement besoin de leadership.

Now, with this legislation, we're obviously playing a bit of catch up, but there are other countries who are doing things a little differently as well. Canada is taking over the presidency of the G7 in January. There will be ministerial meetings. They will feed into a big summit in Kananaskis in June.

Cela dit, avec ce projet de loi, il est évident qu'on a un peu de retard à rattraper, mais d'autres pays font les choses un peu différemment. Le Canada assumera la présidence du G7 en janvier. Il y aura des réunions ministérielles. Et cela se terminera par un grand sommet à Kananaskis en juin.

Do either of you see this as an opportunity throughout the process to reach summits and ministerial meetings for Canada to demonstrate some leadership, not just on best practices but in trying to look ahead and anticipate what the adversary actually can do? Do we have that capability?

L'un d'entre vous estime-t-il que ce serait l'occasion pour le Canada de faire preuve de leadership, depuis les réunions ministérielles jusqu'à la journée du sommet, non seulement en matière de pratiques exemplaires, mais aussi du point de vue de l'avenir et de l'anticipation de ce que l'adversaire peut réellement faire? Avons-nous cette capacité?

Mr. Holland: That's a very important question — thank you for the question — and important to get different perspectives on it. Certainly, from my perspective at the operator level working with organizations like the Canadian Centre for Cyber Security, we just heard about how CSE is seen in the world that they occupy.

We actually have excellent services in this space, not because I'm saying it, but because how they are regarded by their peers in the Five Eyes and G7, the Five Eyes in particular. So there is considerable expertise in this space that is referred to by other agencies of similar and high calibre, yet we are regarded as having some excellent services on that front.

In terms of G7 leadership, I'm a network operator in the cybersecurity space, so I'm not sure I can answer that for you, but we do have very good talent in this space. I take your point about the kinds of meetings you've been at. People gather, people talk, exchange views and then, "see you next time."

The field of play has changed. Certainly, the way Russia is behaving, the corner that they're in, two wars that each one has seen an incredible amount of cybersecurity activity that is pushing the bar to places we have never seen before. Is this time different? I would like to think — not I would like to think. I believe that the times we occupy are forcing the issue upon us in a way that has never been the case before.

Mr. Malone: I want to echo that. The CSE has incredible competence. The sensors that Mr. Curry was talking about during his appearance either here or in the House of Commons — I might be scrambling — are world famous. The U.K. has installed so many of them.

We're really seen as a leader. If you reviewed the CSE annual report last year, between the lines there's a little mention of CSE leading the takedown of a ransomware group and really doing the heavy lifting on that; they were the labouring ore. We have incredible capacity there.

I think the problem is we don't often use that in our own government, so we're not often demonstrating show, not tell. This bill is preoccupied with the private sector, but it ignores the public sector. CSE sensors are world famous such that the U.K. has over 100,000 of them deployed on their systems, but NSICOP recommended that all federal institutions in government should be using them, and they're not. There are still 50 that aren't. Parts of the Canadian government are sort of janky, but we're getting recognition from partners overseas.

M. Holland : C'est une question très importante — je vous en remercie —, et il est important d'obtenir différents points de vue à ce sujet. C'est un fait de mon point de vue d'exploitant travaillant avec des organisations comme le Centre canadien pour la cybersécurité, et nous venons d'entendre comment le CST est perçu dans son domaine.

En réalité, nous avons d'excellents services dans ce domaine, et ce n'est pas parce que je le dis, mais parce qu'ils sont considérés ainsi par leurs homologues du Groupe des cinq et du G7, surtout du Groupe des cinq. Il y a donc une expertise considérable reconnue par d'autres organismes semblables et, de haut niveau, et nous sommes considérés comme ayant d'excellents services à cet égard.

Quant au leadership du G7, je suis un simple exploitant de réseau dans le domaine de la cybersécurité et je ne suis pas sûr de pouvoir répondre à cette question, mais nous avons de très bonnes compétences dans ce domaine. Je comprends bien ce que vous dites au sujet des réunions auxquelles vous avez assisté. Les gens se réunissent, discutent, échangent des points de vue, et puis se disent « à la prochaine ».

Le contexte a changé. Entre le comportement de la Russie et deux guerres caractérisées par une quantité incroyable d'activités de cybersécurité, la barre se trouve à un niveau sans précédent. Est-ce que cette époque est différente? J'aimerais penser — non, en fait, ce n'est pas cela. Je suis convaincu que notre époque nous impose d'envisager cette question comme jamais auparavant.

M. Malone : Je vais faire écho à ces propos. Le CST a une compétence incroyable. Les capteurs dont parlait M. Curry, qui a témoigné ici ou à la Chambre des communes — je m'emmêle peut-être —, sont connus dans le monde entier. Le Royaume-Uni en a installé énormément.

Nous sommes vraiment considérés comme l'avant-garde. Si vous avez lu le rapport annuel du CST de l'an dernier, il y a, entre les lignes, une petite note indiquant que le CST dirige le démantèlement d'un groupe de rançongiciels et fait vraiment le gros du travail à cet égard, et c'est une énorme tâche. Nous avons là une capacité extraordinaire.

À mon avis, le problème est que nous ne l'utilisons pas souvent au sein de notre propre gouvernement, et ce n'est donc pas souvent visible. Ce projet de loi concerne le secteur privé, mais il ne tient pas compte du secteur public. Les capteurs du CST sont connus dans le monde entier, à tel point que le Royaume-Uni en a déployé plus de 100 000 sur ses systèmes, et le CPSNR a recommandé que toutes les institutions fédérales les utilisent, mais ce n'est pas le cas. Il y en a encore 50 qui n'en ont pas. C'est du bricolage dans certaines parties du gouvernement canadien, mais nos compétences sont reconnues par nos partenaires de l'étranger.

I think the real issue is our own conduct when it comes to the government and cleaning up our own posture when it comes to cybercrime. You can point to a lot of examples here. The fact that there's no single reporting place you go, imagine you're a small business and you suffer a cyber incident, where do you go? To the Privacy Commissioner, the RCMP or the CRTC? Are you going to go to a local police station if the RCMP is not available? It gets really complicated really quickly. The Auditor General has a report on this, and the flowchart is wild.

These are real issues, and you can compare them with approaches taken in Estonia, where they have a mission of one touchpoint with the government. As a citizen, you have one touchpoint with the government. There's a reason why, when NATO put up its Cooperative Cyber Defence Centre of Excellence, it did that in Estonia. But also, Estonia has had much earlier experiences with cyber incidents, including a shutdown of government in the early 2000s. We've been saved from that.

I think we're slowly waking up to these issues in Canada. I think we're starting to become really aware of the scourge of cybercrime, ransomware and cybersecurity incidents with our critical infrastructure.

Senator Boehm: Thank you very much.

The Chair: Colleagues, that bring us to the end of our questions for this panel.

To our last panel of the evening, I want to thank you, Mr. Malone and Mr. Holland, for a really impressive couple of presentations and for your very insightful and helpful responses to the large number of questions that you've heard this evening.

It's a great note to end on, to be reminded, Mr. Malone, of CSE's reputation globally. We hear about that all the time as we travel around and certainly hear it through NATO organizations. You've been very helpful to us on a very important piece of legislation, and we thank you very much, including for the important work that you both do every day.

On behalf of the Senate, this committee, thank you. Thank you to my colleagues for the questions that have brought the best out of panellists.

A few thoughts to share with you as I step down from this committee this evening as your chair, with the election of my successor to follow. First off, what a privilege this has been. It's been a highlight of my time in the Senate. I will be staying in the Senate, but it's not going to get any better than this. This has been an absolutely marvellous three years, definitely a highlight.

Le vrai problème est notre propre attitude à l'égard du gouvernement et notre propre position en matière de cybercriminalité. Il y a beaucoup d'exemples, dont le fait qu'il n'existe pas de centre de signalement. À qui une petite entreprise victime d'un cyberincident devrait-elle s'adresser? Au commissaire à la protection de la vie privée, à la GRC, au CRTC? Faut-il se rendre au poste de police local si la GRC n'est pas disponible? Tout devient très vite très compliqué. Le rapport du vérificateur général à ce sujet comprend un diagramme ahurissant.

Ce sont des problèmes réels, et on peut les comparer aux stratégies adoptées en Estonie, où on a décidé de créer un seul point de contact avec le gouvernement. Les citoyens ont un point de contact avec le gouvernement. Ce n'est pas pour rien que l'OTAN a décidé de créer son Centre d'excellence pour la cyberdéfense en coopération en Estonie. Il faut dire que l'Estonie avait connu beaucoup d'incidents cybernétiques auparavant, dont une paralysie totale du gouvernement au début des années 2000. Nous en avons été épargnés.

On prend lentement conscience de ces problèmes au Canada. On commence à vraiment prendre conscience du fléau que sont la cybercriminalité, les rançongiciels et les incidents de cybersécurité liés à nos infrastructures essentielles.

Le sénateur Boehm : Merci beaucoup.

Le président : Chers collègues, cela met fin à nos questions pour ce groupe de témoins.

En conclusion, je tiens à vous remercier, monsieur Malone et monsieur Holland, pour vos exposés vraiment impressionnants et vos réponses très pertinentes et utiles au grand nombre de questions que nous vous avons posées ce soir.

Monsieur Malone, voilà une excellente façon de terminer que de nous rappeler la réputation du CST à l'échelle mondiale. Nous en entendons constamment parler quand nous voyageons et notamment par l'entremise des organisations de l'OTAN. Merci de votre très utile contribution à ce projet de loi très important et merci du travail important que vous faites tous les deux chaque jour.

Je vous remercie au nom du Sénat et du comité. Merci à mes collègues des questions qui ont fait ressortir le meilleur de nos invités.

J'aurais quelques réflexions à partager avec vous au moment où je quitte la présidence ce soir et avant l'élection de mon successeur. Je tiens d'abord à dire que cela a été un grand privilège. Cela a été le point culminant de mes années au Sénat. Je resterai au Sénat, mais rien ne peut se mesurer à cette expérience. Les trois dernières années ont été absolument merveilleuses, et donc effectivement un point culminant pour moi.

None of us realized when I took on the chair that within weeks we would see the Russian invasion of Ukraine. It was a channel changer, to say the least, and I think it's fair to say that things globally have become more intense and more dangerous since then.

We saw Canada jump in with Operation UNIFIER before the invasion to start the training of combat troops. Our forces have been credited by Ursula von der Leyen and others for making a significant difference in the ability of Ukraine to withstand that initial invasion. That is a compliment, indeed, and we've seen that on our watch.

We've seen Canadian Forces lead a 10-nation battle group in Latvia, at Camp Adazi with a show of force on the border as part of a string of multi-country battle groups. We crossed the Arctic together. We travelled across the Arctic visiting Indigenous communities, meeting Canadian Rangers, meeting our Arctic defence forces, meeting with Indigenous representatives and peoples, and we were welcomed and learned so much from that experience.

We saw firsthand the world's only binational military command structure in operation at NORAD HQ in Colorado Springs. We saw the seamless crossover of leadership between the two co-commanders, Canadian and U.S., while those balloons were in the air, if you remember that. That was coincident with our trip there.

It was a privilege, indeed, to do that and, certainly, it was a privilege to do that with you.

We've tackled a slew of important legislative initiatives in this place, including high priority bills and, recently, legislation to combat foreign interference in Canada's democratic processes, which we need, I think, more than ever, and we've heard a lot more about that today. We worked together on firearms legislation. We are now in the midst of reviewing Bill C-26, which is designed to bolster Canadian organizations against cyber interference and cyber attacks, and we have witnessed over the last three years repeated and increasing efforts at foreign interference and cyber interference in our country, as well as an increasingly muscular, Russia, China and Iran, not only in a global context, but in terms of putting pressure on diaspora communities in this country and in our communities. That is a dramatic change in the landscape.

In all of this, in all of the work that you've done, I think we found a spirit of compromise. We've worked really well together. We've had occasional areas of disagreement, but we have respect for one another's views, and we found a way through them together. This is the hallmark of a good committee

Quand j'ai assumé la présidence, personne ici ne pouvait imaginer que la Russie envahirait l'Ukraine quelques semaines plus tard. Le moins qu'on puisse dire est que cela a changé la donne, et on est en droit d'estimer que la situation est devenue plus intense et plus dangereuse à l'échelle mondiale depuis.

Nous avons vu le Canada se joindre à l'opération UNIFIER avant l'invasion pour entamer la formation des troupes de combat. Ursula von der Leyen et d'autres ont reconnu que nos forces ont notablement amélioré la capacité de l'Ukraine à résister à cette première invasion. C'est vraiment un compliment, et nous avons constaté cette capacité pendant notre mandat.

Nous avons vu les Forces canadiennes diriger un groupe de combat composé de dix pays en Lettonie, au camp Adazi, avec une démonstration de force à la frontière dans le cadre d'une série de groupes de combat multinationaux. Nous avons traversé l'Arctique ensemble. Nous y avons rencontré des communautés autochtones, des Rangers canadiens, nos forces de défense de l'Arctique, des représentants autochtones, et nous avons été bien accueillis et avons beaucoup appris de cette expérience.

Nous avons vu de nos propres yeux la seule et unique structure de commandement militaire binationale au monde en opération au QG du NORAD, à Colorado Springs. Si vous vous souvenez bien, les deux commandants canadien et américain ont assuré un leadership sans faille pendant que ces ballons étaient dans les airs. Cela a coïncidé avec notre voyage là-bas.

Cela a été un privilège de le faire, et, plus sûrement encore, de le faire avec vous.

Nous avons examiné des quantités d'initiatives législatives importantes à la Chambre, dont des projets de loi hautement prioritaires et, récemment, des mesures législatives visant à lutter contre l'ingérence étrangère dans les processus démocratiques du Canada, qui nous sont plus que jamais nécessaires et qui ont été plus largement discutées aujourd'hui. Nous avons examiné ensemble le projet de loi sur les armes à feu. Nous sommes en train d'examiner le projet de loi C-26, qui vise à aider les organisations canadiennes à lutter contre l'ingérence et les cyberattaques. Durant les trois dernières années, nous avons été témoins de tentatives multiples et croissantes en matière d'ingérence étrangère et de cyberingérence dans notre pays, mais aussi de tentatives de plus en plus musclées de la part de la Russie, de la Chine et de l'Iran, non seulement à l'échelle globale, mais aussi sous la forme de pressions sur les diasporas dans ce pays et sur nos collectivités. C'est un changement radical de situation.

Dans tout cela, dans tout le travail que vous avez fait, je crois que nous avons su trouver un esprit de compromis. Nous avons vraiment bien travaillé ensemble. Il y a eu des désaccords à l'occasion, mais nous respectons les points de vue les uns des autres, et nous avons trouvé une façon de les conjuguer. C'est la

and any good organization. You have all contributed to that equally, and I'm really grateful for it, and I've benefited from it.

I want to finish with some thank yous, first to my steering committee colleagues and the deputy chair, who stood in for me on some big meetings. I wasn't absent on purpose, Senator Dagenais, but I watched you from afar, and you did a fantastic job, as usual. But joining me at steering, Senator Carignan, Senator Anderson, Senator Cardozo periodically, and, previously, Senator Boisvenu, all who have been wonderful, collaborative colleagues and who have worked to find a good balance among competing priorities and sometimes competing perspectives, but we got there together in the end, which is the best way to do it.

I want to thank our staff, who, every week in this room and across numerous other committees — our translators, our audio technologists, Senate pages and the myriad of others — ensure we look reasonably good every day in the work that we do.

I also want to acknowledge our own staff who support us every day. I thank your staff, but I look to my own staff, Hilary Bittle, who has been by my side for the last year or so and kept me going and kept me on track and reminded me of where I need to be and what I need to do. That is terrific support that has been hugely important, including at this committee.

I want to thank Lauren Thomas, who worked with me going back to Bill C-45, the legalization of cannabis bill, and who worked with me ever since until very recently. I told Ms. Thomas that our work was almost done, and then I joined this committee, and then Lauren had to do that work as well. She has now moved to Senator McNair's office, where I know she continues to do good work.

I'm going to wrap up by thanking our clerk, Ericka Paajanen, and our Library of Parliament analysts, Anne-Marie Therrien-Tremblay and Ariel Shapiro. I've sometimes mistakenly referred to Ms. Paajanen as the chair of the committee, and that's well earned.

Let me say this: I have worked over a long period of my career with public servants at all levels — municipal, provincial and federal — and I have worked with terrific public servants — analysts, advisers, managers and strategists. I can tell you that the three people who sit alongside me every week are second to none in comparison with the people I've worked with in other levels of my work. They are exemplary, and I will say that they bring good judgment, due diligence, emotional intelligence and an ethic of service quality, not just to me, but to this committee and to the Senate as a whole.

caractéristique d'un bon comité et de toute bonne organisation. Vous y avez tous contribué également, et je vous en suis vraiment reconnaissant. J'en ai moi-même tiré profit.

J'aimerais terminer par quelques remerciements, tout d'abord à l'endroit de mes collègues du comité directeur et du vice-président, qui m'ont remplacé à des réunions importantes. Je n'étais pas absent exprès, sénateur Dagenais, mais je vous ai observé de loin, et vous avez fait un travail fantastique, comme d'habitude. Au comité directeur se sont joints périodiquement les sénateurs Carignan, Cardozo et la sénatrice Anderson, ainsi que le sénateur Boisvenu, qui ont tous été des collègues merveilleux et coopératifs et qui ont travaillé à trouver un bon équilibre entre des priorités contradictoires et parfois des points de vue divergents, mais nous avons fini par nous entendre, ce qui est la meilleure façon de procéder.

Je tiens à remercier notre personnel qui, chaque semaine, dans cette salle et dans de nombreux autres comités — nos traducteurs, nos technologues de l'audio, les pages du Sénat et beaucoup d'autres — veillent à ce que nous fassions bonne figure, raisonnablement, chaque jour.

Je tiens également à remercier notre propre personnel, qui nous appuie chaque jour. Je remercie votre personnel, mais je me tourne vers Hilary Bittle, qui est à mes côtés depuis environ un an, qui m'a aidé et qui me rappelait où je devais être et ce que je devais faire. C'est un soutien formidable et extrêmement important, notamment au sein de ce comité.

Je tiens à remercier Lauren Thomas, qui a travaillé avec moi au projet de loi C-45 sur la réglementation du cannabis, et qui est restée à mes côtés jusqu'à tout récemment. J'ai dit à Mme Thomas que notre travail était presque terminé, après quoi je me suis joint à ce comité, et elle a été appelée à faire le même travail. Elle est désormais au service du sénateur McNair, auprès de qui je sais qu'elle continuera de faire du bon travail.

Je vais conclure en remerciant notre greffière, Ericka Paajanen, ainsi que nos analystes de la Bibliothèque du Parlement, Anne-Marie Therrien-Tremblay et Ariel Shapiro. Je me suis parfois trompé en disant que Mme Paajanen était la présidente du comité, mais elle le méritait bien.

Permettez-moi de dire ceci : j'ai travaillé pendant longtemps avec des fonctionnaires de tous les niveaux — à l'échelle municipale, provinciale et fédérale — et j'ai travaillé avec d'excellents fonctionnaires — des analystes, des conseillers, des gestionnaires et des stratèges. Je peux vous dire que les trois personnes qui siègent à mes côtés chaque semaine n'ont rien à envier à ceux avec qui j'ai travaillé à d'autres niveaux. Elles sont exemplaires, et je dirais qu'elles apportent un bon jugement, une diligence raisonnable, une intelligence émotionnelle et une éthique de la qualité du service, non seulement à moi, mais à ce comité et au Sénat dans son ensemble.

And here is the important thing, they are unafraid to provide the right advice when I, or we, are occasionally inclined to go down the wrong path — perhaps for the right reasons, but it might be the wrong path — to take us aside and give us the best of their advice. The three of you have saved me from going to places that I shouldn't have gone, and likely saved this committee as well, and for that, I'm really grateful for your good judgment and counsel and hard work.

That being said, colleagues, I now take my leave, knowing that we have a committee at the top of its game, and I know we'll have a succeeding chair at the top of their game. I congratulate you all on your hard work and achievements, and I thank you for your support.

Do I now — moving on — see a mover for our next chair?

[*Translation*]

Senator Dagenais: Mr. Chair, with your permission, I would like to nominate Senator Yussuff.

[*English*]

The Chair: Thank you for that nomination.

An Hon. Senator: I'd like to second that.

The Chair: Thank you.

What is the wish of the committee? I see approval. Thank you.

I'm going to invite Senator Yussuff to come up and assume the chair. I am going to leave now and leave this room to Senator Yussuff — and to you — as this transition takes place, and I wish you all the best, and I will see you all in the chamber tomorrow.

Thanks very much.

Senator Hassan Yussuff (Chair) in the chair.

The Chair: As our colleague is leaving, I think it would be equally important to acknowledge his eloquence, his thoughtfulness and the collaborative way in which he's chaired our committee meeting.

I don't think there was a time I left this meeting feeling that somehow I wasn't heard or wasn't given a fair opportunity to intervene, even when we were competing for space to try to ask the witnesses a question.

In assuming this responsibility, I realize I will pale in comparison to his leadership, as to what I would bring. I would ask for two things, one, I would bring as much thoughtfulness and collaboration as our previous chair has committed to this

Et surtout, elles n'ont pas peur de nous donner de bons conseils quand moi ou d'autres parmi nous sont parfois enclins à emprunter la mauvaise voie — peut-être pour de bonnes raisons, mais pas par les bons moyens —, et de nous prendre à part pour nous donner le meilleur de leurs conseils. Vous m'avez tous les trois évité de m'engager dans des avenues où je ne devais pas aller, et vous l'avez probablement aussi évité au comité. Je vous suis vraiment reconnaissant de votre bon jugement, de vos conseils et de votre travail acharné.

Cela dit, chers collègues, je vais maintenant vous quitter, sachant que nous avons un excellent comité et que j'aurai aussi un excellent successeur. Je vous félicite tous de votre travail acharné et de vos réalisations et je vous remercie de votre appui.

Est-ce que je vois quelqu'un proposer la candidature de notre prochain président?

[*Français*]

Le sénateur Dagenais : Monsieur le président, avec votre permission, je vais proposer le sénateur Yussuff.

[*Traduction*]

Le président : Merci de cette nomination.

Une voix : J'appuie la proposition.

Le président : Merci.

Que souhaite le comité? Je vois que vous approuvez. Merci.

J'invite le sénateur Yussuff à occuper le fauteuil. Je vais maintenant vous quitter et céder la parole au sénateur Yussuff — et à vous — pendant cette transition. Je vous souhaite la meilleure des chances. Nous nous retrouverons au Sénat demain.

Merci beaucoup.

Le sénateur Hassan Yussuff (président) occupe le fauteuil.

Le président : Au moment où notre collègue nous quitte, je pense qu'il est tout aussi important de souligner son éloquence, sa générosité et sa présidence marquée par la collaboration.

Je ne me souviens pas d'une seule fois où j'aurais quitté la réunion en ayant l'impression que je n'avais pas été entendu ou que je n'avais pas eu l'occasion d'intervenir, même quand nous nous disputions la place pour essayer de poser une question à des témoins.

En assumant cette responsabilité, je me rends compte que ma contribution sera bien modeste en comparaison de son leadership. Je vous demande deux choses : premièrement, je me montrerai aussi généreux et coopératif que notre président

committee, but equally I know in time I will make mistakes and, when I do, I would hope you would show me some kindness but also give me an opportunity to correct whatever it is I may have erred on.

I'm hoping in the context of assuming the responsibility, we can work with the same degree of collaboration we have had, at least for the time I've been on this committee.

I should share a secret. When I first came to this committee, I didn't necessarily volunteer to be here. My arm was twisted because the chair asked me to join the committee. I would have to say in the three years I've been on the committee, I've enjoyed every moment that we have been together and enjoyed every aspect of bills and studies that we have done in the last three years. I want to thank my colleagues for the confidence you're placing in my hands. I commit to continue the collaborative way we work, with the respect and appreciation there will be many things that we will be faced with, hopefully — with steering but also with members of the committee — we can work in the same thoughtful and respectful way we've worked over the last three years. To continue to do the good work on behalf of the citizens of our country, to ensure we're making a difference in the bills we are studying, but also in the studies we are doing, contribute to the greater good of this country.

I'll stop there and take any questions. I want to thank my colleagues for the confidence placed on the Independent Senators Group, or ISG, that is based in me, and I want to thank all colleagues on the committee. I look forward to Ms. Paajanen and our colleagues' guidance because I know there is much to learn. I'm open to learning as much as I need to ensure I do a good job on the committee.

I watched our previous chair break this last time we were meeting, so I will try to be as gentle as I can. If not, I'll bring my own hammer the next time. Without further ado, I declare our meeting adjourned.

(The committee adjourned.)

précédent, mais je sais aussi que je ferai des erreurs et, dans ce cas, j'espère que vous me témoignerez de la gentillesse, mais aussi que vous me donnerez l'occasion de me corriger.

J'espère que, dans le contexte où j'assume cette responsabilité, nous pourrons travailler avec le même degré de collaboration, du moins de ce que j'ai vu depuis que je siège à ce comité.

Je crois devoir partager un secret. Quand je suis arrivé ici, ce n'était pas parce que je l'avais voulu et décidé. On m'a tordu le bras, puisque c'est le président qui m'a demandé de me joindre au comité. Je dois dire que, au cours des trois années où j'y ai siégé, j'ai apprécié chaque moment que nous avons passé ensemble, mais aussi tous les aspects des projets de loi et des études que nous avons réalisés. Je tiens à remercier mes collègues de la confiance qu'ils me témoignent. Je m'engage à continuer de travailler dans un esprit de collaboration et avec respect et gratitude. Nous affronterons bien des choses, et espérons que, avec le comité directeur, mais aussi avec les membres du comité, nous pourrons travailler de la même façon posée et respectueuse que nous l'avons fait depuis trois ans. Continuons de faire du bon travail au nom des citoyens de notre pays, de nous assurer que nous faisons une différence dans les projets de loi que nous étudions, mais aussi dans les études que nous faisons, et contribuons au bien commun de notre pays.

Je vais m'arrêter ici et répondre à vos questions. Je tiens à remercier mes collègues de la confiance qu'ils ont accordée au GSI, le Groupe des sénateurs indépendants, dont je suis responsable, et je remercie tous mes collègues du comité. Je serai attentif aux conseils de Mme Paajanen et de nos collègues, car je sais qu'il y a beaucoup à apprendre. Je suis prêt à en apprendre autant que je le devrai pour m'assurer de faire du bon travail au comité.

J'ai vu comment s'y est pris notre président précédent la dernière fois que nous nous sommes réunis, et je vais donc essayer d'être aussi délicat que possible. Sinon, j'apporterai mon propre marteau la prochaine fois. Sans plus tarder, je déclare la séance levée.

(La séance est levée.)