EVIDENCE

OTTAWA, Monday, October 28, 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: Honourable senators, before we begin, I would ask all senators and other in-person participants to consult the cards on the table for guidelines to prevent audio feedback incidents. Thank you for your cooperation.

Welcome to this meeting of the Standing Senate Committee on National Security, Defence and Veterans Affairs. I am Tony Dean, a senator from Ontario and chair of the committee. I am joined today by my fellow colleagues, who will introduce themselves beginning with our deputy chair.

[*Translation*]

Senator Dagenais: Jean-Guy Dagenais from Quebec.

[*English*]

Senator Richards: Dave Richards, New Brunswick.

Senator Patterson: Rebecca Patterson, Ontario.

Senator Fridhandler: Daryl Fridhandler, Alberta

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

Senator Gold: Marc Gold, Quebec.

Senator Dasko: Donna Dasko, a senator from Ontario and a member of this committee.

Senator Duncan: Pat Duncan, senator for the Yukon.

Senator Kutcher: Stan Kutcher, Nova Scotia.

Senator McNair: John McNair, New Brunswick.

Senator Boehm: Peter Boehm, Ontario.

Senator Yussuff: Hassan Yussuff, Ontario.

TÉMOIGNAGES

OTTAWA, le lundi 28 octobre 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 : Honorables sénateurs, avant de commencer, je demanderais à tous les sénateurs et autres participants en personne de consulter les cartes sur la table pour les directives visant à prévenir les incidents de retour de son. Je vous remercie de votre coopération.

Bienvenue à cette réunion du Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants. Je m'appelle Tony Dean, sénateur de l'Ontario et président du comité. Je suis accompagné aujourd'hui par mes collègues, qui se présenteront en commençant par notre vice-président.

[*Français*]

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

[*Traduction*]

Le sénateur Richards : Je suis Dave Richards, du Nouveau-Brunswick.

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

Le sénateur Fridhandler : Daryl Fridhandler, de l'Alberta.

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

Le sénateur Gold : Marc Gold, du Québec.

La sénatrice Dasko : Je suis Donna Dasko, sénatrice de l'Ontario et membre de ce comité.

La sénatrice Duncan : Pat Duncan, sénatrice du Yukon.

Le sénateur Kutcher : Stan Kutcher, de la Nouvelle-Écosse.

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

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

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

[*Translation*]

Senator Carignan: Claude Carignan from Quebec.

[*English*]

Senator Batters: Denise Batters, Saskatchewan.

The Chair: Thank you. We have a full house today. Ericka Paajanen is the clerk of the committee. To my right are our Library of Parliament analysts Anne-Marie Therrien-Tremblay and Ariel Shapiro.

Today, colleagues, we begin our consideration of Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.

To kick off this work, I am pleased to welcome back the Honourable Dominic LeBlanc, Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs; and the Honourable François-Philippe Champagne, Minister of Innovation, Science and Industry.

The ministers are accompanied today by the following officials from Public Safety Canada: Patrick Boucher, Senior Assistant Deputy Minister, National and Cyber Security Branch; Colin MacSween, Director General, National and Cyber Security Branch; and Kelly-Anne Gibson, Acting Director, National and Cyber Security Branch. From Innovation, Science and Economic Development Canada's Spectrum and Telecommunications Sector, we have Martin Proulx, Director General; Wen Kwan, Senior Director; David Gibson, Director; and from the Strategy and Innovation Policy Sector, Andre Arbour, Director General.

Thank you for joining us today. We now ask you to provide your opening remarks, beginning with Minister LeBlanc. It is good to see you again. Whenever you are ready.

The Honourable Dominic LeBlanc, P.C., M.P., Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs: Mr. Chair, I am always ready, and I am always happy to be here. Thank you, sir, to you and your colleagues for this opportunity as well.

Cyber-threats have grown more complex and sophisticated, and they are being undertaken by state and non-state actors alike. Bill C-26 — which you, Mr. Chair, properly noted, is before this committee — will protect Canadians and bolster cybersecurity across the federally regulated financial, telecommunications, energy and transportation sectors. Those are the big ones that we collectively think of when we speak about federally regulated sectors of the economy.

[*Français*]

Le sénateur Carignan : Claude Carignan, du Québec.

[*Traduction*]

La sénatrice Batters : Denise Batters, de la Saskatchewan.

Le président : Merci. La salle est pleine aujourd'hui. Ericka Paajanen est la greffière du comité. À ma droite se trouvent Anne-Marie Therrien-Tremblay et Ariel Shapiro, analystes à la Bibliothèque du Parlement.

Aujourd'hui, chers collègues, nous entamons l'examen 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.

Pour lancer ces travaux, j'ai le plaisir d'accueillir à nouveau l'honorable Dominic LeBlanc, ministre de la Sécurité publique, des Institutions démocratiques et des Affaires intergouvernementales, et l'honorable François-Philippe Champagne, ministre de l'Innovation, des Sciences et de l'Industrie.

Les ministres sont accompagnés aujourd'hui des fonctionnaires suivants de la Direction de la sécurité nationale et de la cybersécurité à Sécurité publique Canada : M. Patrick Boucher, sous-ministre adjoint principal; M. Colin MacSween, directeur général; et Mme Kelly-Anne Gibson, directrice par intérim. Du Secteur du spectre et des télécommunications d'Innovation, Sciences et Développement économique Canada, nous avons M. Martin Proulx, directeur général; M. Wen Kwan, directeur principal; et M. David Gibson, directeur. Nous avons aussi M. André Arbour, directeur général du Secteur des stratégies et politiques d'innovation à ISDEC.

Merci de vous joindre à nous aujourd'hui. Nous vous demandons maintenant de présenter vos remarques préliminaires, en commençant par le ministre LeBlanc. C'est un plaisir de vous revoir. Si vous êtes prêt, allez-y.

L'honorable Dominic LeBlanc, c.p., député, ministre de la Sécurité publique, des Institutions démocratiques et des Affaires intergouvernementales : Monsieur le président, je suis toujours prêt et je suis toujours heureux d'être ici. Je vous remercie, vos collègues et vous, de me donner cette occasion.

Les cybermenaces, qui émanent tant d'acteurs étatiques que non étatiques, sont de plus en plus complexes et sophistiquées. Le projet de loi C-26, dont vous êtes saisis, comme vous l'avez pertinemment fait remarquer, monsieur le président, protégera les Canadiens et renforcera la cybersécurité dans les secteurs de la finance, des télécommunications, de l'énergie et du transport, qui sont réglementés par le gouvernement fédéral. Ce sont les grands secteurs auxquels nous pensons collectivement lorsque nous parlons des secteurs de l'économie réglementés par Ottawa.

The Communications Security Establishment Canada, or CSE, has said cybercrime is now the most prevalent and pervasive threat to Canadians and Canadian businesses. The CSE's Canadian Centre for Cyber Security has warned us of the many risks, with ransomware at the top of the list. We've already seen the damage that such a cyberincident can cause when a U.S. energy company was the target of a ransomware attack, for example, in May 2021. A Russian criminal group extorted $4.3 million after they disrupted the largest fuel line in the United States. This incident was so significant that it led to President Biden calling a national state of emergency.

[*Translation*]

Over the past two years, we have noted a significant increase in this type of cyber-attack in Canada.

Last year, the Communications Security Establishment, or CSE, stated that a cyber-threat actor "had the potential to cause physical damage to Canadian critical infrastructure". Thankfully, there was no physical damage to Canadian infrastructure, but as the CSE's Canadian Centre for Cyber Security stated, "the threat is real". We shouldn't fool ourselves.

In June of last year, the *Calgary Herald* reported that Canadian energy company Suncor suffered a serious cyber-incident that shut down debit and credit processing at Petro-Canada gas stations across the country.

Last March, the City of Hamilton was the latest victim of a ransomware attack that interrupted a number of its online services. These are but a few examples of the recent attacks clearly showing that Canada must act immediately.

This bill would allow the government to take security measures and prohibit Canadian telecommunications service providers from using products and services from high-risk suppliers.

[*English*]

Additionally, this act will increase information sharing between industry and government by requiring designated critical infrastructure operators to report cybersecurity incidents to the CSE's Cyber Centre. Mandating the sharing of essential information will improve the government's awareness of the cyber-threat landscape across the country. When the government has a clearer picture of the threat facing critical infrastructure providers, we can warn operators of potential threats and vulnerabilities. Bill C-26 will make one organization's detection another's prevention. Further, designated operators of vital

Le Centre de la sécurité des télécommunications Canada, ou CST, a déclaré que la cybercriminalité est désormais la menace la plus répandue et la plus omniprésente pour les Canadiens et les entreprises canadiennes. Le Centre canadien pour la cybersécurité du CST nous a mis en garde contre les nombreux risques, les rançongiciels figurant en tête de liste. Par exemple, nous avons déjà constaté les dégâts qu'un tel cyberincident peut causer lorsqu'une entreprise énergétique américaine a été la cible d'une attaque par rançongiciel en mai 2021. Un groupe criminel russe a extorqué 4,3 millions de dollars après avoir interrompu la plus grande canalisation de carburant des États-Unis. Cet incident a été si important qu'il a conduit le président Biden à décréter l'état d'urgence national.

[*Français*]

Au cours des deux dernières années, nous avons constaté une augmentation notable de ce genre de cyberattaques au Canada.

L'année dernière, le Centre de la sécurité des télécommunications Canada (CST) a déclaré qu'un cyberacteur « [...] avait le potentiel de causer des dommages physiques à des infrastructures essentielles canadiennes » . Heureusement, aucune infrastructure canadienne n'a subi de dommages physiques, mais comme l'a dit le Centre canadien pour la cybersécurité du CST : « [...] la menace est réelle ». Il ne faut pas se leurrer.

En juin de l'année dernière, le *Calgary Herald* a rapporté que la société énergétique canadienne Suncor avait été victime d'un grave incident cybernétique qui avait interrompu les transactions de débit et de crédit dans les stations-service de Petro-Canada dans tout le pays.

En mars dernier, la ville de Hamilton a été la dernière victime d'une attaque de rançongiciel qui a interrompu plusieurs de ses services en ligne. Ces exemples sont seulement quelques-unes des attaques récentes qui montrent clairement que le Canada doit agir de toute urgence.

Le projet de loi permettra au gouvernement de prendre des mesures de sécurité et d'interdire aux fournisseurs de services de télécommunication canadiens d'utiliser des produits ou des services provenant de fournisseurs à haut risque.

[*Traduction*]

De plus, cette loi renforcera le partage d'informations entre l'industrie et le gouvernement, en obligeant les opérateurs d'infrastructures essentielles désignées à signaler les incidents de cybersécurité au Centre pour la cybersécurité du CST. L'obligation de partager des informations névralgiques permettra au gouvernement de mieux connaître le paysage des cybermenaces dans l'ensemble du pays. Lorsque le gouvernement a une idée plus précise de la menace à laquelle sont confrontés les fournisseurs d'infrastructures essentielles, il peut les avertir des menaces et des vulnérabilités potentielles.

services and systems would be obligated to implement cybersecurity programs, mitigate supply chain and third-party risks, and comply with cybersecurity directions.

The House Standing Committee on Public Safety and National Security, as members of this committee will know, made a number of notable amendments related to reasonableness, oversight and privacy protection. The committee amended the bill in the House to add reasonableness standards for the issuing of ministerial orders and cybersecurity directions; implement robust review provisions to ensure the National Security and Intelligence Committee of Parliamentarians and the National Security and Intelligence Review Agency have the ability to review the government's orders and directions; and references, as colleagues would know, were explicitly made to the Privacy Act and the government's obligation, of course, to respect that legislation.

[*Translation*]

Dear colleagues, we believe this bill has great merit. It was passed unanimously in the House of Commons. To conclude, the bill is in line with legislation established by our Five Eyes partners.

[*English*]

It's a much better acronym in English — Five Eyes. When the ministers meet, there are actually 10 eyes in the room. I pointed that out at my first meeting. Secretary Mayorkas still makes that joke.

[*Translation*]

The bill will protect Canadians, private sector firms and the cyber-systems Canadians rely on each day. Thank you very much.

[*English*]

The Chair: Thank you, Minister LeBlanc.

Colleagues, we will hear next from Minister Champagne. Whenever you are ready.

[*Translation*]

The Honourable François-Philippe Champagne, P.C., M.P., Minister of Innovation, Science and Industry: Thank you, Mr. Chair. Thank you, colleagues. I believe this is the first time I have appeared before this senate committee. Thank you

Avec le projet de loi C-26, la détection au sein d'une organisation permettra de prévenir les autres. En outre, les fournisseurs désignés de services et de systèmes essentiels seraient tenus de mettre en œuvre des programmes de cybersécurité, d'atténuer les risques liés à la chaîne d'approvisionnement et aux tiers, et de se conformer aux directives en matière de cybersécurité.

Comme vous le savez, le Comité permanent de la sécurité publique et nationale de la Chambre des communes a apporté un certain nombre d'amendements notables concernant le caractère raisonnable, la surveillance et la protection de la vie privée. Le comité a amendé le projet de loi afin d'ajouter des normes liées au caractère raisonnable pour la prise d'arrêtés ministériels et de directives en matière de cybersécurité; de mettre en œuvre des dispositions d'examen solides afin de garantir que le Comité des parlementaires sur la sécurité nationale et le renseignement et l'Office de surveillance des activités en matière de sécurité nationale et de renseignement aient la capacité d'examiner les arrêtés et les directives du gouvernement; et des références, comme les collègues le savent, ont été explicitement faites à la Loi sur la protection des renseignements personnels et à l'obligation du gouvernement, bien sûr, de respecter cette loi.

[*Français*]

Chers collègues, il s'agit d'un projet de loi qui a un grand mérite, à notre avis. Il a été adopté par l'autre Chambre de façon unanime. En guise de conclusion, le projet de loi est conforme à la législation établie par nos partenaires du Groupe des cinq.

[*Traduction*]

C'est une bien meilleure désignation en anglais : les *Five Eyes*. Quand les ministres se rencontrent, il y a toutefois 10 yeux dans la salle. Je l'ai fait remarqué lors de la première séance à laquelle je participais. D'ailleurs, le secrétaire Mayorkas répète toujours cette blague.

[*Français*]

Le projet de loi protégera les Canadiennes et les Canadiens, les entreprises du secteur privé et les cybersystèmes dont dépendent nos concitoyens quotidiennement. Merci beaucoup.

[*Traduction*]

Le président : Merci, monsieur le ministre.

Nous entendrons maintenant le ministre Champagne. Allez-y quand vous serez prêt.

[*Français*]

L'honorable François-Philippe Champagne, c.p., député, ministre de l'Innovation, des Sciences et de l'Industrie : Merci, monsieur le président. Merci, chers collègues. Je pense que c'est la première fois que je comparais

for your welcome and for inviting me to appear and discuss Bill C-26, a bill of paramount importance for Canada's security.

The fact that I am here today with my friend and colleague the Honourable Minister of Public Safety shows the intersectionality between telecommunications and public safety in the 21st century.

More specifically, I would like to speak to you about Part I of the bill, which will amend the Telecommunications Act to better secure our telecommunications networks.

[*English*]

Canadians increasingly rely on the internet and wireless services in their day-to-day lives. Anyone who has kids or who operates a business in this country will know this to be true. From financial transactions and e-commerce to education, health care and emergency services, such as 9-1-1, these critical services need to rely on a robust, modern and safe telecommunications system.

We know, however, that risks to this critical infrastructure are on the rise. Minister LeBlanc mentioned many of them, and we have seen many of them not only in Canada but with many of our partners and allies around the world. We need to be vigilant and engaged when we talk about cyber threats and cybersecurity, with our eyes wide open. The risks I am talking about include nefarious actions by hostile foreign states who seek to compromise our critical infrastructure — Minister LeBlanc mentioned a number of ransom threats, some of which have been very public in the recent past — and telecom products from global suppliers that pose an unacceptable risk to the Canadian telecommunications systems.

This is where Bill C-26 comes in. I would echo the words of Minister LeBlanc to say there is urgency to act to make sure that we would, as a government, have the tools to protect Canadians, protect our national security and protect our economic security. It would allow the government, when necessary, to prohibit Canadian telecom service providers from using products from high-risk suppliers. This will, in turn, help secure our critical infrastructure from various threats.

[*Translation*]

We need to act quickly and decisively. I'm therefore pleased the bill has such strong cross-party support at the House of Commons. Honourable senators, you saw that all members of the House of Commons supported the initiative we put forward in

devant ce comité du Sénat. Je vous remercie de votre accueil et de votre invitation à comparaître au sujet du projet de loi C-26, un projet de loi d'importance capitale pour la sécurité du Canada.

Le fait que je sois ici aujourd'hui avec mon collègue et ami, l'honorable ministre de la Sécurité publique, témoigne de l'intersection qui existe entre les télécommunications et la sécurité publique au 21e siècle.

Plus précisément, je vais vous parler aujourd'hui de la partie I du projet de loi qui modifiera la Loi sur les télécommunications afin de mieux sécuriser nos réseaux de télécommunications.

[*Traduction*]

Les Canadiens dépendent de plus en plus d'Internet et des services sans fil dans leur vie quotidienne. Ceux qui ont des enfants ou qui exploitent une entreprise dans ce pays le savent bien. Qu'il s'agisse de transactions financières, de commerce électronique, d'éducation, de soins de santé ou de services d'urgence tels que le 9-1-1, ces services essentiels doivent pouvoir compter sur un système de télécommunications robuste, moderne et sûr.

Nous savons cependant que les risques qui pèsent sur cette infrastructure critique sont en augmentation. Le ministre LeBlanc en a mentionné plusieurs, et nous en avons vu beaucoup, non seulement au Canada, mais aussi chez bon nombre de nos partenaires et alliés dans le monde. Nous devons être vigilants et déterminés lorsque nous parlons de cybermenaces et de cybersécurité, en gardant les yeux grands ouverts. Les risques dont je parle comprennent les actions malveillantes d'États étrangers hostiles qui cherchent à compromettre nos infrastructures critiques — le ministre LeBlanc a mentionné un certain nombre de menaces de rançon, dont certaines ont été très publiques ces derniers temps —, et les produits de télécommunications de fournisseurs mondiaux qui posent un risque inacceptable pour les systèmes de télécommunications canadiens.

C'est là qu'intervient le projet de loi C-26. J'aimerais faire écho au ministre LeBlanc en déclarant qu'il est urgent d'agir pour s'assurer que le gouvernement dispose des outils nécessaires pour protéger les Canadiens, notre sécurité nationale et notre sécurité économique. Il permettrait au gouvernement, si nécessaire, d'interdire aux fournisseurs canadiens de services de télécommunications d'utiliser des produits provenant de fournisseurs à haut risque. Cela contribuera à son tour à protéger nos infrastructures essentielles contre diverses menaces.

[*Français*]

Nous devons agir de façon rapide et décisive. C'est pourquoi je suis ravi d'un appui aussi fort de tous les partis à la Chambre des communes pour ce projet de loi. Les honorables sénateurs ont vu que l'ensemble des membres de la Chambre des

Bill C-26. Protecting and securing our telecommunication networks is essential.

[*English*]

I was also pleased to see strong cross-party support in the House to further strengthen the bill at the committee stage in response to views that have been expressed by stakeholders and a number of witnesses. For example, we have seen amendments that were made to ensure that confidential information remains protected. Indeed, the bill now explicitly states that Canadians' personal information and privacy will be protected in accordance with the Privacy Act. I want to be clear that Bill C-26 has never been about collecting the data of Canadians or monitoring communications. That is precisely why language has been added to eliminate any confusion in this regard. Moreover, amendments were added to provide further transparency to stakeholders in terms of reporting, as well as an explicit reasonableness test for the powers that have been vested in the minister and the Governor-in-Council in the bill. In short, there is solid consensus when it comes to Bill C-26, and we expect telecom service providers to act decisively to protect Canada's telecommunications system.

Now let me say a few words about what this bill is not. For one, Bill C-26 is not intended to punish providers that diligently work to protect consumers and themselves. This has been made clear with an explicit due diligence defence. You may have seen that this has been added at the committee stage. The due diligence defence is in the monetary penalties authorities that have been vested with the minister and the Governor-in-Council, having heard and incorporated the concerns of stakeholders.

Second, Bill C-26 is not about avoiding accountability in the name of quick action. This is more about giving the minister, in the case of the telecom network, the ability to act decisively, strategically and in accordance with best practices to protect our national security. On the contrary, this bill will help to protect the safety and security of Canada's critical infrastructure without compromising individual privacy or rights.

[*Translation*]

Mr. Chair, allow me to conclude with the following: A modern and innovative nation like Canada has a duty to ensure it has reliable and secure telecommunications networks. I am firmly convinced that Bill C-26 sets the path for working with telecommunication operators to ensure the security of our

communes ont appuyé l'initiative que l'on propose dans le projet de loi C-26. En effet, la protection et la sécurité de nos réseaux de télécommunication sont primordiales.

[*Traduction*]

J'ai également été heureux de constater que l'ensemble des partis de la Chambre ont soutenu le renforcement du projet de loi au stade du comité, en réponse aux points de vue exprimés par les parties prenantes et par un certain nombre de témoins. Par exemple, des amendements ont été apportés pour garantir la protection des informations confidentielles. En effet, le projet de loi stipule désormais explicitement que les renseignements personnels et la vie privée des Canadiens seront protégés conformément à la Loi sur la protection des renseignements personnels. Je tiens à préciser que le projet de loi C-26 n'a jamais eu pour objet de recueillir les données des Canadiens ou de surveiller leurs communications. C'est précisément la raison pour laquelle un libellé a été ajouté afin d'éliminer toute confusion à cet égard. En outre, des amendements ont été ajoutés afin d'assurer une plus grande transparence pour les parties prenantes pour les rapports, ainsi qu'un test explicite de caractère raisonnable pour les pouvoirs qui ont été conférés au ministre et au gouverneur en conseil dans le projet de loi. En résumé, le projet de loi C-26 fait l'objet d'un consensus solide et nous attendons des fournisseurs de services de télécommunications qu'ils agissent de manière décisive pour protéger le système canadien de télécommunications.

Maintenant, permettez-moi de dire quelques mots sur ce que ce projet de loi n'est pas. Tout d'abord, le projet de loi C-26 ne vise pas à punir les fournisseurs qui travaillent avec diligence pour protéger les consommateurs et se protéger eux-mêmes. C'est clairement établi par une défense explicite de diligence raisonnable. Vous avez peut-être vu qu'elle a été ajoutée à l'étape du comité. La défense de diligence raisonnable se trouve dans les pouvoirs de sanctions pécuniaires qui ont été conférés au ministre et au gouverneur en conseil, après avoir entendu et pris en compte les préoccupations des parties prenantes.

Deuxièmement, le projet de loi C-26 ne vise pas à éviter la responsabilité au nom d'une action rapide. Il s'agit plutôt de donner au ministre, dans le cas du réseau de télécommunications, la capacité d'agir de façon décisive, stratégique et conformément aux meilleures pratiques afin de protéger notre sécurité nationale. Au contraire, ce projet de loi contribuera à protéger la sûreté et la sécurité des infrastructures essentielles du Canada sans compromettre la vie privée ou les droits des personnes.

[*Français*]

Monsieur le président, permettez-moi de conclure en disant ceci : un pays moderne et novateur comme le Canada se doit d'avoir des systèmes de télécommunication qui sont fiables et sécurisés. Je suis fermement convaincu que le projet de loi C-26 ouvre la voie à la collaboration avec les opérateurs de

systems and networks in the interest of the country and of Canadians.

In closing, Mr. Chair, thank you for giving me the opportunity to address the committee. Like my colleague, I believe we must act quickly to protect our systems and face the threats that we are subjected to in the 21st century and ensure the health and safety of Canadians.

Thank you, Mr. Chair.

[*English*]

The Chair: Thank you very much, Mr. Champagne.

Colleagues, we will now proceed to questions. Four minutes is allotted for each question, including the answer, as usual. Please keep your questions succinct in an effort to allow as many interventions as possible. We have a long list, so when there are 30 seconds remaining, I will be showing the red card, for those football fans in the room. The first question goes to our deputy chair, Senator Dagenais.

[*Translation*]

Senator Dagenais: My first question is to Minister LeBlanc.

Minister, with the opinions that businesses such as Bell and Québecor have put forward over the past few months on the CRTC's capacity and slowness in modernizing Canadian telecommunications regulations, to what degree can you assure us that the organization will be able to quickly and effectively apply the cybersecurity rules set out in C-26? How quickly do you expect the CRTC to respond? Also, does the CRTC have the resources needed to meet this type of challenge?

Mr. LeBlanc: If you'll allow me, senator, that's an excellent question. The portions dealing with the CRTC are in my colleague's hands. He will be able to provide a more specific answer than I can.

Mr. Champagne: Is that all right with you, senator?

Senator Dagenais: That works for me.

Mr. Champagne: We cover it in tandem, Minister LeBlanc and me.

Senator, you ask a very important question. You'll see that, in Bill C-26, the authority is in the hands of the Minister of Industry in a number of ways. To take specific and decisive measures, as we said, we need to act quickly. The nature of the threats we are facing is varied. There is the issue of cybersecurity

télécommunication pour assurer la sécurité de nos systèmes et de nos réseaux dans l'intérêt du Canada et de ses citoyens.

En terminant, monsieur le président, merci de m'avoir donné l'occasion d'intervenir ici devant le comité. Comme mon collègue, je dirais qu'il y a urgence d'agir pour protéger nos systèmes à faire face aux menaces que l'on vit présentement au XX^{e} siècle et assurer la santé et la sécurité des Canadiens.

Merci, monsieur le président.

[*Traduction*]

Le président : Merci beaucoup, monsieur Champagne.

Chers collègues, nous allons maintenant passer aux questions. Quatre minutes sont prévues pour chaque question, y compris la réponse, comme d'habitude. Nous vous demandons de poser des questions succinctes afin de permettre le plus grand nombre d'interventions possibles. Nous avons une longue liste. C'est pourquoi, lorsqu'il restera 30 secondes, je montrerai le carton rouge, pour les amateurs de football présents dans la salle. La première question revient à notre vice-président, le sénateur Dagenais.

[*Français*]

Le sénateur Dagenais : Ma première question s'adresse au ministre LeBlanc.

Monsieur le ministre, avec les opinions énoncées ces derniers mois par des entreprises comme Bell et Québecor sur la capacité et la lenteur du CRTC de moderniser la réglementation canadienne sur les télécommunications, dans quelle mesure pouvez-vous nous rassurer sur la capacité de cet organisme d'être efficace et rapide en matière d'application des règles de cybersécurité qui sont énoncées dans le projet de loi C-26? Quel temps de réaction exigez-vous de sa part? Puis, le CRTC a-t-il les ressources nécessaires pour ce genre de défi?

M. LeBlanc : Si vous me le permettez, sénateur, c'est une excellente question. Les aspects qui touchent le CRTC sont entre les mains de mon collègue, qui pourra vous fournir une réponse plus précise que la mienne.

M. Champagne : Cela vous convient-il, monsieur le sénateur?

Le sénateur Dagenais : Cela me convient.

M. Champagne : On fait cela en tandem, le ministre LeBlanc et moi.

Monsieur le sénateur, c'est une question fort importante que vous posez. Vous allez voir que dans le projet de loi C-26, les pouvoirs se trouvent entre les mains du ministre de l'Industrie à plusieurs égards. Pour prendre des mesures précises et décisives, on l'a dit, il y a urgence d'agir. La nature des menaces

but, remember that in cases of bad weather and natural disasters, the Minister of Industry was called in. You'll remember also that during the Rogers incident, that infamous time when telecommunications went down for a number of hours in Canada, decisive action had to be taken. That's why, at the time, there was even an agreement made between telecommunications providers to ensure interoperability between the networks in cases of emergency, so that communications would be provided for public authorities and citizens. A mutual assistance program was also put in place because that's what we expect from telecommunication companies in extraordinary circumstances. In that specific case, you can see we were quite specific in Bill C-26 in terms of that authority, as I exercised it at the time, and so that it is in the hands of the Minister of Industry.

One aspect that I see as anachronistic, and I don't use that word lightly, is that it is one of the rare laws that provides a framework for essential infrastructure, where security is not one of the objectives. Bill C-26 corrects this situation. Security will be at the heart of the objectives, as it is in the case of energy and other critical sectors for transport. I wasn't there when the law was adopted. When I intervened at the time, senator, I would say that I often did so as a soft power. At the time, the minister did not necessarily have the authority to direct telecommunications companies to take certain actions. History has shown us that we cannot rely solely on the good faith of players. There needs to be authority under the law to require that certain actions be taken. Think of the Internet. In terms of 5G, once everything is connected, there may arise extraordinary instances in which the minister will have to take targeted and strategic action quickly to protect the country's network as a whole.

Senator Dagenais: Thank you very much for your answer.

Senator Carignan: Thank you, ministers, for being here.

While examining Bill C-26, I wondered what measures the government would put in place for itself, what it would do to practise what it preaches. I have great appreciation for that. However, it seems that the government is requiring much more of the private sector than of itself.

There is, for example, the leaks at the Canada Revenue Agency this past spring, that we just learned about through reporting by CBC/Radio-Canada. Is it not misleading to say that you are taking this seriously when leaks impacting around 30,000 people are hidden and not disclosed? Individual who were identified as victims were not informed, either. If a private sector actor did that, it would be required to pay $10 million in fines. For its part, the government of Canada and its revenue

auxquelles on fait face est variée. Il y a la question de la cybersécurité, mais vous vous rappellerez aussi dans le cas d'intempéries, de catastrophes naturelles, le ministre de l'Industrie a été appelé. Vous vous rappellerez aussi dans l'épisode de Rogers, le fameux épisode où l'on a perdu la télécommunication pendant plusieurs heures au Canada, il a fallu agir de façon décisive. C'est pour cela qu'à l'époque, on a même conclu un accord entre les télécommunicateurs pour assurer l'interopérabilité des réseaux en matière d'urgence, afin qu'il y ait de la communication avec les autorités publiques et les citoyens et un programme d'assistance mutuelle, parce qu'en cas de circonstances extraordinaires, on s'attend à cela des télécommunicateurs. Dans le cas précis, vous avez vu dans le projet de loi C-26, on a été assez précis pour ces pouvoirs, comme je les ai exercés à l'époque et qu'ils puissent être entre les mains du ministre de l'Industrie.

Une chose qui, à mon sens, est un anachronisme, et je n'utilise pas ces mots à la légère, c'est qu'il s'agit d'une des rares lois qui encadre un secteur d'infrastructures essentielles pour lequel l'aspect de la sécurité ne fait pas partie des objectifs. Le projet de loi C-26 corrige cette situation. La sécurité sera au cœur des objectifs, comme on le fait aussi en matière d'énergie dans d'autres secteurs critiques en matière de transport. Je n'étais pas là quand on a adopté la loi. Quand je suis intervenu à l'époque, je vous dirais, monsieur le sénateur, je l'ai fait souvent à titre de puissance douce. À l'époque, le ministre n'avait pas nécessairement le pouvoir de diriger certaines actions de la part des télécommunicateurs. L'histoire nous a montré qu'on ne peut pas se fier uniquement sur la bonne volonté des acteurs. Il faut avoir un pouvoir législatif pour être capable de demander que certaines actions soient prises. Pensez à Internet. Quand on parlera du 5G, quand tout sera connecté, il y aura peut-être des situations extraordinaires où le ministre devra prendre des actions très rapides, ciblées et stratégiques pour protéger l'ensemble du réseau au pays.

Le sénateur Dagenais : Merci beaucoup de votre réponse.

Le sénateur Carignan : Merci, messieurs les ministres, d'être ici.

En regardant le projet de loi C-26, je me posais des questions en lien avec ce que le gouvernement fait pour lui-même, comme les gens qui pratiquent la religion qu'ils enseignent. J'aime beaucoup cela. Cependant, j'ai l'impression que le gouvernement exige plus au privé qu'il ne s'en exige à lui-même.

Je cite entre autres les fuites à l'Agence du revenu du Canada qui ont eu lieu au printemps passé, qu'on vient d'en apprendre l'existence par l'entremise d'un reportage de CBC/Radio-Canada. N'est-ce pas le fait d'induire les gens en erreur que de dire que vous prenez cela au sérieux, alors que des fuites qui touchent quelque 30 000 personnes sont cachées et non divulguées? Les gens qui ont été identifiés comme en étant des victimes n'ont pas été avisées non plus. Si quelqu'un du secteur

agency hide behind systems and prepare communiqués for ministers in cases that become public, but that's it. Isn't there a double standard?

Mr. LeBlanc: Thank you, senator. I will provide some comments and Mr. Champagne can add what he'd like.

I acknowledge that double standards must be avoided at all costs. We need to be able to do what we require of others. I completely agree with your first comment. It's not the first time a government is accused of this type of thing.

However, I'm not a cybersecurity expert, far from it. I take part in information sessions with the Canadian Security Intelligence Service, the RCMP and other government stakeholders. You're right to say that the threats are evolving very rapidly. Governments, whether at the federal, provincial or municipal level, have also been victims of these attacks and threats. I hope it was never implied that we, as governments, are immune. In fact, we have to be very aware of the threats. We have quite effective resources at the Department of National Defence that I am very impressed with, such as the Communications Security Establishment and other organizations that you know well. I saw, in the case of some provincial governments, such as the one for Newfoundland and Labrador, that during a fairly significant attack on its health care system on the Avalon peninsula, in St. John's, where information was stolen, that the federal government was able to help very quickly.

We try to help each other. We should never create obligations that we wouldn't agree to for ourselves. I don't believe it's the case, but I am aware of the ongoing need to invest in technologies, experts and other instruments to protect ourselves, because the threats are real.

And I just did what Mr. Champagne did with your colleague's question: I didn't let him answer. I know this is a big disappointment to you, senator.

Senator Carignan: He's my member of parliament for Champlain.

Mr. LeBlanc: He may have something to add.

Mr. Champagne: Senator, your MP will always be available to answer your questions.

privé faisait cela, il serait contraint de payer des amendes de 10 millions de dollars. Pour sa part, le gouvernement du Canada et son agence du revenu se cachent derrière des systèmes et préparent des communiqués de presse pour les ministres, si cela devient public, mais on en reste là. Ne s'agit-il pas de deux poids, deux mesures?

M. LeBlanc : Merci, sénateur. J'offrirai quelques commentaires et M. Champagne pourra ajouter des éléments s'il le souhaite.

Je reconnais qu'il faut absolument éviter le double standard; il faut que l'on puisse pratiquer la même chose que l'on exige aux autres. Je suis totalement d'accord avec votre premier commentaire. Ce n'est pas la première fois qu'un gouvernement se fait accuser d'une telle chose.

Cependant, je ne suis pas expert en cybersécurité, loin de là. Je participe à des séances d'informations avec le Service canadien du renseignement de sécurité, la GRC et d'autres intervenants du gouvernement. Vous avez raison, la menace évolue très vite. Les gouvernements, que ce soit le gouvernement fédéral ou les gouvernements provinciaux et municipaux, ont eux aussi été victimes de ces attaques et de ces menaces. J'espère qu'on n'a jamais prétendu que, en tant que gouvernement, nous en étions à l'abri, et il faut d'ailleurs être très conscient que cela existe. On a des ressources assez efficaces du ministère de la Défense nationale dont je suis extrêmement impressionné, telles que le Centre de la sécurité des télécommunications Canada et d'autres organismes que vous connaissez bien. J'ai vu des gouvernements provinciaux, comme celui de Terre-Neuve-et-Labrador, où, au moment d'une attaque assez importante contre un système de soins de santé dans la péninsule d'Avalon, à St. John's, des renseignements ont été volés, et le gouvernement fédéral a été en mesure de les aider très rapidement.

On essaie donc de s'entraider. Il ne faudra jamais créer des obligations que nous n'acceptons pas pour nous-mêmes. Je ne crois pas que ce soit le cas, mais je suis conscient du besoin continuel que nous avons d'investir dans des technologies, des experts et d'autres instruments pour nous protéger, parce que la menace est bien présente.

Là, j'ai fait ce que M. Champagne a fait avec la question de votre collègue : je l'ai empêché d'y répondre. Je sais que cela vous déçoit beaucoup, monsieur le sénateur.

Le sénateur Carignan : C'est mon député de Champlain.

M. LeBlanc : Il voudra peut-être ajouter quelque chose.

M. Champagne : Monsieur le sénateur, votre député sera toujours là pour répondre à vos questions.

I understand your frustration and that of Canadians. Of course, we must do better. I think that Bill C-26 does call for cooperation. I can say that we regularly work with operators on telecommunications systems.

What's critically missing today in the Telecommunications Act is that it's not within the purpose of the act to focus on security. It's a bit anachronistic, given what you've just said about attacks on the private sector, provincial, municipal and federal governments. Just imagine the effect of artificial intelligence, quantum computing and the Internet. When it comes to cybersecurity and telecommunications, we're doing right by Canadians by sharing all the information over the networks, and thereby enabling better protection.

[*English*]

Senator Boehm: Thank you, ministers, for being here. As we heard in the last exchange, the nature of the threat is getting more sophisticated. It replicates itself more quickly, it develops, and governments have to catch up.

This is a question for both of you. You have both been involved in not just Five Eyes discussions but also G7 discussions under the current Italian presidency. We are picking up the flame from Italy in January. In 2018, work was done by a cybersecurity working group in the G7 context, and there was work done on infrastructure and shielding infrastructure. I was a little involved in that. So it goes beyond Five Eyes and all our partners, friends and even those who are not as friendly. Here is my question: Do you think that in each of your portfolios, Canada will be in a position to exercise leadership, bring in new ideas and push the agenda forward?

Mr. Champagne: Senator, you did very well. I hope we can replicate your leadership. The Italians, our friends, are expecting a lot from us. They had a successful G7 presidency.

There is already a global-coordination group working on telecom with some G7 countries and beyond. It has to do with two things. One is standards, and as you know, it is key in the international arena to promote standards that will be in line with our values, let me say, in terms of telecom infrastructure. I come back to that in particular. In the 5G world, things will be different. By the way, we've now signed a protocol with the Americans on 6G now. Believe it. We are not just working on 5G. We are already thinking about what 6G will be doing. I will stop there so Minister LeBlanc can follow up on that.

Je comprends votre frustration et celle des Canadiens. C'est sûr qu'on doit faire mieux. Je pense que dans le projet de loi C-26, on prône quand même la collaboration. Je peux dire qu'en ce qui a trait aux systèmes des télécommunications, on travaille régulièrement avec les opérateurs.

Ce qui manque aujourd'hui dans la Loi sur les télécommunications, qui est assez fondamentale, c'est que le fait de promouvoir la sécurité ne fasse pas partie des objectifs de la loi. C'est un peu anachronique, compte tenu de ce que vous venez de dire et de ce qu'on voit des attaques qui touchent le privé et les gouvernements provinciaux, municipaux et fédéral. Imaginez donc quand on arrive avec l'intelligence artificielle, le quantique et Internet. Dans un cadre de cybersécurité, on rend service aux Canadiens et aux Canadiennes en matière de télécommunications en permettant à toute l'information de se transporter sur les réseaux, ce qui permet une meilleure protection.

[*Traduction*]

Le sénateur Boehm : Messieurs les ministres, je vous remercie d'être venus. Comme nous l'avons entendu lors du dernier échange, la nature de la menace est de plus en plus sophistiquée. Elle se multiplie plus rapidement, elle se développe et les gouvernements doivent la rattraper.

Cette question s'adresse à vous deux. Vous avez tous deux participé non seulement aux discussions du Groupe des cinq, mais aussi à celles du G7 sous l'actuelle présidence italienne. Nous reprenons le flambeau de l'Italie en janvier. En 2018, il y a eu un groupe de travail sur la cybersécurité dans le cadre du G7, et des travaux ont été menés sur l'infrastructure et la protection de celle-ci. J'ai y été un peu impliqué. On va donc au-delà du Groupe des cinq et de tous nos partenaires, amis et même ceux qui ne sont pas aussi amicaux. Voici ma question : pensez-vous que dans chacun de vos portefeuilles, le Canada sera en mesure d'exercer un leadership, d'apporter de nouvelles idées et de faire avancer les choses?

M. Champagne : Monsieur le sénateur, vous vous êtes très bien débrouillé. J'espère que nous pourrons reproduire votre leadership. Les Italiens, nos amis, attendent beaucoup de nous. Leur présidence du G7 a été couronnée de succès.

Un groupe de coordination mondiale travaille déjà sur les télécommunications avec certains pays du G7 et d'autres. Il y a deux volets. Le premier concerne les normes et, comme vous le savez, il est essentiel, sur la scène internationale, de promouvoir des normes qui soient conformes à nos valeurs, si je puis dire, pour l'infrastructure de télécommunications. Je reviens sur ce point en particulier. Dans le monde de la 5G, les choses seront différentes. D'ailleurs, nous venons de signer un protocole avec les Américains sur la 6G. Croyez-le. Nous ne travaillons pas seulement sur la 5G. Nous pensons déjà à ce que fera la 6G. Je m'arrêterai là pour que le ministre LeBlanc puisse poursuivre sur ce point.

More important is the supply chain. We have been working with a number of allies. You may have seen Ericsson has made a generational investment, close to a billion dollars, in Kanata. It is the same with the Nokia research centre, one of the largest in the world, here in Kanata, in Ottawa.

I would say we are working on both standards and supply chain because if we want to have reliable and secure vendors and supply chains and equipment, we need to work with our international partners in the Five Eyes and the G7 to make sure we lead in research and development, standards and equipment so we're not beholden to nations who would use our networks to spy on our people, to disrupt or to gather information.

Mr. LeBlanc: Senator Boehm, you are absolutely right. The Five Eyes as a security partnership is very much seized with these issues. I have participated in a handful of Five Eyes meetings where cyber-threats were very much on the agenda.

As you noted and as Minister Champagne said, we have been participating in an active series of ministerial meetings that the Italians organized. I was at one near Naples a few weeks ago where the Italian interior minister, who was there with the new minister from France and all of our G7 colleagues, was talking about how this is a borderless threat. Some regions are more active than others, and you would have seen the intelligence in your previous role, senator. Some particular regions and countries are very active. Others are themselves victims and then house some of these threat actors. I think there has to be a continuation. Certainly, my understanding of the G7 priorities and the public safety area for our presidency would absolutely include a continuation of this work that began with the Italians.

The intelligence services are active, including, as you said, with countries that may not be in the European Union, Five Eyes or G7 — pick your nice bureaucratic name for the group. There are a lot of countries that themselves detect this, and the intelligence sharing is extensive. I'm reassured of that by non-traditional partners.

Senator Gold: Welcome, ministers. It is nice to see you.

I want to ask a question about the powers in the bill that are bestowed on the government and the safeguards that are built in. For example, the government has powers, as you have described, to direct the telecom providers to do certain things or not to do certain things. They also, in some cases, provide that the orders

La chaîne d'approvisionnement est plus importante. Nous avons travaillé avec un certain nombre d'alliés. Vous avez peut-être vu qu'Ericsson a fait un investissement générationnel de près d'un milliard de dollars à Kanata. Il en va de même pour le centre de recherche de Nokia, l'un des plus grands au monde, ici à Kanata, à Ottawa.

Je dirais que nous travaillons à la fois sur les normes et la chaîne d'approvisionnement. En fait, si nous voulons avoir des fournisseurs, des chaînes d'approvisionnement et de l'équipement fiables et sûrs, nous devons travailler avec nos partenaires internationaux du Groupe des cinq et du G7 pour nous assurer d'être chefs de file en matière de recherche et développement, de norme et d'équipements dans le but de ne pas être redevables à des nations qui utiliseraient nos réseaux pour espionner nos citoyens, perturber nos activités ou collecter des informations.

M. LeBlanc : Sénateur Boehm, vous avez tout à fait raison. À titre de partenariat de sécurité, le Groupe des cinq est très sensible à ces questions. J'ai participé à plusieurs réunions du Groupe où les cybermenaces n'étaient pas du tout ignorées de l'ordre du jour.

Comme vous l'avez noté et comme l'a dit le ministre Champagne, nous avons participé à une série active de réunions ministérielles organisées par les Italiens. Il y a quelques semaines, j'ai assisté à une réunion dans la région de Naples où le ministre italien de l'Intérieur, accompagné du nouveau ministre français et de tous nos collègues du G7, a parlé du fait que la menace ne connaît pas de frontières. Certaines régions sont plus actives que d'autres. Dans le cadre de votre rôle précédent, vous auriez pu consulter les renseignements, monsieur le sénateur. Certaines régions et certains pays sont très actifs. D'autres sont eux-mêmes victimes et protègent ensuite certains de ces acteurs de la menace. Je pense qu'il faut poursuivre dans cette voie. Il est certain que ma compréhension des priorités du G7 et du domaine de la sécurité publique pour notre présidence inclurait absolument la poursuite de ce travail qui a commencé avec les Italiens.

Les services de renseignement sont actifs, notamment, comme vous l'avez mentionné, auprès de pays qui ne font peut-être pas partie de l'Union européenne, du Groupe des cinq ou du G7 — choisissez un quelconque joli nom bureaucratique pour décrire le groupe. De nombreux pays détectent eux-mêmes ce phénomène, et les échanges de renseignements sont nombreux. Je suis rassuré par les partenaires non traditionnels.

Le sénateur Gold : Bienvenue, messieurs les ministres. C'est un plaisir de vous recevoir.

Je voudrais poser une question sur les pouvoirs conférés au gouvernement dans le projet de loi et sur les garanties qui y sont intégrées. Par exemple, le gouvernement a le pouvoir, comme vous l'avez décrit, d'ordonner aux fournisseurs de services de télécommunication de faire ou de ne pas faire certaines choses.

to do or not to do should not be disclosed. Could you talk about, in general, the safeguards, limitations and the oversight that would exist? Could the cabinet use these authorities to intercept the communications of political adversaries? Could the RCMP use them for investigative tools? Perish the thought, but I am asking the question. Why would orders not be disclosed, and what safeguards are in place for those?

Mr. LeBlanc: Mr. Chair, thanks to our friend Senator Gold for the question. He is absolutely right. I have learned a lot about this area since becoming the Public Safety Minister. There is an important balance to be struck in terms of the transparency of these measures.

Some of the witnesses on the House committee, some of the private businesses, are, understandably, concerned if some of these orders were made public. The advice that I got, Senator Gold, from the security and intelligence agencies is that by divulging, for example, these orders that the government may issue publicly, you certainly paint a vulnerability landscape for the threat actors. You can point the way for some less sophisticated threat actors: "Oh, this particular group is zeroing in here; maybe we should try that." They are understandably hesitant to make this stuff public.

Minister Champagne can talk about big publicly traded companies. I'm not sure what that does to the investor confidence in a large telecommunications company if they have been subject to four orders and their competitor to zero. Does that speak to their own lack of protection?

The transparency requirement has to be balanced against some of the unintended consequences — the House of Commons committee looked at this a lot — by mandating, for example, the government to be transparent on an annual basis about the number of orders that were issued and by specifically referring to NSICOP or the National Security and Intelligence Review Agency. There is a role for the Federal Court. There are designated judges of the Federal Court, like the ones that would see the CSIS warrants that I might sign. These aren't dragged into an open court process. It would be reckless and dangerous to do so. But there is an appropriate judicial oversight with amicus curiae. There is a process that is well worn and quite effective, but we will be listening to the work of this committee to ensure we have the balance right.

Mr. Champagne: I think you may be thinking about the telecom CEOs watching today, but there was an amendment that was made that, for example, the orders the minister of industry could direct would have to be reasonable. There is a reasonable

Dans certains cas, on prévoit également que les décrets ne doivent pas être divulgués. Pourriez-vous nous parler, d'une manière générale, des garanties, des limites et de la surveillance qui existeraient? Le Cabinet pourrait-il utiliser ces pouvoirs pour intercepter les communications d'adversaires politiques? La GRC pourrait-elle s'en servir comme outils d'enquête? Je n'ose le croire, mais je pose la question. Pourquoi les décrets ne seraient-ils pas divulgués et quelles sont les garanties mises en place à cet égard?

M. LeBlanc : Monsieur le président, je remercie notre ami, le sénateur Gold pour sa question. Il a tout à fait raison. J'ai beaucoup appris dans ce domaine depuis que je suis ministre de la Sécurité publique. Il est important de trouver un équilibre dans la transparence de ces mesures.

Certains témoins au comité de la Chambre, notamment des entreprises privées, sont inquiets à juste titre de ce qui se passerait si ces décrets étaient rendus publics. Le conseil que j'ai reçu, sénateur Gold, de la part des agences de sécurité et de renseignement est qu'en divulguant ces décrets que le gouvernement pourrait donner publiquement, vous peignez certainement un paysage de vulnérabilité pour les acteurs de la menace. Vous pouvez montrer la voie à des acteurs malveillants moins avertis : « Oh, puisque ce groupe s'attarde ici, nous devrions peut-être faire de même. » On peut comprendre qu'ils hésitent à rendre ces informations publiques.

Le ministre Champagne peut parler des grandes entreprises cotées en bourse. Je ne sais pas ce que cela signifie pour la confiance des investisseurs dans une grande entreprise de télécommunications, si elle a fait l'objet de quatre décrets et que son concurrent n'en a aucun. Cette situation témoigne-t-elle du manque de protection de l'entreprise?

L'exigence de transparence doit tenir compte de certaines conséquences involontaires — le comité de la Chambre des communes s'est beaucoup penché sur cette question. On peut par exemple obliger le gouvernement à divulguer chaque année le nombre de décrets émis, et faire spécifiquement référence au Comité des parlementaires sur la sécurité nationale et le renseignement ou à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement. La Cour fédérale a un rôle à jouer. Il y a des juges désignés de la Cour fédérale, comme ceux qui verraient les mandats du SCRS que je pourrais signer. Ces mandats ne sont pas soumis à une procédure judiciaire publique. Il serait imprudent et dangereux de le faire. Mais il existe un contrôle judiciaire approprié avec l'amicus curiae. Il existe une procédure bien rodée et très efficace, mais nous écouterons les travaux de ce comité pour nous assurer que nous avons trouvé le bon équilibre.

M. Champagne : Je pense que vous songez peut-être aux PDG des entreprises de télécommunications qui nous regardent aujourd'hui, mais un amendement a été apporté pour que, par exemple, les ordres que le ministre de l'Industrie pourrait donner

standard. The amendments also talk about the financial impact and the impact on telecommunication services.

Whilst the minister and the Governor-in-Council would have the power, we have put the checks and balances in the system to ensure that we achieve the purpose that this is intended, which is to protect the network, but, at the same time, there would be due consideration to, for example, the due diligence standard. If a company had done everything they could to achieve a particular outcome, they would have a defence. We got the balance right, in my view.

As Minister LeBlanc said, there is a reason why the warrants would go to NSICOP, because, in my view, at least, and the players in the telecom industry, you don't want to bring that to the public eye, because then, as Minister LeBlanc said, we could just attract even more at the particular time we need to put a patch on a breach. If you are going public with that before you have the patch, that would be terrible for the network.

The Chair: Thank you, minister.

Senator Yussuff: Thank you, both ministers, for being here. I have two questions, and they are specific.

First, what has been the consultation with private interests and the telecom companies in trying to understand the legislation that is coming? How are they cooperating and recognizing that they have an important role to play in that regard?

Second, at least three of our national telecom companies have a lot of their work contracted out of the country. This is being processed in other places. We have no control. They are in other countries, and some of them I would identify as countries that are not so amenable. With one of them, we just kicked their diplomats out of our country. How are we going to protect Canadians' data now that it has been processed offshore when we don't have any control over what these telecom companies are subjected to in other places?

Mr. Champagne: We have been working with the telecoms. We have seen more violent and more frequent natural disasters, and when people are facing a tragedy or a threat to their safety, for example, the 9-1-1 network and the telecommunications network become essential. It is true in our daily lives, but it's even more true in cases of emergency.

I would say we have a robust cooperation with them, especially after the Rogers' outages when we put the MOU in place to ensure there would be roaming, mutual assistance and communication with the public. They understood that we needed

soient raisonnables. Il y a une norme de décision raisonnable. Les amendements parlent également de l'impact financier et de l'incidence sur les services de télécommunications.

Bien que le ministre et le gouverneur en conseil aient le pouvoir, nous avons mis en place des freins et des contrepoids dans le système pour garantir que nous atteignions l'objectif visé, qui est de protéger le réseau, tout en tenant dûment compte de la norme de diligence raisonnable. Si une entreprise a fait tout ce qui était en son pouvoir pour obtenir un résultat particulier, elle pourra se défendre. Je pense que nous avons trouvé le bon équilibre.

Comme l'a dit le ministre LeBlanc, il y a une raison pour laquelle les mandats sont transmis au Comité des parlementaires sur la sécurité nationale et le renseignement. À mon avis, du moins, et à celui des joueurs de l'industrie des télécommunications, il ne faut pas rendre l'information publique, car alors, comme l'a dit le ministre LeBlanc, nous pourrions attirer encore plus de menaces au moment où nous avons besoin de colmater la brèche. Si vous rendez l'information publique avant d'avoir le correctif, ce serait terrible pour le réseau.

Le président : Merci, monsieur le ministre.

Le sénateur Yussuff : Merci aux deux ministres de leur présence. J'ai deux questions, et elles sont précises.

Premièrement, quelles consultations ont été menées auprès des intérêts privés et des entreprises de télécommunications pour essayer de comprendre les mesures législatives à venir? Comment collaborent-ils et reconnaissent-ils qu'ils ont un rôle important à jouer à cet égard?

Deuxièmement, au moins trois de nos entreprises nationales de télécommunications sous-traitent une grande partie de leurs activités à l'étranger. Les données sont traitées ailleurs. Nous n'avons aucun contrôle. Les données se trouvent dans d'autres pays, dont certains que je qualifierais de pas très accommodants. Nous venons d'expulser les diplomates de l'un d'entre eux. Comment allons-nous protéger les données des Canadiens maintenant qu'elles sont traitées à l'étranger, alors que nous n'avons aucun contrôle sur ce à quoi sont assujetties ces entreprises de télécommunications dans d'autres pays?

M. Champagne : Nous travaillons avec les entreprises de télécommunications. Les catastrophes naturelles se font plus violentes et plus fréquentes, et lorsque les gens font face à une tragédie ou à une menace pour leur sécurité, par exemple, le réseau 911 et le réseau de télécommunications deviennent essentiels. C'est vrai dans nos vies au quotidien, mais c'est encore plus vrai en cas d'urgence.

Je dirais que nous avons une collaboration solide avec elles, surtout après les pannes de Rogers. Nous avons alors mis en place un protocole d'entente pour garantir l'itinérance, l'assistance mutuelle et la communication avec le public. Elles

to play a role to protect the public interest. Today, that's giving us the tools.

A lot of the things we have done, senator, rely on the goodwill and the advocacy of the government to ensure that we reach the right outcome. But experts would have said that you also need to have the tools in the toolbox, if you need to demand and even force a provider, for example, to do something.

Coming to your example, if there was a network provider using equipment from a country which we know through the Five Eyes and other agencies could compromise the entirety of our network or spy on Canadians or collect information, you would want the minister and the government to have the power to ask that particular operator to cease using that type of equipment. You have seen we have done that with Huawei and ZTE when we issued a directive. Obviously, the law will give us the tools now to implement that. Those are the types of things that you want to see in the toolbox.

Mr. LeBlanc: Mr. Boucher reminded me that there were extensive consultations with many of those private telecommunications companies that you referred to in your question and that Minister Champagne touched on.

Assuming this legislation gets to Royal Assent and we get to the regulatory stage and making regulations under the act, there is also a comprehensive plan to include provinces, territories and private-sector actors. You would want to hear from academic experts and others. And, of course, there is the oversight of the joint committee and so on. We haven't finished the effort to consult. We think it is important in the regulatory phase as well.

Senator Kutcher: Thank you, both, for being with us.

You both mentioned health care systems, and I would like to ask about that. One of the largest data breaches in our history came from LifeLabs, which is a health care data system. Increasingly, we find national telecommunications companies providing direct health care and collecting all that data. We also have the complexity of provincial-based health care systems. Health care is not identified in Schedule 1. Can this bill protect health care data, particularly health care data that is collected by a national telecommunications company? You can see your doctor online from Telus Health, for example. No province runs that system. Have you given any thoughts to how we could better protect Canadians' health care data given this reality?

ont compris que nous devions jouer un rôle pour protéger l'intérêt public. Aujourd'hui, cela nous donne les outils nécessaires pour agir.

Beaucoup de mesures que nous avons mises en place, sénateur, reposent sur la bonne volonté et sur les efforts du gouvernement pour que nous parvenions au bon résultat. Cependant, les experts disaient qu'il faut aussi avoir des outils dans la boîte à outils, si l'on doit exiger d'un fournisseur, par exemple, qu'il fasse quelque chose, ou même le forcer à le faire.

Pour en revenir à votre exemple, si un fournisseur de réseau utilisait du matériel provenant d'un pays dont nous savons, grâce au Groupe des cinq et à d'autres organismes, qu'il pourrait compromettre l'intégralité de notre réseau, ou servir à espionner les Canadiens ou à recueillir des informations, vous voudriez que le ministre et le gouvernement aient le pouvoir de demander à ce fournisseur de cesser d'utiliser ce type de matériel. Vous avez vu que nous l'avons fait dans le cas de Huawei et de ZTE en émettant une directive. La loi nous donnera, bien sûr, les outils nécessaires pour mettre cela en œuvre. C'est le genre d'outils que l'on veut voir dans sa boîte à outils.

M. LeBlanc : M. Boucher m'a rappelé qu'il y a eu des consultations approfondies auprès d'un grand nombre de ces entreprises de télécommunications privées auxquelles vous avez fait référence dans votre question et dont le ministre Champagne a parlé.

En supposant que ce projet de loi reçoive la sanction royale et que nous passions à l'étape de la réglementation et de l'élaboration des règlements d'application de la loi, il existe également un plan global visant à inclure les provinces, les territoires et les acteurs du secteur privé. On voudra aussi entendre le point de vue des experts universitaires et autres. Et, bien sûr, il y a la surveillance exercée par le comité conjoint, etc. La consultation n'est pas terminée. Nous pensons qu'elle est également importante dans la phase de réglementation.

Le sénateur Kutcher : Merci à vous deux d'être avec nous.

Vous avez tous deux mentionné les régimes de soins de santé, et je voudrais vous poser une question à ce sujet. L'une des plus grandes atteintes à la sécurité des données de notre histoire concernait LifeLabs, un système de données sur les soins de santé. Nous avons de plus en plus d'entreprises nationales de télécommunications qui fournissent des soins de santé directs et qui recueillent ainsi une foule de données. Il faut ajouter à cela la complexité des régimes de soins de santé provinciaux. Les soins de santé ne sont pas mentionnés dans l'annexe 1. Ce projet de loi peut-il protéger les données relatives aux soins de santé, en particulier celles qui sont recueillies par une société nationale de télécommunications? Vous pouvez consulter votre médecin en ligne à partir de Telus Santé, par exemple. Aucune province ne gère ce système. Avez-vous réfléchi à la manière dont nous pourrions mieux protéger les données relatives aux soins de santé des Canadiens compte tenu de cette réalité?

Mr. Champagne: That is a very good point, senator, and it is interesting. There are more and more telecoms now are involved in the provision of health care. Again, I hate to come back to this, but we need to think forward 10, 20 or 30 years from now, when you add AI and other technologies. That's all going on the network one way or the other. The day of the fax machine used by doctors is, hopefully, something of the past in the not-too-distant future.

Mr. LeBlanc: Senator Kutcher still faxes prescriptions to people.

Mr. Champagne: There will be a world one day where you would imagine there would be a flow of information that would be different and that would transit through the network. That's why one of our objectives is to protect privacy. That was one of the amendments made at the committee stage, to ensure that the networks make sure that the data they collect — and the power we have — protects privacy.

In terms of designated sector, I will leave that to Minister LeBlanc. You are right. We said the finance sector, energy, transport and telecom. With respect to health care, I may leave Minister LeBlanc to speak to that. I think there is an intersection, and we are both here because all that data transits through a network, even when it's through a fax machine.

It's all about protecting the security and resiliency of the network and ensuring that people don't have access. When everything is connected, you are dependent on the weakest link not interfering in our network. That is why you need new powers to ensure that the weakest link is not compromising the entirety of the system, such that you can shut down part of it, patch it and make sure that we don't compromise the rest of the system.

Mr. LeBlanc: Senator Kutcher, Mr. Boucher reminded me that we're purporting to use the federal legislative power for federally regulated sectors. With health care, I'm thinking of the example in Newfoundland and Labrador that Premier Furey and I worked on, and it was a provincial health authority. As you would know better than anybody, our regulatory ability doesn't touch that. However, you gave the example of telecommunications companies such as Telus Health, whose ads I see all over the place. If we deem that to be a critical piece of the infrastructure — I can't imagine, for the reasons you said, that we wouldn't, but I don't purport to have seen that advice now — they would absolutely fall under our ability to regulate their activities and the protection of the private health care information of the patients they are treating. I can't imagine it wouldn't be part of that. It is an interesting issue you raise, and I will push down on it.

M. Champagne : C'est une très bonne question, sénateur, et elle est intéressante. De plus en plus d'entreprises de télécommunications jouent maintenant un rôle dans la prestation des soins de santé. Encore une fois, je déteste revenir sur ce sujet, mais il faut songer aux 10, 20 ou 30 prochaines années, lorsque l'intelligence artificielle et d'autres technologies seront aussi à considérer. Tout cela passera par le réseau d'une manière ou d'une autre. L'époque des télécopieurs utilisés par les médecins appartiendra, je l'espère, au passé dans un avenir rapproché.

M. LeBlanc : Le sénateur Kutcher envoie encore des ordonnances par télécopieur.

M. Champagne : On vivra un jour dans un monde où l'information circulera d'une façon différente et transitera par les réseaux. C'est pourquoi l'un de nos objectifs est de protéger la vie privée. C'est l'un des amendements déposés en comité, afin de garantir que les réseaux veillent à ce que les données qu'ils recueillent — et les pouvoirs dont nous disposons — protègent la vie privée.

En ce qui concerne les secteurs désignés, je laisserai le soin au ministre LeBlanc de répondre à cette question. Vous avez raison. Nous avons parlé des secteurs financier, de l'énergie, des transports et des télécommunications. En ce qui concerne les soins de santé, je laisserai le ministre LeBlanc en parler. Je pense que ces éléments se rejoignent, et nous sommes tous les deux ici parce que toutes ces données transitent par un réseau, même lorsqu'il s'agit d'un télécopieur.

Il s'agit de protéger la sécurité et la résilience du réseau et de veiller à ce qu'il ne soit pas perméable. Lorsque tout est connecté, il faut que le maillon le plus faible n'interfère pas dans notre réseau. C'est pourquoi il faut se donner de nouveaux pouvoirs pour garantir que le maillon le plus faible ne compromette pas l'ensemble du système, de sorte que l'on puisse en fermer une partie, y apporter des correctifs et s'assurer que le reste du système n'est pas touché.

M. LeBlanc : Sénateur Kutcher, M. Boucher m'a rappelé que nous entendons utiliser le pouvoir législatif fédéral pour les secteurs réglementés par le gouvernement fédéral. Au sujet des soins de santé, je pense au dossier sur lequel le premier ministre Furey et moi avons travaillé à Terre-Neuve-et-Labrador, et il s'agissait d'une autorité sanitaire provinciale. Comme vous le savez mieux que personne, notre capacité de réglementation ne concerne pas ce secteur. Cependant, vous avez donné l'exemple d'entreprises de télécommunications telles que Telus Santé, dont je vois les publicités un peu partout. Si nous jugeons qu'il s'agit d'un élément essentiel de l'infrastructure — et je ne peux imaginer le contraire pour les raisons que vous avez évoquées, mais je ne dis pas avoir vu ce conseil —, nous pourrions assurément réglementer leurs activités et protéger les renseignements privés sur la santé des patients qu'elles traitent. Je ne peux pas imaginer que cela n'en fasse pas partie. Vous

Senator M. Deacon: Thank you for being here today.

I had the opportunity to sit around the table in Europe this summer and have a very similar conversation to this one about what we are doing — mostly Five Eyes, but other countries also — and where we are at. One of the takeaways for me was that we have an opportunity to take this on, and we know it is a huge issue, but we want to get it right. As the minister said, we have to look down the road, around the curve and the other curve as we're doing this.

Could tell me today what we have presently in front of us, looking at the minutes in the House and following the other committee? Are there any pieces through the changes that were made or amendments that were made that you wish were still here? I know you have a bias, but is there anything, from listening to people and different experts, that you would add to make this bill better for the time, knowing where we're trying to go?

Mr. Champagne: Bill C-26 is a game changer when it comes to telecom policy. I go back to my opening statement. The fact that security is not even one of the listed objectives strikes me as a gap we need to fill very quickly, because, obviously, you want the minister of industry, under the Telecommunications Act, to promote security. That is just common sense, like you said. We would be one of the very few nations in the Five Eyes or even the G7 which doesn't even have that as an objective. You want reliability, resiliency and many other things, but in this day and age — above all or equally with other things — you want security of the system.

I'm fine with the checks and balances that were put in there in terms of reasonableness standards and the defence because we want to work with the telecom sector and the providers to reach the best possible outcome. However, the most important thing is for the minister and those who are going to succeed me in 10 or 20 years from now — whether in an emergency, natural disaster or cyberattack, in a world that we can barely foresee now, especially when you add quantum and AI — that person, whoever it may be, would have the authority to direct telcos to do something specific, or someone specific in the network, to prevent a bigger outcome, threat or damage that could occur to the country and to the whole network. I'll stop there.

Particularly when you have the Internet of Things, your question is very pointed when if you think that one day under 5G let alone 6G, everything is interconnected and instant. What I

La sénatrice M. Deacon : Je vous remercie de votre présence aujourd'hui.

J'ai eu l'occasion de participer à des discussions en Europe cet été et d'avoir une conversation très similaire à celle que nous avons aujourd'hui — principalement avec les pays du Groupe des cinq, mais aussi avec d'autres pays — pour faire le point sur la situation. L'une des conclusions que j'en ai tirées est que nous pouvons nous attaquer à ce problème, et nous savons qu'il est de taille, mais nous voulons faire les choses correctement. Comme l'a dit le ministre, nous devons regarder vers l'avenir et penser à ce qui s'en vient, pas seulement demain, mais aussi après-demain.

Compte tenu de ce que nous avons actuellement sous les yeux, de ce qui s'est dit à la Chambre et dans l'autre comité, y a-t-il des éléments qui ont été modifiés ou amendés et dont vous souhaiteriez qu'ils soient encore là? Je sais que vous avez un parti pris, mais y a-t-il quelque chose — après avoir écouté les gens et les différents experts — que vous ajouteriez pour améliorer ce projet de loi en ce moment, en sachant ce que nous voulons atteindre?

M. Champagne : Le projet de loi C-26 change la donne en matière de politique des télécommunications. Je reviens à ma déclaration préliminaire. Le fait que la sécurité ne soit même pas l'un des objectifs énumérés me semble être une lacune que nous devons combler très rapidement, parce que, de toute évidence, on veut que le ministre de l'Industrie, en vertu de la Loi sur les télécommunications, promeuve la sécurité. C'est une question de bon sens, comme vous l'avez dit. Nous serions l'une des rares nations du Groupe des cinq ou même du G7 à ne pas avoir cet objectif. On veut de la fiabilité, de la résilience et bien d'autres choses, mais à notre époque, on veut avant tout, ou tout autant, la sécurité du système.

Je suis satisfait des freins et contrepoids qui sont prévus, les normes de la décision raisonnable et la défense, parce que nous voulons travailler avec le secteur des télécommunications et les fournisseurs pour atteindre le meilleur résultat possible. Toutefois, ce qui importe le plus, c'est que le ministre — et mes successeurs dans 10 ou 20 ans, quels qu'ils soient — puisse ordonner, en cas d'urgence, de catastrophe naturelle ou de cyberattaque, dans un monde que nous pouvons à peine imaginer aujourd'hui, surtout si l'on y ajoute l'informatique quantique et l'intelligence artificielle, qu'il puisse ordonner aux entreprises de télécommunications ou à un intervenant dans le réseau de prendre une mesure précise, pour prévenir une conséquence, une menace ou un dommage plus important qui pourrait toucher le pays et l'ensemble du réseau. Je m'arrêterai là.

Votre question est très pertinente, notamment en ce qui concerne l'Internet des objets, quand on pense qu'un jour, avec la 5G, et a fortiori la 6G, tout sera interconnecté et instantané. Ce

don't have today, but I wish my successor would have, or perhaps if you approve the bill and then we have Royal Assent, is the ability to act swiftly. Time is of the essence. You need to take decisive action. The only way a minister could do it today would be to self-power, and we need to enshrine that in the law. This is a game changer today, and I can live with the checks and balances that are in it.

Senator McNair: Thank you to both ministers and the officials for being here tonight. We appreciate it.

I think this question is properly to Minister Champagne, and it is comprised of two parts. Is there a divergence between the government's stated goal of ensuring reliable access, especially in remote and rural areas of Canada, with the desire to secure our 5G networks, especially given the decision to restrict high-risk suppliers from our telecom service providers?

Secondly, will smaller providers be disproportionately impacted by the decision to ban certain high-risk providers such as Huawei and ZTE, as you discussed earlier?

Mr. Champagne: Thank you, senator, for your role in the bill.

When you are making billions of dollars of investments, you want predictability and certainty. You need these big infrastructure investments. You need to have a vision, going back to Senator Deacon. You need to look at 5, 10, 20 or 30 years down the road. We have always been very forthcoming with the industry about the type of risk we see with certain vendors. You have seen what we did in May 2022 with ZTE and Huawei. This was on the back of what we had seen in other Five Eyes countries, which had determined that this would be detrimental.

I didn't see a push back in the sense that the operators understood that it was in their best interests to transition to something more reliable and that would be permanent in their system. In that sense, I think they saw that coming, and even the directive we had issued has been accepted by the telcos as being the way to do it. It is in our mandate and duty — you as the Senate and we as the government — to make sure that when everything is interconnected, an operator's decision could compromise all the others in the ecosystem. We cannot allow that. Therefore, it was well understood that we needed to take action.

que je n'ai pas aujourd'hui, mais que j'aimerais que mon successeur ait, si vous approuvez le projet de loi et qu'il reçoit la sanction royale, c'est la capacité d'agir rapidement. Le temps presse. Il faut prendre des mesures décisives. La seule façon pour qu'un ministre le fasse aujourd'hui serait de lui accorder ces pouvoirs, et nous devons inscrire cela dans la loi. Cela change la donne aujourd'hui, et je peux m'accommoder des freins et contrepoids que le projet de loi contient.

Le sénateur McNair : Merci aux deux ministres et aux fonctionnaires d'être avec nous ce soir. Nous vous en sommes reconnaissants.

Je pense que le ministre Champagne est le mieux placé pour répondre à ma question, qui comporte deux volets. Existe-t-il une discordance entre l'objectif que s'est donné le gouvernement de garantir à la population un accès fiable aux réseaux, en particulier dans les régions rurales et éloignées du Canada, et la volonté de protéger nos réseaux 5G, compte tenu notamment de la décision consistant à empêcher nos fournisseurs de services de télécommunications de recourir à des fournisseurs présentant un risque élevé?

Deuxièmement, la décision d'exclure certains fournisseurs à haut risque tels que Huawei et ZTE, dont vous avez parlé précédemment, aura-t-elle des répercussions disproportionnées sur les petits exploitants?

M. Champagne : Merci, sénateur, de votre contribution aux travaux sur ce projet de loi.

Lorsque les investissements se chiffrent en milliards de dollars, il faut pouvoir disposer de prévisibilité et de certitude. Nous avons besoin de ces investissements importants dans l'infrastructure. Pour reprendre les propos de la sénatrice Deacon, il faut avoir des objectifs à long terme, c'est-à-dire se projeter dans 5, 10, 20 ou 30 ans. Nous avons toujours communiqué ouvertement à l'industrie le type de risque que nous considérons comme inhérent à certains fournisseurs. Vous avez pu constater que nous avons pris des mesures en mai 2022 à l'égard de ZTE et de Huawei. Cette décision se fondait sur ce que nous avions constaté dans d'autres pays du Groupe des cinq, qui avaient estimé qu'il existait un risque de préjudice.

Je n'ai pas constaté de réactions négatives de la part des exploitants, qui ont compris qu'il était dans leur intérêt de faire la transition vers des éléments plus fiables et intégrés de manière permanente dans leurs réseaux. Je pense que ce changement avait été anticipé, et les entreprises de télécommunications ont elles-mêmes reconnu que la directive émanant du gouvernement constituait la meilleure voie à suivre. Nous avons le mandat et le devoir, tant au Sénat qu'au gouvernement, de veiller à ce que la décision d'un seul exploitant ne puisse pas nuire à tous les autres exploitants qui composent notre écosystème, surtout dans un contexte de grande interconnexion. Nous ne pouvons pas le permettre. C'est pourquoi tous ont compris qu'il fallait agir.

To your point about the smaller operators, there was not much of Huawei and ZTE equipment in the 5G network. It was more in the 4G, for which we left a bit of time to ensure that everyone could replace that equipment safely, proactively and in the best interests of the ecosystem.

In my interactions with the leaders of the telecom companies in the country, they understand we are doing this because we have at heart the best interests of everyone. First and foremost, I would say economic security is national security today. We cannot allow someone to compromise everyone else, and that's why we adopted the directive at the time and we're going to back it by legislation with Bill C-26.

Senator Batters: I have so many questions, but not enough time with both of you.

Minister LeBlanc, Bill C-26 imposes some significant requirements for cybersecurity for small- and medium-sized Canadian businesses without really acknowledging that those requirements could be a lot more onerous for smaller enterprises than for massive organizations.

Today, to follow up on what Senator Carignan was asking about, we saw an alarming news article about a huge cyberattack on a branch of your government, the Canada Revenue Agency, with serious implications for Canadian taxpayers involving millions of dollars. We also see in that report that Minister Bibeau was advised about that major cyberattack on the Canada Revenue Agency many months ago, and she was provided with media lines and messages to respond to any questions, but the article notes, "In the end, the public was never alerted to the scheme." Minister LeBlanc, why didn't your government tell Canadian taxpayers about this? As Public Safety Minister, with the responsibility for cybersecurity, were you also notified about this major cyberattack? If so, why didn't you insist Canadians were told about it?

Mr. LeBlanc: Senator, thank you for the question.

I agree entirely that this legislation can't create an undue burden on small- and medium-sized enterprises. We don't believe that's the case. It is intended to ensure that small businesses and all Canadians, for the reasons that Minister Champagne and others enunciated, can rely on some of these larger providers essential for their business activities. Only federally regulated operators who deliver services in the system, which would be vital to national security or public safety like, to Senator Kutcher's point, health, safety, security and economic

En ce qui concerne les petits exploitants, il n'y avait pas beaucoup de matériel provenant de Huawei et de ZTE dans le réseau 5G. Ce matériel se trouvait plutôt dans le réseau 4G, et pour lequel nous avons accordé un délai supplémentaire afin que le remplacement des éléments visés puisse se faire de manière sûre et proactive tout en veillant à assurer le bon fonctionnement de l'écosystème.

Lors de mes échanges avec les dirigeants des entreprises de télécommunications du pays, ils ont compris que nous agissions dans le but de servir au mieux les intérêts de tous. Avant toute chose, je dirais qu'aujourd'hui, la sécurité économique fait partie de la sécurité nationale. Nous ne pouvons pas permettre à un seul des maillons de la chaîne de mettre en péril tous les autres, c'est pourquoi nous avons adopté cette directive à ce moment et que nous entendons l'inscrire dans la loi par le biais du projet de loi C-26.

La sénatrice Batters : J'ai bien des questions à vous poser, mais pas assez de temps.

Monsieur le ministre LeBlanc, le projet de loi C-26 impose aux petites et moyennes entreprises canadiennes de prendre des mesures importantes en matière de cybersécurité, sans toutefois reconnaître que ces mesures pourraient être beaucoup plus onéreuses pour de petites entreprises que pour de très grandes organisations.

Permettez-moi de rebondir sur une question qu'a posé le sénateur Carignan. Aujourd'hui, nous avons appris dans les médias une nouvelle alarmante. Un organisme dirigé par votre gouvernement, l'Agence du revenu du Canada, a été la cible d'une cyberattaque de grande ampleur qui aura de graves conséquences pour les contribuables et où des millions de dollars sont en cause. Nous apprenons également que la ministre Bibeau avait été informée de cette cyberattaque majeure il y a de cela des mois. On lui a fourni des réponses toutes faites aux questions qui lui seraient posées, mais le public n'a jamais été mis au courant du stratagème employé par les malfaiteurs. Comment se fait-il, monsieur le ministre, que le gouvernement n'en ait rien dit aux contribuables? Vous êtes le ministre de la Sécurité publique et vous êtes responsable de la cybersécurité. Avez-vous été informé de cette grave cyberattaque? Et si oui, pourquoi n'avez-vous pas insisté pour que les Canadiens en soient mis au courant.

M. LeBlanc : Merci, sénatrice, de me poser cette question.

Je suis tout à fait d'accord avec vous. Il importe que ce projet de loi n'accable pas les petites et moyennes entreprises. Nous ne croyons pas qu'il ait de telles conséquences. Le projet de loi vise, pour les raisons énoncées par le ministre Champagne et d'autres, à ce que les petites entreprises et tous nos concitoyens puissent s'appuyer sur les gros fournisseurs, sans qui ces entreprises et les particuliers ne pourraient mener leurs activités commerciales. Seuls les exploitants sous réglementation fédérale, dont les services sont essentiels pour la sécurité

well-being of Canadians, would be captured. I totally agree that we have to be careful not to create that burden on small and medium-sized businesses. We'll be sensitive as the legislation and regulations are adopted that we look at the effects of some of these potential orders and so on, to be conscious of that.

With respect to the breach, I personally was not aware until today of the circumstances that I read about publicly with respect to the Canada Revenue Agency. I'm told that the agency would have, perhaps, talked to officials in our department — obviously, the Centre for Cyber Security, and there is an important element of the Department of National Defence and the Communications Security Establishment, but I'm not aware of the details of how officials at Canada Revenue Agency would have spoken to officials either in our department or at National Defence with respect to this breach.

Separate and apart from the specific circumstances at Revenue Canada that I'm not in a position to talk about, there is a balance. I have seen this with provincial and municipal governments and talked informally with large private sector operators around the transparency of telling their shareholders, their partners — and in the case of public governments, municipalities, provinces and territories their taxpayers — about preserving the confidence that people have in the system or also not giving a road map for the next potential negative or hostile actor to identify a vulnerability until the vulnerability is fixed. I have been in meetings where people say, "This has happened to our province. We're not going to discuss it publicly until we have been able to build a backbone" — that was the phrase I heard — "to ensure that somebody won't come right in behind them," and then I think that particular provincial government talked about it publicly. That's just one circumstance I was in.

Senator Batters: I don't really understand how that applies here, given that the minister had lines ready to give.

Minister LeBlanc, this bill has been a long time in coming. The Trudeau government first held public consultations on it back in 2016. In 2018, your government released a National Cyber Security Strategy, and took it another four years, until 2022, for you to draft and introduce this bill in Parliament. It then two more years to work its way through the House of Commons, which included major amendments at the committee stage which basically overhauled this bill. Even after it passes the Senate, it will take another two years in the regulatory phase before much of the impact of the legislation even comes into effect. Minister, all of this means that this cybersecurity bill will take your government a full decade to bring protections on this critical topic into effect. Why this extreme delay?

publique ou nationale, auraient à se conformer aux nouvelles exigences. Comme l'a indiqué le sénateur Kutcher, je pense aux exploitants qui sont actifs dans les domaines de la santé, de la sécurité et du bien-être économique. Il faut effectivement veiller à ne pas imposer un fardeau aux petites et moyennes entreprises. Je suis tout à fait de votre avis. Nous serons attentifs aux conséquences de la réglementation et des éventuelles ordonnances sur les PME.

Au sujet de la cyberattaque contre l'Agence du revenu, je n'en étais pas au courant. J'en ai eu connaissance aujourd'hui dans les médias. On me dit que l'agence aurait peut-être eu des discussions avec des fonctionnaires de notre ministère, mais je ne suis pas au fait des échanges qu'auraient eus les fonctionnaires de l'agence avec ceux de notre ministère ou celui de la Défense nationale. Le Centre canadien pour la cybersécurité, le ministère de la Défense nationale et le Centre de la sécurité des télécommunications ont évidemment un rôle important à jouer dans ces circonstances.

De façon générale, et mises à part les circonstances à Revenu Canada, dont je ne peux parler, il y a plusieurs choses à prendre en considération dans de telles situations. J'en ai discuté avec des gouvernements provinciaux et municipaux et de façon informelle avec de grandes entreprises du secteur privé. Les gouvernements, qu'ils soient provinciaux, territoriaux ou municipaux, ont des comptes à rendre à leurs contribuables, et les grandes entreprises, à leurs actionnaires et partenaires. Ces entités sont toutefois soucieuses de préserver la confiance du public et de ne pas permettre au prochain acteur hostile d'exploiter une faille dans le système avant qu'elle n'ait été corrigée. J'ai assisté à des réunions où une province déclare avoir été victime d'un incident, mais décide de ne pas l'annoncer au public avant d'avoir pris des mesures correctives, pour éviter d'être de nouveau victime d'un acte malveillant. Je pense que le gouvernement provincial en question en avait ensuite parlé publiquement. C'est une situation parmi d'autres, dont j'ai été témoin.

La sénatrice Batters : Je ne vois pas en quoi ces éléments sont pertinents, étant donné que la ministre avait déjà en main des réponses aux questions des journalistes.

Monsieur le ministre LeBlanc, cela fait longtemps que nous attendons ce projet de loi. Le gouvernement Trudeau a d'abord lancé des consultations publiques en 2016. Deux ans plus tard, en 2018, votre gouvernement a annoncé une stratégie nationale de cybersécurité, puis il a fallu quatre ans de plus pour que vous présentiez ce projet de loi au Parlement, soit en 2022. La Chambre des communes a ensuite eu besoin de deux ans pour examiner ce texte de loi. Des amendements y ont été apportés en comité, ce qui a eu pour effet de changer le projet de loi du tout au tout. Même après son adoption au Sénat, il faudra attendre encore deux ans pour que les règlements soient pris et que la loi entre en vigueur. Monsieur le ministre, au bout du compte, il aura fallu une décennie à votre gouvernement pour instaurer des

The Chair: I am going to ask the minister to reflect on that, because we have gone a minute over. We will go to Senator Dasko now, and if there is time, perhaps you can address that later.

Senator Dasko: Thank you to the ministers for being here today.

I want to get back to the topic of the overall landscape, this being the cybercrime side of the issue. You mentioned, minister, that there are both state and non-state actors. I am interested in who they are. Who are the state actors, and who are the non-state actors? Are the non-state actors mainly foreign actors? I'm talking about the perpetrators, those who are committing these crimes, and their motivation. It sounds like there may be mixed motivations. You mentioned extortion in one example. Is this a main motivation of the perpetrators? Is it information gathering? Is it disruption of our services? There are all kinds of potential motivations.

My second question is about the remedies, this being a crime. It sounds like the remedies are for us to secure our systems, but what about sanctions? Are there sanctions against these perpetrators? Is that viable? How does that work? What are they?

Then, can we repel these actors? I'm thinking of cyber wars — maybe I have seen too many movies — but there is a possibility of repelling them, at least potentially. Those are my questions.

Mr. LeBlanc: Thank you, senator. That is a series of very thoughtful and appropriate questions.

You began by asking us to reflect on hostile state and non-state actors. That's the phrase that we often use or in meetings that I am in that people use. A great deal of this, of course, is classified intelligence or police information if there are ongoing investigations, but it is a well-known, public fact, for example, that Russia is very active in many of these disinformation and potential cyberattacks. There have been public comments around China. But, again, I'm just going with what has been in the public space. I sometimes see briefings where other state actors are quite active.

Many of the threats that would come from nonhostile state actors are organized crime networks operating, again, in some of the countries that themselves perpetrate some of these attacks or countries that may not have extradition treaties. You can think of countries that wouldn't have extradition treaties with the United

mesures de protection dans ce domaine d'une importance critique. Pourquoi ce délai démesuré?

Le président : Sénatrice Batters, votre temps est écoulé depuis déjà une minute. Je vais demander au ministre de réfléchir à la réponse à votre question. Monsieur le ministre, s'il reste du temps, vous pourriez y répondre plus tard. Je vais donner la parole à la sénatrice Dasko.

La sénatrice Dasko : Merci aux ministres d'avoir accepté notre invitation.

Je voudrais vous poser quelques questions sur la cybercriminalité en général. Vous avez parlé, monsieur le ministre, d'acteurs étatiques et non étatiques. J'aimerais savoir qui sont ces acteurs. Les acteurs non étatiques sont-ils surtout étrangers? Je m'intéresse aux auteurs, à ceux qui commettent ces crimes. Qu'est-ce qui les motive à les commettre? On dirait qu'ils ont plus d'un motif à la fois. Vous avez parlé d'extorsion par exemple. Est-ce la principale motivation des auteurs de ces crimes? Cherchent-ils à recueillir de l'information, à perturber nos systèmes? Il y a tout un éventail de motifs, il me semble.

Ma deuxième question porte sur les recours, puisqu'il s'agit de crimes. On dirait que la solution, c'est de protéger nos systèmes, mais qu'en est-il des sanctions? A-t-on imposé des sanctions aux auteurs de ces crimes? Est-ce une solution viable? Comment fonctionnent les sanctions et en quoi consistent-elles?

Et pour finir, peut-on repousser ces acteurs? Je pense aux guerres cybernétiques. Je m'inspire peut-être trop du cinéma, mais il est possible de les repousser, non? Ce sont les questions que je souhaitais vous poser.

M. LeBlanc : Merci, sénatrice. Vos questions sont tout à fait pertinentes et appropriées.

Votre première question portait sur les acteurs hostiles étatiques et non étatiques. Ce sont les expressions que nous entendons couramment et que j'entends dans mes réunions. Je ne peux trop vous en dire toutefois, car bien entendu ces renseignements sont classifiés ou alors ils sont entre les mains de la police si une enquête est en cours. Cela étant dit, il est bien connu du public que la Russie, par exemple, mène des campagnes de désinformation et éventuellement des cyberattaques. La Chine est également mentionnée dans les débats publics sur le sujet. Je vous dis simplement ce qui est connu du public. Je suis parfois informé de situations où d'autres acteurs étatiques sont assez actifs.

Les acteurs hostiles non étatiques, quant à eux, sont souvent des réseaux criminels organisés qui sont actifs dans les pays qui commettent eux-mêmes ces attaques ou dans des pays qui n'ont pas de traité d'extradition avec les États-Unis, le Canada et les pays d'Europe. Il est possible de trouver certains de ces réseaux

States, European countries and Canada. You may find some of these organized criminal networks that do these ransomware attacks or extortions based there.

The threat is evolving all the time. A lot of it increasingly — this has been publicly commented on by the Communications Security Establishment — becomes a source of funding for organized crime. Large transnational criminal networks may have a branch that does this kind of activity from country X, and it can be quite lucrative in what we take as the public reporting of large companies or public sector entities that have paid ransoms. Some are paid that we don't know about and are never reported publicly, for obviously understandable reasons as well. That is the threat landscape, and I think there is more we could say in terms of the countries.

I'll conclude with this: You asked why they would do this. I'm not a criminal profiler, but a lot of these hostile state actors, these countries, do it precisely to shake people's confidence in public institutions — in banking, telecommunications, in your local health authority. They seek to disrupt confidence in large Western democracies. Some of it can be designed by ideologically motivated violent extremists who are also seeking to create a context where they can recruit in certain communities. It is a vast myriad of reasons why. I see it in some of the intelligence reporting some of these elements, but they are as vast as are the attacks.

The Chair: Thank you very much.

Ministers, I'm doing a time check here. It is closing in on 5:00. I'm going to ask if you would have 11 or 12 minutes remaining to cover off four senators who have questions. We'll give them three minutes each, if you are agreeable.

Mr. LeBlanc: Yes, absolutely, but I have a meeting at 5:30 with two of my cabinet colleagues at the Marriott hotel, which has been planned for a number of months. We're meeting a group of Indigenous leaders from the Jay Treaty Border Alliance.

The Chair: We will be quick.

Senator Patterson: Thank you, ministers.

Minister LeBlanc, this is for you. It follows up on Senator Kutcher's question. There is a federal health care system, the Canadian Armed Forces, and they do have an electronic system that must reach into provinces and territories to exchange information. While information has been held in a repository, we already know there was accidental deletion of massive amounts of data. Why does this matter? Because the health of our troops is also a definite cyber target for nefarious actors out there. I

criminels, qui mènent des cyberattaques pour ensuite exiger une rançon, dans des pays dépourvus de traités d'extradition.

La menace évolue constamment et devient de plus en plus souvent — et cela a été dit publiquement par le Centre de la sécurité des télécommunications — une source de financement pour le crime organisé. Les grands réseaux criminels transnationaux peuvent avoir une filiale qui se livre à ce type d'activité à partir d'un pays X, et cela peut s'avérer très lucratif, comme le rapportent les grandes entreprises ou les entités du secteur public qui ont payé des rançons. Certaines rançons sont payées sans que nous le sachions, et ne sont jamais rendues publiques pour des raisons évidemment compréhensibles. Voilà des exemples de menaces, et nous pourrions en dire plus sur les pays.

Je conclurai par ceci : vous avez demandé quelles sont leurs motivations. Je ne suis pas un spécialiste du profilage criminel, mais un grand nombre de ces acteurs étatiques hostiles agissent précisément pour ébranler la confiance des gens dans les institutions publiques, dans les banques, les télécommunications, les autorités sanitaires locales. Ils cherchent à ébranler la confiance dans les grandes démocraties occidentales. Certains de ces actes peuvent être posés par des extrémistes violents qui sont motivés par une idéologie et qui cherchent à créer un contexte leur permettant de recruter dans certaines communautés. Il peut y avoir une multitude de raisons. Je vois certains de ces éléments dans les rapports des services de renseignement, mais ils sont aussi nombreux que les attaques.

Le président : Merci beaucoup.

Messieurs les ministres, je vérifie l'heure. Il est presque 17 heures. Je vais vous demander si vous pouvez rester encore 11 ou 12 minutes pour répondre aux quatre sénateurs qui ont des questions à poser. Nous leur accorderons trois minutes chacun, si vous êtes d'accord.

M. LeBlanc : Oui, bien sûr, mais j'ai une réunion à 17 h 30 avec deux de mes collègues du Cabinet à l'hôtel Marriott, qui est prévue depuis plusieurs mois. Nous rencontrons un groupe de dirigeants autochtones de la Jay Treaty Border Alliance.

Le président : Nous ferons vite.

La sénatrice Patterson : Merci.

J'ai une question pour le ministre LeBlanc. Elle fait suite à la question du sénateur Kutcher. Nous avons un réseau de soins de santé fédéral, c'est-à-dire au sein des Forces armées canadiennes, et il dispose d'un système électronique qui est connecté comme il se doit aux provinces et aux territoires pour échanger des renseignements. Ces données sont conservées dans un répertoire, mais nous savons que des quantités massives de données ont été supprimées accidentellement. Pourquoi est-ce important? Parce

wanted to add that to it. My question is also related to Indigenous Services, which is outside provincial and territorial jurisdictions. When you're looking at vital services and vital systems — the Department of National Defence has an un-classed stake in this as well — how will that be addressed by this bill?

Mr. LeBlanc: Senator, you are right. The RCMP is also provided some medical services, like people who serve in the Armed Forces. Correctional Service Canada has 13,500 federally sentenced inmates who need health care. You're absolutely right. We have a responsibility to protect that data and its reliability for a person offering treatment to those persons and to do so in a way that would not compromise their security in the case of serving members of the Armed Forces or the RCMP. If you will, Mr. Boucher may be able to provide a specific answer in the context of how that operates.

Patrick Boucher, Senior Assistant Deputy Minister, National and Cyber Security Branch, Public Safety Canada: As the minister alluded to earlier, there was extensive engagement with various stakeholders from across the country — provinces, territories, Indigenous organizations and the private sector. That was all to get baseline information on how to define vital systems.

As the minister said earlier on the question of small to medium-sized enterprises, chances are that these vital systems will be held by the major corporations, the big telcos that are out there. There was a methodology applied to start identifying those vital systems, and we will continue to work with industry, with partners, to zero in through the regulatory process to lock those down and, through the regulatory process, to ensure we have the flexibility to update them, because it will evolve. The threat will evolve. New vital systems may be needed to be protected under this act, so the regulatory framework will allow us to do that.

Senator Duncan: I thank the ministers for being here.

The physical threat in the North is twofold. There are threats from climate change and equipment failure, and this occurs more often than we care to count. It was evident this spring when Yukon lost all communications for a period of time. The Government of Yukon has made significant investments in redundancy for the future. Does there exist — I think Mr. Boucher touched on this — a realistic account or analysis of the infrastructure throughout the North, particularly identifying the gaps? One of those threats is the physical critical infrastructure, where it exists, how vulnerable it is and where it doesn't exist. Those are the gaps. The other concern is when the equipment failed, many Yukoners turned to Starlink. Starlink is

que la santé de nos troupes est aussi, assurément, une cybercible pour des acteurs malveillants. Je voulais le mentionner. Ma question porte également sur Services aux Autochtones, dont le champ de compétence se situe en dehors de celui des provinces et des territoires. Comment les services et les réseaux vitaux sont-ils pris en compte dans ce projet de loi? Le ministère de la Défense nationale a également un intérêt particulier dans ce domaine.

M. LeBlanc : Sénatrice, vous avez raison. Les agents de la GRC bénéficient également de certains services médicaux, à l'instar des membres des forces armées. Service correctionnel du Canada fournit des soins de santé à 13 500 détenus sous responsabilité fédérale. Vous avez tout à fait raison. Nous avons la responsabilité de protéger ces données et leur fiabilité pour les fournisseurs de soins et de le faire d'une manière qui ne compromettrait pas leur sécurité dans le cas des membres actifs des forces armées ou de la GRC. Si vous le voulez bien, M. Boucher pourra peut-être apporter des précisions sur le fonctionnement.

Patrick Boucher, sous-ministre adjoint principal, Direction de la sécurité nationale et de la cybersécurité, Sécurité publique Canada : Comme le ministre y a fait allusion plus tôt, des discussions importantes ont été tenues avec diverses parties prenantes de tout le pays — les provinces, les territoires, les organisations autochtones et le secteur privé —, et tout cela pour obtenir des informations de base sur la manière de définir les systèmes vitaux.

Comme le ministre l'a dit plus tôt en réponse à la question sur les petites et moyennes entreprises, il y a de fortes chances que ces systèmes vitaux soient détenus par les grandes entreprises, les grandes sociétés de télécommunications. Une méthodologie a été appliquée pour commencer à recenser ces systèmes vitaux, et nous continuerons à travailler avec l'industrie et avec nos partenaires, dans le cadre du processus réglementaire, pour les inclure et avoir la flexibilité nécessaire pour mettre à jour la liste, parce que la situation évoluera. La menace évoluera. Il se peut que de nouveaux systèmes vitaux doivent être protégés dans cette loi, et le cadre réglementaire nous permettra de le faire.

La sénatrice Duncan : Je remercie les ministres d'être ici.

La menace physique dans le Nord est double. Il y a les menaces liées aux changements climatiques et aux pannes d'équipement, qui se produisent plus souvent qu'on ne le pense. On a pu le constater au printemps dernier lorsque le Yukon a perdu toutes ses communications pendant un certain temps. Le gouvernement du Yukon a fait d'importants investissements dans la redondance pour l'avenir. Existe-t-il — je pense que M. Boucher en a parlé — un rapport ou une analyse réaliste qui porte sur l'infrastructure dans tout le Nord, en particulier pour recenser les lacunes? L'une de ces menaces est l'infrastructure physique essentielle, où elle existe, à quel point elle est vulnérable, et où elle n'existe pas. Ce sont les lacunes. L'autre

evident everywhere. How secure is it? It's used by government agencies. What is its level of security, and how do we intend to address that? Does Bill C-26 address the issue of security in cyberspace communications?

Mr. Champagne: I will try to do justice to your question, but we would need to talk for an hour to go over all of that.

The fact that we will promote security resilience and reliability in the network is key now. I am mindful of the situation you are describing because I was very much involved when Yukoners lost connectivity. You may have seen Telesat's recent investment in low-Earth-orbit satellites to make sure we would be covered. I would say it has much to do with national security and resiliency because, to your point, I don't think we should outsource national security when it comes to the Northwest Passage, aviation for maritime services, law enforcement and others. We are tasked, obviously, to protect the North, but we also have our NATO obligations. I think this was a wise investment that will allow us to support a Canadian company and have the equipment there to help the resiliency of communications in the North. I am happy to have a longer discussion, but I see that the chair would like me to offer only a brief response.

Senator Al Zaibak: Thank you, ministers, for being here, and my apologies for missing the first part of your statements.

Mr. LeBlanc: They were fantastic. Your colleagues were absolutely captured. It was a seminal performance.

Senator Al Zaibak: I am sure.

In my humble view, neither technology alone nor legislative power alone can provide a viable solution to the questions we have and the threats we are facing, especially when it comes to cybersecurity. I believe cybersecurity requires a concerted effort between the federal government and private industry, the stakeholders, as private industry stakeholders often own the telecommunications and IT infrastructure.

Bill C-26 appears to create obligations for the telecommunications providers, yet optimal implementation requires strong public-private partnership. What frameworks or incentives within Bill C-26, in your view, could foster effective collaboration between the federal government and private telecommunications companies to ensure long-term viable cybersecurity solutions?

préoccupation est que, lorsque l'équipement est tombé en panne, de nombreux Yukonnais se sont tournés vers Starlink. Starlink est présent partout. Quel est son niveau de sécurité? Il est utilisé par les organismes gouvernementaux. Quel est son niveau de sécurité et comment entendons-nous aborder cette question? Le projet de loi C-26 aborde-t-il la question de la sécurité des communications dans le cyberespace?

M. Champagne : Je vais essayer de répondre à votre question, mais il nous faudrait une heure pour en faire le tour.

Le fait que nous allons promouvoir la sécurité, la résilience et la fiabilité du réseau est un élément clé aujourd'hui. Je suis conscient de la situation que vous décrivez, car j'ai été très impliqué lorsque les habitants du Yukon ont perdu leur connectivité. Vous avez peut-être vu les récents investissements de Télésat dans des satellites en orbite basse pour garantir la couverture. Je dirais que cela a beaucoup à voir avec la sécurité nationale et la résilience, car, pour répondre à votre question, je ne pense pas que nous devrions externaliser quoi que ce soit qui concerne le passage du Nord-Ouest, l'aviation pour les services maritimes, l'application de la loi, etc. Nous sommes chargés, évidemment, de protéger le Nord, mais nous avons aussi nos obligations envers l'OTAN. Je pense qu'il s'agit d'un investissement judicieux qui nous permettra de soutenir une entreprise canadienne et de disposer de l'équipement nécessaire pour contribuer à la résilience des communications dans le Nord. Je serais heureux de pouvoir en discuter plus longuement, mais je vois que le président souhaite que je sois bref.

Le sénateur Al Zaibak : Je vous remercie, messieurs les ministres, de votre présence et je m'excuse d'avoir manqué la première partie de vos déclarations.

M. LeBlanc : Elles étaient formidables. Vos collègues ont été totalement conquis. C'était une performance très originale.

Le sénateur Al Zaibak : Je n'en doute pas.

À mon humble avis, ni la technologie seule ni le pouvoir législatif seul ne peuvent apporter une solution viable aux questions que nous nous posons et aux menaces auxquelles nous faisons face, en particulier lorsqu'il s'agit de cybersécurité. Je crois que la cybersécurité exige un effort concerté entre le gouvernement fédéral et l'industrie privée, les parties prenantes, car les parties prenantes de l'industrie privée sont souvent propriétaires de l'infrastructure des télécommunications et des technologies de l'information.

Le projet de loi C-26 semble créer des obligations pour les fournisseurs de télécommunications, mais sa mise en œuvre optimale nécessite un partenariat public-privé solide. À votre avis, quels cadres ou incitatifs du projet de loi C-26 pourraient favoriser une collaboration efficace entre le gouvernement fédéral et les entreprises de télécommunications privées, afin de nous assurer d'avoir des solutions viables à long terme en matière de cybersécurité?

Mr. Champagne: Thank you, senator.

One of the objectives is also to provide general security of the telecom network in Canada. There are many ways we can do that. As you said, the powers we have here are to direct certain actions, acts or omissions, by certain actors within the ecosystem.

Senator, I don't know if you arrived after I spoke and after the eloquent introductory comments from the very humble Minister LeBlanc, but I mentioned that we have seen significant investments, for example, in Kanata. One of Nokia's largest research centres is here. Ericsson recently invested here. Both companies invested more than $500 million. To your point, policy will help, and having regulatory power will help, but we need to work hand-in-hand in research and development.

We talk about standards and supply chains with our allies. I don't know if you had arrived by the time I said this, but believe it or not, we signed an understanding to work together with the Americans not on 5G but on 6G, so you see we are already beyond the next technology. The fact that some of that research will be done in Canada is a good example that we want to lead, secure our network and be sure that we have the highest standard when it comes to our telecom network because it will be vital for our security and economic prosperity in the country.

The Chair: Thank you, colleagues.

Sadly, this brings us to the end of our time with the ministers today. We not only had the red card but we also went into overtime, so we thank you for that. Thank you, Minister LeBlanc and Minister Champagne, for taking the time to be with us today. On behalf of our colleagues in the room and the broader Senate, we thank you for the hard work that you do on behalf of us and Canadians every day and most nights and weekends. We appreciate that. It is always good to see you.

Colleagues, officials from Public Safety Canada and Innovation, Science and Economic Development have graciously agreed to stay behind to answer questions until 6:25. They will be joined for the next 75 minutes by officials from Communications Security Establishment Canada, which we've heard a lot about today. We will now continue our question period with officials from Public Safety Canada and Innovation, Science and Economic Development Canada who are joined on this panel by the following representatives from the Communications Security Establishment: Sami Khoury, Government of Canada Senior Official for Cyber Security; Danielle Couillard, Director General, Partnerships and Risk

M. Champagne : Merci, sénateur.

L'un des objectifs est également d'assurer la sécurité générale du réseau des télécommunications au Canada. Il y a plusieurs façons de le faire. Comme vous l'avez dit, les pouvoirs dont nous disposons ici consistent à ordonner à des acteurs au sein de l'écosystème de faire ou de ne pas faire certaines choses.

Sénateur, je ne sais pas si vous êtes arrivé après ma déclaration et après la déclaration éloquente du très humble ministre LeBlanc, mais j'ai mentionné qu'il y a eu des investissements importants, par exemple, à Kanata. L'un des plus grands centres de recherche de Nokia se trouve ici. Ericsson a récemment investi ici. Ces deux entreprises ont investi plus de 500 millions de dollars. Pour répondre à votre question, la politique et les pouvoirs réglementaires seront utiles, mais nous devons travailler main dans la main dans le domaine de la recherche et du développement.

Nous parlons de normes et de chaînes d'approvisionnement avec nos alliés. Je ne sais pas si vous étiez arrivé au moment où je l'ai mentionné, mais croyez-le ou non, nous avons signé un accord pour collaborer avec les Américains non pas sur la 5G mais sur la 6G, alors comme vous le voyez, nous regardons déjà au-delà de la prochaine technologie. Le fait qu'une partie de cette recherche sera effectuée au Canada montre bien que nous voulons prendre les devants, sécuriser notre réseau et nous assurer que nous disposons des normes les plus élevées en matière de réseau des télécommunications, car ce sera vital pour notre sécurité et la prospérité économique du pays.

Le président : Merci, chers collègues.

Malheureusement, cela nous mène à la fin du temps prévu avec les ministres aujourd'hui. Nous avons non seulement reçu un carton rouge, mais nous avons également joué les prolongations, alors nous vous en remercions. Merci, messieurs les ministres, d'avoir pris le temps d'être avec nous aujourd'hui. Au nom de nos collègues présents dans la salle et de l'ensemble du Sénat, nous vous remercions pour le travail que vous accomplissez sans relâche en notre nom et au nom des Canadiens tous les jours et souvent en soirée et les fins de semaine. Nous vous en sommes reconnaissants. C'est toujours un plaisir de vous voir.

Chers collègues, les fonctionnaires de Sécurité publique Canada et d'Innovation, Sciences et Développement économique ont gentiment accepté de rester pour répondre aux questions jusqu'à 18 h 25. Ils seront accompagnés pendant les 75 prochaines minutes par des fonctionnaires du Centre de la sécurité des télécommunications Canada, dont nous avons beaucoup entendu parler aujourd'hui. Nous allons maintenant poursuivre notre période de questions avec les fonctionnaires de Sécurité publique Canada et d'Innovation, Sciences et Développement économique Canada, qui sont accompagnés par les fonctionnaires suivants du Centre de la sécurité des télécommunications : Sami Khoury, agent supérieur pour la

Mitigation at the Canadian Centre for Cybersecurity; and Stephen Bolton, Director General, Strategic Policy. Welcome to you all, and thank you for joining this panel. I understand that our officials will interchange as necessary to be fully responsive to our questions.

[*Translation*]

Senator Dagenais: My question is for Mr. MacSween.

There's talk of concerted action with the Five Eyes. Are there any actions or prohibitions here in Canada that are not in line with those of our allies? If so, can you give us examples and explanations to justify why we are not aligned with our allies, the Five Eyes?

Colin MacSween, Director General, National and Cyber Security Branch, Public Safety Canada: Thank you for your question.

[*English*]

In terms of the prohibitions, currently, absent Bill C-26, when we look at our Five Eyes partners, many of them do have similar regimes in place now, specifically in the U.S., the U.K. and Australia, and I am talking specifically about Part 2 of the bill here. There are similarities and differences in what they do. One of the main similarities is the mandatory reporting requirement that we do see in those three other countries. I would say we are learning a lot from them in terms of how we want to set the threshold for that mandatory reporting. To your point on gaps and prohibitions, absent Bill C-26, the mandatory requirement to report in is not there for the CI sector. That is a big gap for Canada.

Part of the reason we want do that is to ensure we have a full line of sight on all the threats that are coming in. Also, this allows our colleagues at the Canadian Centre for Cyber Security to push out threat-related advice to other impacted CI sectors, and I would note that's not just federally regulated sectors but they can go out to all CI sectors as well. That's certainly one of the gaps we want to address and one of the differences we see in the law in Part 2.

cybersécurité; Daniel Couillard, directeur général, Partenariats et atténuation des risques, Centre canadien pour la cybersécurité, et Stephen Bolton, directeur général, Politique stratégique. Je vous souhaite à tous la bienvenue et vous remercie de vous joindre à nos autres témoins. Je comprends que les fonctionnaires changeront de place au besoin pour répondre à nos questions.

[*Français*]

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

On parle de concertation avec les pays du Groupe des cinq. Est-ce qu'il y a des actions ou des interdictions, ici au Canada, qui ne sont pas en alignées avec les actions de nos alliés? Si oui, pouvez-vous nous donner des exemples et des explications qui justifient que nous ne sommes pas solidaires de nos alliés, soit les pays du Groupe des cinq?

Colin MacSween, directeur général, Direction de la sécurité nationale et de la cybersécurité, Sécurité publique Canada : Merci de votre question.

[*Traduction*]

En ce qui concerne les interdictions, actuellement, en l'absence du projet de loi C-26, lorsque nous regardons nos partenaires des pays du Groupe des cinq, beaucoup d'entre eux ont mis en place des régimes semblables, en particulier aux États-Unis, au Royaume-Uni et en Australie, et je parle ici plus particulièrement de la partie 2 du projet de loi. Ces régimes présentent des ressemblances et des différences. L'une des principales similitudes est l'exigence de déclaration obligatoire que l'on retrouve dans ces trois autres pays. Je dirais que nous apprenons beaucoup de ces pays en ce qui concerne la manière dont nous voulons fixer le seuil de la déclaration obligatoire. En ce qui concerne les lacunes et les interdictions, en l'absence du projet de loi C-26, l'obligation de déclaration n'existe pas pour le secteur des infrastructures essentielles. C'est une grosse lacune pour le Canada.

La raison pour laquelle nous voulons agir, c'est en partie pour nous assurer que nous avons une vue d'ensemble de toutes les menaces qui nous parviennent. En outre, cela permet à nos collègues du Centre canadien de cybersécurité d'envoyer des conseils sur les menaces à d'autres secteurs des infrastructures essentielles touchés, et je précise qu'il ne s'agit pas seulement des secteurs sous réglementation fédérale, mais aussi de tous les secteurs des infrastructures essentielles. C'est certainement l'une des lacunes que nous voulons combler et l'une des différences que nous voyons dans la partie 2 du projet de loi.

[*Translation*]

Senator Dagenais: Some of the provisions of Bill C-26 that were passed may have retroactive effects on threats to Canada. Can you give us examples of provisions in Bill C-26 that were adopted and would have retroactive effects?

[*English*]

Mr. MacSween: Retroactive effect, I think that's a bit more related to Part 1 of the bill. With Part 2, upon Royal Assent, nothing immediately switches on right away. In order to build out the requirements, we have to go through the regulatory process, and only then would the designated operators that be will be identified as part of that process become subject to the requirements of the act. There is no retroactive action in Part 2.

I don't know if Mr. Arbour wants to mention anything about Part 1.

[*Translation*]

Andre Arbour, Director General, Strategy and Innovation Policy Sector, Innovation, Science and Economic Development Canada: Thank you.

To clarify, the policy announced by the government in 2022 is entirely voluntary. It's an agreement that sets out intentions with respect to Huawei and ZTE equipment, but it's voluntary. Under the bill, we'd be consulting once again on the order in question. So it's not retroactive, it's forward-looking in terms of the application of the act specifically.

Senator Dagenais: Thank you.

Senator Carignan: I'd like some clarification on the scope of the act and the minister's powers. My question concerns GPS or geo-referenced data, like what you'd find in my Garmin watch, my self-driving car, the self-driving taxis we're increasingly seeing in the U.S. and information held by location-based systems like Google Maps.

Under Bill C-26, would the minister have the power to intervene if someone were to use this data for interference purposes, to threaten or spy on or even take control of autonomous cars? It may seem like science fiction, but it's not far off. What powers would the minister have?

Mr. Arbour: Thanks for the question.

[*Français*]

Le sénateur Dagenais : On parle de certaines dispositions du projet de loi C-26 qui ont été adoptées et qui peuvent avoir un effet rétroactif sur certaines actions qui menacent le Canada. Pouvez-vous nous donner des exemples de dispositions du projet de loi C-26 qui ont été adoptées et qui auraient un effet rétroactif?

[*Traduction*]

M. MacSween : Je pense que l'effet rétroactif est un peu plus lié à la partie 1 du projet de loi. Avec la partie 2, après la sanction royale, rien ne s'enclenche immédiatement. Afin d'établir les exigences, nous devons passer par le processus réglementaire, et ce n'est qu'alors que les exploitants désignés qui seront recensés dans le cadre de ce processus deviendront assujettis aux exigences de la loi. La partie 2 ne prévoit pas d'action rétroactive.

M. Arbour pourrait souhaiter dire quelque chose au sujet de la partie 1.

[*Français*]

Andre Arbour, directeur général, Secteur des stratégies et politiques d'innovation, Innovation, Sciences et Développement économique Canada : Merci.

Pour tirer les choses au clair, la politique annoncée par le gouvernement en 2022 est entièrement volontaire. C'est une entente qui explique certaines intentions en ce qui concerne l'équipement de Huawei et de ZTE, mais c'est volontaire. Sous les autorités du projet de loi, on va consulter encore une fois pour le décret en question. Ce n'est donc pas rétroactif, c'est plutôt pour l'avenir en ce qui concerne l'application de la loi spécifiquement.

Le sénateur Dagenais : Merci.

Le sénateur Carignan : J'aimerais avoir plus de précisions sur l'étendue de la loi et des pouvoirs du ministre. Ma question concerne les données GPS ou géoréférencées, tout comme en contiennent ma montre Garmin, ma voiture autonome, le taxi autonome qu'on voit de plus en plus aux États-Unis et les informations détenues par les systèmes de localisation comme Google Maps.

En vertu du projet de loi C-26, est-ce que le ministre aurait un certain pouvoir d'intervention si quelqu'un utilise ces données à des fins d'ingérence, de menace ou d'espionnage ou même de contrôle, s'il décidait de prendre le contrôle de voitures autonomes? Cela relève un peu de la science-fiction, mais on s'en approche. Quels seraient alors ses pouvoirs?

M. Arbour : Merci pour la question.

The bill deals with matters under federal jurisdiction. In the context of telecommunications, for example, if it has to do with the supply of telecommunications services, that could include GPS data, but if there's a link with —

Senator Carignan: There's no link to the cellular antenna; I mean satellites, for instance.

Mr. Arbour: Satellite communications could be included in telecommunications, but it depends on the circumstances. This technology exists in several sectors — health care and energy, for example — but the scope of the bill concerns sectors under federal jurisdiction, i.e., telecommunications, finance, energy and transport.

So, it depends on the circumstances. If part of the sector, service or activity in question is under federal jurisdiction, like Bell Canada, a telecommunications service, then it may be possible to take action. However, if it's under provincial jurisdiction, like, for example —

Senator Carignan: Let me be more specific. If we're talking about autonomous cars or taxis, which we're increasingly seeing in the United States, and there's a risk the vehicle could be controlled remotely, does the minister have the power to act?

Mr. Arbour: If the vehicle in question is operating within a federal area of jurisdiction, it's possible —

Senator Carignan: So, the minister can intervene if the taxi is used for interprovincial transportation or travel between Ottawa and Gatineau, but not if it's strictly in Montreal, say? Is that what you're saying?

Mr. Arbour: As for jurisdiction over regulations in the transportation sector, certain things can be done. This is because transportation falls under the jurisdiction mentioned in part 2. Again, it depends on the circumstances.

Other tools are also available to the government, for example if it's an economic measure that has a similar effect on tax security issues, for example, or control over access to certain vehicles in Canada.

I would also add that this is an open question for the current government, the option to take all necessary measures for autonomous or electronic vehicles. The government has stressed the importance of this issue.

Le projet de loi touche ce qui est de compétence fédérale. Dans le contexte des télécommunications, par exemple, s'il y a un lien avec l'approvisionnement des services de télécommunications, cela pourrait comprendre les questions de données de GPS, mais s'il y a un lien avec —

Le sénateur Carignan : Il n'y a pas de lien avec l'antenne cellulaire; je parle plutôt d'un satellite, par exemple.

M. Arbour : La communication par satellite pourrait faire partie des télécommunications, mais cela dépend des circonstances. La technologie existe dans plusieurs secteurs — la santé et l'énergie, par exemple —, mais l'envergure du projet de loi porte sur les secteurs de compétence fédérale, soit les télécommunications, les finances, l'énergie et les transports.

Cela dépend donc de circonstances précises. S'il y a un lien dans un contexte de compétence fédérale quant au secteur, au service ou à l'activité en question, par exemple Bell Canada, qui est un service de télécommunications, il y a alors la possibilité d'intervenir. Toutefois, si on est dans un contexte de compétence provinciale, telle que, par exemple...

Le sénateur Carignan : Je vais être plus précis. Si on parle de voiture ou de taxi autonomes, comme on le voit de plus en plus aux États-Unis, et d'un risque de menace de prise de contrôle externe du véhicule, est-ce que le ministre a un pouvoir?

M. Arbour : Si le véhicule en question existe dans un contexte d'un secteur fédéral, il y a la possibilité de...

Le sénateur Carignan : Donc, le ministre a un pouvoir si le taxi fait du transport interprovincial ou s'il se promène entre Ottawa et Gatineau, mais s'il reste sur le territoire de Montréal, il n'en a pas? C'est ce que vous me dites?

M. Arbour : En ce qui concerne les compétences de la réglementation du secteur des transports, il existe certaines possibilités, ce dernier faisant partie de la compétence mentionnée à la partie 2. Cela dépend encore une fois des circonstances.

D'autres outils sont également à la disposition du gouvernement, par exemple si c'est une mesure économique, et cela a un impact semblable en ce qui concerne les questions de sécurité pour les impôts, par exemple, et le contrôle de la disponibilité de certains véhicules au sein du Canada.

J'ajouterais également qu'il s'agit d'une question ouverte pour le gouvernement actuel, soit la possibilité de prendre toutes les mesures nécessaires concernant les véhicules autonomes ou électroniques, et le gouvernement a souligné l'importance de cet enjeu.

[*English*]

Senator Yussuff: I asked a question previously to the two ministers and I did not get an answer, so I will repeat myself and hope to get an answer this time.

Many of the telecom companies in our country are currently subcontracting work out to subcontractors abroad. They are collecting our data and processing that data in other countries, and yet, here we are having a debate and discussion about a bill that will protect our cybersecurity. Can you assure me that this bill will protect that data that Canadians entrust in those telecom communities? We have no control over it. Somebody can call me from India, Egypt or anywhere in the world, and they are collecting that information, and yet we have no control over what the telecom companies are doing and how that data could be compromised if it is now in another country.

Mr. Arbour: Thank you for the question.

Starting with existing measures, there are privacy requirements under PIPEDA that are conditional on the consent of the user, as well as voluntary measures that my department has for engaging with telecommunications providers in terms of the protection of their networks. I appreciate the perspective that that it is insufficient. Indeed, that is one of the reasons why this bill is so important.

Part 1 does allow for a pretty broad set of considerations. It is for protecting the security of the telecommunications system writ large, from the full set of threats. It is not just an individual cyberattack, but it would include a full set of other risks. There is scope there to take regulatory action to protect those networks and services against those risks.

Senator Yussuff: Let me follow up with that. What Canadians are entrusting with their telecom provider — whoever that might be right now — is the responsibility that they are protecting their data. There is nothing you are telling me that makes me assured that it is going to be any better under this legislation, because if they continue to subcontract that work outside of the country to a foreign entity, we have no control. If that was breached in another country, you tell me, "Sorry, we don't have any control over what happened in Egypt or India, but we're here to tell you we're going to protect you under this piece of legislation." We can't do that under the current law, so how do we do it in the future under this bill?

[*Traduction*]

Le sénateur Yussuff : J'ai déjà posé la question aux deux ministres et je n'ai pas obtenu de réponse, je vais donc me répéter et j'espère obtenir une réponse cette fois-ci.

De nombreuses entreprises de télécommunications de notre pays sous-traitent actuellement des activités à des sous-traitants à l'étranger. Elles recueillent nos données et les traitent dans d'autres pays, et pourtant, nous sommes en train de débattre et de discuter d'un projet de loi qui protégera notre cybersécurité. Pouvez-vous m'assurer que ce projet de loi protégera les données que les Canadiens confient à ces entreprises de télécommunications ? Nous n'avons aucun contrôle sur ces données. On peut m'appeler de l'Inde, de l'Égypte ou de n'importe où dans le monde, et on recueille ces informations, mais nous n'avons aucun contrôle sur ce que font les entreprises de télécommunications et sur la façon dont ces données pourraient être compromises si elles se trouvaient maintenant dans un autre pays.

M. Arbour : Merci de la question.

En commençant par les mesures existantes, il existe des exigences en matière de protection de la vie privée en vertu de la Loi sur la protection des renseignements personnels et les documents électroniques qui sont conditionnelles au consentement de l'utilisateur, ainsi que des mesures volontaires que mon ministère a mises en place pour mobiliser les fournisseurs de télécommunications en ce qui concerne la protection de leurs réseaux. Je comprends que ces mesures puissent être considérées comme insuffisantes. C'est d'ailleurs l'une des raisons pour lesquelles ce projet de loi est si important.

La partie 1 prévoit un ensemble assez large de considérations. Il s'agit de protéger la sécurité du système des télécommunications dans son ensemble, contre toutes les menaces. On ne parle pas seulement d'une cyberattaque individuelle, mais d'un ensemble de risques. Il existe une marge de manœuvre pour prendre des mesures réglementaires afin de protéger ces réseaux et ces services contre ces risques.

Le sénateur Yussuff : Permettez-moi de poursuivre. Ce que les Canadiens confient à leurs fournisseurs de télécommunications — quels qu'ils soient actuellement —, c'est la responsabilité de protéger leurs données. Rien de ce que vous me dites ne m'assure que la situation sera meilleure avec ce projet de loi, car s'ils continuent à sous-traiter ces activités à l'extérieur du pays à une entité étrangère, nous n'avons aucun contrôle. En cas de violation dans un autre pays, vous me dites : « désolé, nous n'avons aucun contrôle sur ce qui s'est passé en Égypte ou en Inde, mais nous sommes ici pour vous dire que nous allons vous protéger grâce à ce projet de loi ». Nous ne pouvons pas le faire dans le cadre de la loi actuelle, alors comment ce projet de loi nous permettra-t-il de le faire à l'avenir?

Mr. Arbour: To clarify, currently, we don't have a legal authority to take action, which is part of the point of the bill.

Senator Yussuff: Is that not what most Canadians are wondering about, what is allowed right now? Here we are talking about cybersecurity for some of the most important entities that we trust, our telecom companies, and we have no control right now to even say, "Excuse me, you are compromising something that is so fundamental to our national security."

Mr. Arbour: There has been good action that has been taken basically through moral suasion and leaning on the companies, as well as through other measures such as the way that the government engages with the telecom operators.

To circle back to what this bill can and cannot do, the point is to have a framework that allows for the government to take action against a set of threats. It doesn't spell out in detail the specific issue that you are raising because it is intended to be technologically neutral and flexible to respond to the set of threats that do arise and to have an effective toolbox to be able to respond to those risks. It does include a set of powers to allow for the monitoring of the behaviour of the telecom operators, to compel the provision of information based on their activities in terms of how they are securing their network and how they are protecting in the data of their customers, and then measures to raise the bar in terms of what rules and behaviours they would need to put in place to better protect that. It is about ensuring that we have the tools to be able to take action against risks that could include this and the broad range of risks that we know about now or could appear in the future.

Senator Gold: Thank you for being with us.

I want to ask you to comment in greater detail on a question that I put to the two ministers. Given the increased powers, which we need to protect ourselves, comes a requirement that the right balance needs to be struck.

Could you give us a little more detail on the safeguards, limitations and oversight that is built into this act? If there are other acts that complement that, please feel free to provide that larger context.

[*Translation*]

Mr. MacSween: Thank you for the question.

M. Arbour : Pour préciser, actuellement, nous n'avons pas d'autorité légale pour agir, ce qui fait partie de l'objet du projet de loi.

Le sénateur Yussuff : N'est-ce pas ce qui inquiète la plupart des Canadiens, soit ce qui est autorisé à l'heure actuelle ? Nous parlons de la cybersécurité de certaines des entités les plus importantes auxquelles nous faisons confiance, nos entreprises de télécommunications, et nous n'avons aucun contrôle actuellement pour même leur dire : « pardon, mais vous compromettez un élément fondamental pour assurer notre sécurité nationale ».

M. Arbour : De bonnes mesures ont été prises, essentiellement par la persuasion morale et la pression exercée sur les entreprises, ainsi que par d'autres moyens, comme la façon dont le gouvernement collabore avec les fournisseurs de services de télécommunications.

Pour en revenir à ce que le projet de loi peut et ne peut pas faire, il s'agit d'instaurer un cadre qui permet au gouvernement de prendre des mesures contre un ensemble de menaces. Le projet de loi ne décrit pas en détail la question précise que vous soulevez parce qu'il se veut technologiquement neutre et souple pour contrer l'ensemble des menaces qui se présentent et pour offrir une boîte à outils efficace qui nous permet de réagir à ces risques. Il prévoit un ensemble de pouvoirs visant à surveiller le comportement des fournisseurs de services de télécommunications et à les obliger à fournir des renseignements sur leurs activités pour montrer comment ils sécurisent leur réseau et protègent les données de leurs clients. Le projet de loi prévoit également des mesures destinées à relever la barre en ce qui concerne les règles et les comportements que les exploitants devraient adopter pour mieux protéger ces données. Il s'agit de faire en sorte que nous disposions des outils nécessaires pour prendre des mesures contre les risques, au nombre desquels pourraient figurer cette menace et la vaste gamme de risques que nous connaissons aujourd'hui ou qui pourraient survenir à l'avenir.

Le sénateur Gold : Je vous remercie d'être des nôtres.

J'aimerais vous demander de commenter plus en détail une question que j'ai posée aux deux ministres. Compte tenu des pouvoirs accrus, dont nous avons besoin pour nous protéger, il faut trouver un juste équilibre.

Pourriez-vous nous donner un peu plus de détails sur les garanties, les limites et les mécanismes de surveillance qui ont été intégrés au projet de loi? S'il existe d'autres mesures législatives complémentaires, n'hésitez pas à nous en parler afin d'élargir le contexte.

[*Français*]

M. MacSween : Merci pour la question.

[*English*]

In terms of the safeguards, I'm focusing on Part 2 here, but some of these apply to Part 1, and the ministers mentioned this. As it relates to privacy, one of the specific provisions that was built into the act was an explicit reference to the Privacy Act to reassure Canadians that the Privacy Act does apply to the collection and use of their personal information. Bill C-26 also provides no new authorities or powers to organizations like our friends at the Communications Security Establishment. They will still be subject to the existing privacy protection requirements in their act. That's one piece there.

What was built in as well — and I think the ministers alluded to this — was related to the exercise of their order-making power and to ensure some transparency around that. In Part 2, the Minister of Public Safety will be required to advise the NSICOP or NSIRA, our international security review bodies, of the issuance of cybersecurity directions. This was a deliberate amendment made to ensure that the review body itself would have the authority to review those, but I think the intention there was to ensure that the review body was aware it happened and had the opportunity to look into it if they so desired. They have their own discretion as to what they will seek to review.

Obviously, for any of the provisions in the act, there is recourse to the Federal Court, and this absolutely applies to the issuance of, in the case of Part 2, cybersecurity directions, as well as the administrative monetary penalty regime or the summary offences as well. So there is judicial oversight of the bill as well.

The other aspect that was built in, and I think this was included in both parts of the act, and again, this is more around the transparency aspect, but to ensure everybody is aware of the administration of the law, the ministers will be required to table a report in Parliament. There is a non-exhaustive list included in the legislation of all the information that is to be included in that report. That is another measure to make sure that there is sufficient transparency and oversight of the bill.

Mr. Arbour: To build on that, I think there are different stages of consideration in terms of the overall framing of what is in scope and what is not. For example, the policy objective is to protect the telecommunications system in the case of telecommunications, not to advance national security writ large. That is not to say that there aren't important national security or law enforcement objectives, but that's not what is within scope.

[*Traduction*]

En ce qui a trait aux garanties, je vais m'attarder à la partie 2, mais certaines d'entre elles s'appliquent à la partie 1, comme les ministres l'ont mentionné. Pour ce qui est de la protection de la vie privée, l'une des dispositions précises qui ont été intégrées au projet de loi constitue le renvoi explicite à la Loi sur la protection des renseignements personnels afin de rassurer les Canadiens sur le fait que la Loi sur la protection des renseignements personnels s'applique à la collecte et à l'utilisation de leurs renseignements personnels. De plus, le projet de loi C-26 n'accorde pas de nouveaux pouvoirs à des organismes comme nos amis du Centre de la sécurité des télécommunications. Ceux-ci seront toujours assujettis aux exigences actuelles en matière de protection de la vie privée prévues dans leur loi. Voilà le premier point.

Les autres dispositions qui ont été intégrées — et je pense que les ministres y ont fait allusion — portaient sur l'exercice de leur pouvoir d'ordonnance et la nécessité de garantir une certaine transparence à cet égard. Aux termes de la partie 2, le ministre de la Sécurité publique sera tenu d'aviser le CPSNR ou l'OSSNR — nos organismes de surveillance de la sécurité internationale — de la publication de directives en matière de cybersécurité. On a apporté cet amendement de façon délibérée pour faire en sorte que l'organisme de surveillance lui-même ait le pouvoir d'examiner ces directives, mais je pense que l'intention était de veiller à ce que l'organisme de surveillance soit au courant de ce qui se passe et puisse se pencher là-dessus s'il le souhaite. L'organisme de surveillance a toute la latitude voulue pour déterminer l'objet de ses examens.

Évidemment, toutes les dispositions du projet de loi prévoient un recours à la Cour fédérale, et cela s'applique absolument, dans le cas de la partie 2, à la publication de directives en matière de cybersécurité, ainsi qu'au régime de sanctions administratives pécuniaires ou aux infractions sommaires. Le projet de loi fait donc l'objet d'un contrôle judiciaire.

Il y a un autre aspect qui a été intégré — et je pense que c'est prévu dans les deux parties du projet de loi — et, encore une fois, cela rejoint la question de la transparence, mais pour s'assurer que tout le monde est au courant de l'administration de la loi, les ministres seront tenus de déposer un rapport au Parlement. Le projet de loi dresse une liste non exhaustive de tous les renseignements qui doivent figurer dans ce rapport. Il s'agit là d'une autre mesure visant à garantir une transparence et un contrôle suffisants du projet de loi.

M. Arbour : Pour poursuivre sur cette lancée, je pense qu'il y a différentes étapes à prendre en considération pour déterminer ce qui est visé et ce qui ne l'est pas. Par exemple, l'objectif stratégique est de protéger, en l'occurrence, le système de télécommunications, et non de faire progresser la sécurité nationale dans son ensemble. Cela ne veut pas dire qu'il n'y a pas d'importants objectifs en matière de sécurité nationale ou

If it is not about protecting our network infrastructure — it has nothing to do with the RCMP cracking down on organized crime or anything like that. That's out of scope.

There are provisions that were added to help provide further comfort. They include the reasonableness test so that the orders must be reasonably linked to that objective. That was a requirement already established by the Supreme Court, but it is spelled out clearly in the legislation now. There are provisions added given the concerns about having further comfort around privacy. For instance, personal information and de-identified information are defined in that section. There is the reference to the Privacy Act. There is a "for greater certainty" note order in the telecommunications section which can be used to intercept personal communications. We couldn't do that as it was drafted on tabling, but it is for extra certainty there.

To the question about the confidential orders, generally speaking, when we are regulating the telecom sector, we want everyone to know the rules of the road. We have a public consultation — we are required to — and that still exists with the bill in general. The minister spoke to a few specific examples, such as if there is a specific vulnerability in an individual operator such that publishing that would advertise to the world where to attack, that does allow for a confidential order in those exceptional circumstances. To help ensure that in those narrow circumstances it would not be used inappropriately, there are the additional oversight mechanisms, in particular, notification to NSIRA and NSICOP.

Senator Batters: First of all, to officials from the Communications Security Establishment, CSE, civil liberties organizations have expressed some major concerns about the lack of accountability in Bill C-26, even though the bill was amended to now include notification of NSICOP and NSIRA in the event of confidential orders. An updated brief from the Canadian Civil Liberties Association specifically highlighted CSE's repeated refusal in the past to comply with NSIRA directives, stating:

> As presently drafted, C-26 risks continuing a situation where the CSE interprets its mandates now supercharged with even more Canadians' personal information in manners that have been found noncompliant with the Privacy Act by their reviewer. The Senate has a role and obligation to prevent such a mishandling of Canadians' often most sensitive information, especially given the CSE's long track record of failing to cooperate with its review agencies.

d'application de la loi, mais cela n'entre pas dans la portée du projet de loi. S'il ne s'agit pas de protéger l'infrastructure de notre réseau... cela n'a rien à voir avec la lutte de la GRC contre le crime organisé ou n'importe quoi de ce genre. Ces questions dépassent la portée du projet de loi.

Certaines dispositions ont été ajoutées pour plus de certitude. Elles concernent notamment le critère du caractère raisonnable, de sorte que les décrets doivent être raisonnablement liés à cet objectif. C'est une exigence déjà établie par la Cour suprême, mais elle est maintenant clairement énoncée dans le projet de loi. Des dispositions ont également été ajoutées en raison des préoccupations relatives à la protection de la vie privée. Par exemple, les renseignements personnels et les renseignements dépersonnalisés sont définis dans cet article. Il y a un renvoi à la Loi sur la protection des renseignements personnels. L'article sur les télécommunications contient une « précision » qui peut être invoquée pour l'interception de communications privées. Nous ne pouvions pas le faire aux termes de la version préliminaire, mais cet ajout offre une certitude supplémentaire.

Pour répondre à la question sur les décrets confidentiels, de façon générale, lorsque nous réglementons le secteur des télécommunications, nous voulons que tout le monde connaisse les règles du jeu. Nous organisons une consultation publique — nous y sommes tenus —, et cette obligation demeure inchangée dans le projet de loi en général. Le ministre a donné quelques exemples précis, comme dans le cas d'un exploitant qui présente une vulnérabilité particulière, si bien que la publication de cette information l'exposerait à des attaques. Les décrets confidentiels sont donc justifiés dans de telles circonstances exceptionnelles. Pour éviter qu'ils soient utilisés à mauvais escient dans ces circonstances précises, il existe des mécanismes de surveillance supplémentaires, en particulier les avis adressés à l'OSSNR et au CPSNR.

La sénatrice Batters : Je voudrais d'abord m'adresser aux représentants du Centre de la sécurité des télécommunications, ou CST. Les organismes de défense des libertés civiles ont exprimé de vives inquiétudes quant à l'absence de responsabilité dans le projet de loi C-26, même s'il a été amendé pour que l'OSSNR et le CPSNR soient désormais avisés lorsqu'un décret confidentiel est pris. Un mémoire mis à jour de l'Association canadienne des libertés civiles souligne en particulier que le CST a refusé à maintes reprises par le passé de se conformer aux directives de l'OSSNR. En voici un extrait :

> Dans son libellé actuel, le projet de loi C-26 risque de perpétuer une situation où le Centre de la sécurité des télécommunications interprète ses mandats — maintenant surchargés de renseignements personnels sur un nombre encore plus grand de Canadiens — d'une manière qui a été jugée non conforme à la Loi sur la protection des renseignements personnels par ses organismes de surveillance.

Could you please tell me how you would respond to those serious concerns?

Sami Khoury, Senior Official for Cyber Security, Communications Security Establishment Canada: Thank you for the question.

We take the role of the review body very seriously, and we cooperate with them in all of their reviews.

In the context of Bill C-26, the information that we will be receiving from the designated operators is meant to be indicators of compromise. We are not receiving or we will not be in receipt of any personal information from the operators. All we want to be able to do is assess the severity of the cyber incident by understanding how it happened and the telltales of the compromise or the vulnerability that was exploited. Those tend to be fairly technical exchanges that we would have with the various operators in order to understand the severity of the incident and be able to maybe understand the breadth of the incident and warn other operators, if they have similar technologies, or warn more organizations if they use that technology. So, in a sense, what we will be receiving are technical details to understand what has happened, and nothing of a personal nature will be exchanged between us, whether it is a telecom operator, a financial organization or an energy company. We would not be in receipt of anything that would be of a personal nature in that case.

Senator Batters: Isn't it the case that you would potentially still be receiving personal information, although de-identified information? The two are different. Is that not the case? Am I incorrect on that?

Mr. Khoury: Every incident is different, so I cannot speculate on what an operator would be in a position to share with us in the context of a specific incident. If it was up to us, we would want to understand how the incident happened. Again, we're looking at cybersecurity incidents, and we would want to understand how it happened. If there was a reason for that operator to maybe identify some e-mail or something that would be personal information, either it would be de-identified or we have obligations to protect the privacy of Canadians under our own legislation.

Senator Batters: To the Public Safety officials, this bill has taken eight years to advance to this point, and the federal government still hasn't produced a Gender-based Analysis Plus for it. This government had promised to make GBA Plus documents mandatory for all bills they introduced in Parliament. When I inquired as to whether there was a Gender-based Analysis Plus for Bill C-26, the government finally replied with only this: "If passed, a GBA Plus analysis will be conducted as part of the regulations development process." How does the

Que répondriez-vous à ces graves préoccupations?

Sami Khoury, agent supérieur pour la cybersécurité, Centre de la sécurité des télécommunications Canada : Je vous remercie de cette question.

Nous prenons le rôle de l'organisme de surveillance très au sérieux et nous collaborons avec lui dans le cadre de tous ses examens.

Dans le contexte du projet de loi C-26, les renseignements que nous recevrons des exploitants désignés sont censés être des indicateurs de compromission. Nous ne recevons pas ou nous ne recevrons pas de renseignements personnels de la part des exploitants. Tout ce que nous voulons être en mesure de faire, c'est d'évaluer la gravité du cyberincident en comprenant comment il s'est produit et en repérant les signes révélateurs de la compromission ou de la vulnérabilité qui a été exploitée. Nous avons généralement des échanges assez techniques avec les divers exploitants afin de comprendre la gravité de l'incident, de pouvoir en saisir l'ampleur et d'avertir d'autres exploitants, s'ils disposent des technologies similaires, ou de prévenir d'autres organisations qui utilisent cette technologie. Donc, en un sens, nous recevrons des détails techniques pour comprendre ce qui s'est passé, et aucun renseignement de nature personnelle ne sera échangé entre nous, qu'il s'agisse d'un fournisseur de services de télécommunications, d'une organisation financière ou d'une société d'énergie. Nous ne recevrons rien qui soit de nature personnelle en pareil cas.

La sénatrice Batters : N'est-il pas vrai que vous pourriez tout de même recevoir des renseignements personnels, bien qu'ils soient dépersonnalisés? Les deux sont différents. N'est-ce pas le cas? Est-ce que je me trompe?

M. Khoury : Chaque incident est différent; je ne peux donc pas avancer d'hypothèses sur ce qu'un exploitant serait en mesure de nous communiquer dans le contexte d'un incident précis. S'il en tenait qu'à nous, nous voudrions comprendre comment l'incident s'est produit. Encore une fois, nous examinons les incidents de cybersécurité, et nous cherchons à comprendre comment cela s'est produit. Si l'exploitant avait une raison d'identifier un courriel ou un document contentant des renseignements personnels, le tout serait dépersonnalisé, à défaut de quoi nous avons quand même l'obligation de protéger la vie privée des Canadiens en vertu de notre loi.

La sénatrice Batters : Je m'adresse maintenant aux fonctionnaires du ministère de la Sécurité publique. Il a fallu huit ans pour que le projet de loi en arrive à ce stade, et le gouvernement fédéral n'a toujours pas produit d'analyse comparative entre les sexes plus, ou ACS Plus, à ce sujet. Le gouvernement actuel avait promis de rendre obligatoires les documents d'ACS Plus pour tous les projets de loi qu'il présenterait au Parlement. Lorsque j'ai demandé si le projet de loi C-26 avait fait l'objet d'une analyse comparative entre les

government justify their failure to produce a GBA Plus document — their own requirement — on Bill C-26 until long after the bill passes both Houses of Parliament?

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

In the case of Bill C-26, there was a GBA Plus analysis that was completed, and I understand a summary of this analysis — it happened in two instances — was provided to the committee.

Senator Batters: I'm the critic of the bill. I asked for it, and the response I got was, "If passed, a GBA Plus analysis will be conducted as part of the regulations development process." They told me there wasn't one. If you have one, I would sure be happy to get it, but I note it still hasn't been produced after the House of Commons had the bill for two years.

Mr. MacSween: My understanding is the summary was provided to the committee today.

Senator Batters: Today? Okay. Interesting.

Senator McNair: I would like to drill down a little more around the confidential proceedings questioning or responses.

Bill C-26's critic in the Senate raised concerns during her second reading speech about closed court proceedings. Can you comment on how long closed proceedings have been an element of our court system whenever matters of national security are concerned? Can you also expand on what factors a court might consider in determining whether such proceedings might be appropriate in a specific case?

Mr. MacSween: Thank you for the question.

I don't have the exact time frame for how long these types of proceedings have existed. I have been a national security practitioner for about 12 years now, and they have existed for my lifetime in that field.

Generally speaking, just to the second part of the question, the intention behind the confidential proceedings is to protect classified information or, specifically, information that is deemed injurious to national security or international relations. How that plays out — and the way it is written in the legislation — is that a person that is subject to a proceeding has to identify to the Attorney General of Canada whether they intend to rely on classified information. Should that be the case,

sexes plus, le gouvernement a finalement répondu ce qui suit : « Si le projet de loi est adopté, une analyse ACS Plus sera effectuée dans le cadre du processus d'élaboration des règlements. » Comment le gouvernement justifie-t-il son incapacité à produire un document d'ACS Plus — comme il l'exige lui-même — pour le projet de loi C-26 longtemps après son adoption par les deux Chambres du Parlement?

M. MacSween : Je vous remercie beaucoup de cette question.

Dans le cas du projet de loi C-26, une analyse ACS Plus a été effectuée, et je crois comprendre qu'un résumé de cette analyse — en deux volets — a été fourni au comité.

La sénatrice Batters : Je suis la porte-parole pour le projet de loi. J'ai posé une question à ce sujet, et on m'a répondu : « Si le projet de loi est adopté, une analyse ACS Plus sera effectuée dans le cadre du processus d'élaboration des règlements. » On m'a dit que rien de la sorte n'avait été fait. Si vous avez une telle analyse, je serai heureuse de l'obtenir, mais je remarque qu'elle n'a toujours pas été produite après que la Chambre des communes a reçu le projet de loi il y a deux ans.

M. MacSween : Je crois comprendre que le résumé a été remis au comité aujourd'hui même.

La sénatrice Batters : Aujourd'hui même? D'accord. C'est intéressant.

Le sénateur McNair : J'aimerais approfondir un peu plus les questions ou les réponses relatives aux procédures confidentielles.

Lors de son discours à l'étape de la deuxième lecture, la porte-parole au Sénat pour le projet de loi C-26 a soulevé des préoccupations au sujet des procédures judiciaires à huis clos. Pouvez-vous nous dire depuis combien de temps les procédures à huis clos font partie de notre système judiciaire lorsque des questions de sécurité nationale sont en cause? Pouvez-vous également préciser les facteurs qu'un tribunal pourrait prendre en compte pour déterminer si de telles procédures s'imposent dans un cas précis?

M. MacSween : Je vous remercie de cette question.

Je ne sais pas exactement depuis combien de temps ces types de procédures existent. Je travaille dans le domaine de la sécurité nationale depuis une douzaine d'années maintenant, et ces procédures ont toujours été là pendant cette période.

De façon générale, pour répondre à la deuxième partie de la question, les procédures confidentielles visent à protéger les renseignements classifiés ou, plus précisément, les renseignements jugés préjudiciables à la sécurité nationale ou aux relations internationales. Voici comment les choses se déroulent, conformément à la loi : la personne faisant l'objet d'une poursuite doit faire savoir au procureur général du Canada si elle a l'intention de s'appuyer sur des renseignements

the Attorney General of Canada can then make an application to the court to have that information protected. At that point, a justice would review the relevant information and make their own determination as to whether there is injury to national security, international relations or public safety. That conversation would take place with the Attorney General and the minister.

In the case of the regime being proposed here, I think we all understand Bill C-70 passed and that regime will take over. One of the items in that regime is that the court can avail itself to special counsel who is there to protect the rights of the individual who cannot see the information. That, again, is at the discretion of the court as to whether it is required, but that's kind of the process and how it plays out.

In terms of the confidential information, it is just limited to that information, which is classified and could, at the end of the day, be injurious to international relations or public safety. The open court principle would apply to everything else.

Senator Boehm: My questions are for Mr. Khoury. It is good to have you back.

You have been in this business for a while. You have been waiting for this bill to pass for a while. From your vantage point, what do you see as the most critical challenge in terms of implementing the legislation effectively, ensuring both the public and private sectors are adequately prepared? Is it FTEs? Is it budget? That's one question.

The other question is, assuming passage of the bill and its implementation, are you prepared for any retaliation from malign actors who are going to try to test you and test us?

Mr. Khoury: Thank you, senator, for the question.

If I can answer in reverse order, no, I don't necessarily expect malign actors to retaliate because Canada is raising its cyber-resilience. If anything, they might be a bit more determined. But the hope is that with that bill, we raise the collective cyber-resilience not only of critical infrastructure sectors but also of other sectors that are not subject to the bill and ensure that our collective cybersecurity is better. Maybe that's the answer to the second part.

For the first on the challenges, Canada is a huge country, very diverse and dispersed, and the biggest challenge will be how we tackle all of these operators across all these sectors and support them in their cybersecurity journey. They are not all at the same

classifiés. Le cas échéant, le procureur général du Canada peut alors présenter une demande au tribunal pour que ces renseignements soient protégés. À partir de là, un juge examinerait les renseignements pertinents et déterminerait lui-même s'il y a atteinte à la sécurité nationale, aux relations internationales ou à la sécurité publique. Cette conversation aurait lieu avec le procureur général et le ministre.

Dans le cas du régime proposé ici, je pense que nous comprenons tous que le projet de loi C-70 a été adopté et que ce régime prendra le relais. Entre autres, ce régime permet au tribunal de faire appel à un conseiller juridique spécial chargé de protéger les droits de la partie en cause lorsque les renseignements sont présentés à huis clos. Encore une fois, c'est à la discrétion du tribunal de décider si cela s'avère nécessaire, mais voilà en gros comment se déroule le processus.

Pour ce qui est des renseignements confidentiels, ils se limitent aux renseignements qui sont classifiés et qui pourraient, au bout du compte, porter atteinte aux relations internationales ou à la sécurité publique. Le principe de l'audience publique s'appliquerait à tout le reste.

Le sénateur Boehm : Mes questions s'adressent à M. Khoury. Je suis heureux de vous revoir.

Vous travaillez dans ce domaine depuis un certain temps. Vous attendiez l'adoption de ce projet de loi depuis un bon moment. De votre point de vue, quel est le défi le plus important à relever pour mettre en œuvre le projet de loi de manière efficace, en veillant à ce que les secteurs public et privé soient adéquatement préparés? S'agit-il des effectifs? S'agit-il du budget? Voilà pour ma première question.

L'autre question est la suivante : en supposant que le projet de loi soit adopté et mis en œuvre, êtes-vous prêt à faire face à des représailles de la part d'acteurs malveillants qui essaieront de mettre à l'épreuve vos systèmes et les nôtres?

M. Khoury : Je vous remercie, sénateur, de me poser cette question.

Si je peux me permettre de répondre dans l'ordre inverse, non, je ne m'attends pas nécessairement à ce que des acteurs malveillants ripostent parce que le Canada accroît sa résilience contre les cybermenaces. À tout le moins, ils seraient peut-être un peu plus déterminés. J'espère toutefois que le projet de loi nous permettra d'accroître la cyberrésilience collective non seulement des secteurs d'infrastructures essentielles, mais aussi d'autres secteurs qui ne sont pas visés par le projet de loi, et d'améliorer notre cybersécurité collective. Cela répond peut-être à la deuxième partie de votre question.

Pour ce qui est de la première partie concernant les défis, le Canada est un pays immense, très diversifié et doté d'une population dispersée. Par conséquent, le plus grand défi sera d'établir comment collaborer avec ces exploitants dans tous les

point in their cyber maturity. Some big companies are well vested in cybersecurity; smaller ones might need a bit more hand-holding.

Also, maybe a challenge in the short term would be drawing the threshold on what is a cyber incident that is a reportable cyber incident. We don't want to be putting the line too low, so that — for argument's sake — if you lose your password, you report it. But we don't want to put it very high, so that we don't receive any cyber reports at the end of the year. We want to find the right balance in defining a cyber incident, but we also want to be mindful of the impact of our definition of trans-border activities. For a Canadian company that operates in the U.S., we might have to be mindful of the fact that we don't want to create confusion by having one definition in Canada and one definition in the U.S. How do we balance that?

Senator Boehm: Going back to Senator Batters' earlier question, do you have any plans for small and medium-sized enterprises, SMEs, that will need assistance? She asked the ministers but didn't quite get the answer that we all wanted. Are you looking more closely at that in terms of a plan?

Mr. Khoury: For Bill C-26, we will have to look at who the designated entities are and work with them. Some of them could be big companies, some of them could be a potentially small- or medium-sized company, and they will all be treated with the Bill C-26 umbrella. For small and medium businesses that are not part of Bill C-26, we have a separate program at the Cyber Centre that is meant to work with them to promote cybersecurity best practices and security controls. That is ongoing today. For either one, we don't have to wait for Bill C-26. We are working with those industries and businesses today to make sure that they have all the necessary tools to raise their cyber-resilience.

Senator Kutcher: Thank you for being with us today.

I'm going to come back to the health care data issue. In addition to what Senator Patterson talked about, we are finding that more and more health care is being delivered online mostly by private vendors in a telecommunications space, but by other private vendors as well. Some of the health care that's being delivered online is not just what we found in LifeLabs with lab results, but psychotherapy is being delivered online with an incredible amount of personal data that could be very damaging to individuals who have major roles to play in government, captains of industry and all sorts of other people. Don't you think that health care should be added to Schedule 1?

secteurs visés et comment les soutenir dans leur démarche de cybersécurité. Ils n'en sont pas tous au même degré de cybermaturité. Certaines grandes entreprises participent très activement à la cybersécurité; les petites entreprises, quant à elles, auront peut-être besoin d'un peu plus de soutien.

Par ailleurs, un défi à court terme consisterait peut-être à définir le seuil à partir duquel un cyberincident doit être signalé. Nous ne voulons pas que la barre soit trop basse, à tel point que, par exemple, si vous perdez votre mot de passe, vous aurez à le signaler. Cependant, nous ne voulons pas non plus placer la barre si haut que nous finissions par ne recevoir aucun rapport de cyberincident à la fin de l'année. Nous voulons trouver un juste milieu dans la définition d'un cyberincident, mais nous voulons aussi tenir compte de l'impact de notre définition sur les activités transfrontalières. Pour une entreprise canadienne qui exerce ses activités aux États-Unis, nous devrons peut-être ne pas perdre de vue le fait que nous ne voulons pas créer de confusion en ayant une définition au Canada et une autre aux États-Unis.

Le sénateur Boehm : Pour revenir à la question précédente de la sénatrice Batters, avez-vous des plans pour les petites et moyennes entreprises, les PME, qui auront besoin d'aide? Elle a posé la question aux ministres, mais elle n'a pas obtenu la réponse que nous souhaitions tous. Envisagez-vous un plan particulier à cet égard?

M. Khoury : Pour le projet de loi C-26, nous devrons établir qui sont les entités désignées et travailler avec elles. Certaines pourraient être de grandes entreprises, d'autres pourraient être des PME, et elles seront toutes traitées aux termes du projet de loi C-26. Le centre pour la cybersécurité a un programme distinct pour collaborer avec les petites et moyennes entreprises qui ne sont pas concernées par le projet de loi afin de promouvoir les meilleures pratiques et les contrôles de sécurité en matière de cybersécurité. Ce programme est en cours. Dans un cas comme dans l'autre, il n'est pas nécessaire d'attendre le projet de loi C-26. Nous travaillons d'ores et déjà avec ces industries et ces entreprises pour nous assurer qu'elles disposent de tous les outils nécessaires pour améliorer leur cyberrésilience.

Le sénateur Kutcher : Merci de vous être joints à nous aujourd'hui.

Je vais revenir sur la question des données sur les soins de santé. En plus de ce qu'a dit le sénateur Patterson, nous constatons que de plus en plus de soins de santé sont fournis en ligne, principalement par des fournisseurs privés dans l'espace des télécommunications, mais aussi par d'autres fournisseurs privés. Les soins de santé fournis en ligne ne se limitent pas à ceux que fournit LifeLabs avec les résultats de laboratoire. Il y a aussi des services de psychothérapie qui sont fournis en ligne avec une quantité incroyable de données personnelles qui pourraient être très préjudiciables à des particuliers qui ont des rôles importants à jouer au sein du gouvernement, à des capitaines d'industrie et à toutes sortes d'autres personnes. Ne

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

I don't disagree that the health care sector has absolutely been a target of malicious cyberactivity, and certainly it is the case that a lot of very sensitive personal information is held in that sector. However, as the ministers pointed out, the bill as written only applies to federally regulated critical infrastructure sectors.

In the case of Part 2, we will have to go through a process where we designate the operators of the vital services and systems, and that will happen as part of the regulatory process. I can't say whether or not telecom service providers would be caught up in that if they are providing health care advice. I just don't have that information right now. That process will happen later on.

Mr. Arbour: To build on that, the schedule under Part 2 is pre-populated with the most obvious, very clearly federal jurisdiction systems and sectors. We're chomping at the bit to move forward — should this receive Royal Assent — with some very clear, urgent and pressing needs that are very clearly in federal jurisdiction. There is a range of more cooperative activities that perhaps Sami could speak to as well.

To the extent that there are issues within the telecommunications sector tied specifically to telecommunication services, there is scope there. To the extent that they are not captured but under federal jurisdiction, the schedule can be amended by the Governor-in-Council. It doesn't require going back to Parliament, which allows for some flexibility, provided that it is within federal jurisdiction.

The last point I would make is that there are obligations within the privacy sphere in terms of generalized obligations on the private sector if in federal jurisdiction. If you are a private company — even in the health care space — you are subject to PIPEDA, and potentially under Bill C-27 as well which has expanded authorities to ensure that the private sector is protecting Canadians' personal information.

Mr. Khoury: Besides Bill C-26, we at the Cyber Centre at CSE are very busy working with the health care sector. We take the protection of Canadians' medical data very seriously, and we have seen, unfortunately, too many incidents affect the data and the health care system. We have constant engagement with the health care community to bring to their attention the latest threats that we are seeing and how to promote cyber hygiene to raise the

pensez-vous pas que les soins de santé devraient être ajoutés à l'annexe 1?

M. MacSween : Merci beaucoup de cette question.

Je ne conteste pas le fait que le secteur des soins de santé a été la cible de cyberactivités malveillantes. Il est certain que ce secteur détient une grande quantité de renseignements personnels très confidentiels. Toutefois, comme l'ont souligné les ministres, le projet de loi précise qu'il ne s'applique qu'aux secteurs des infrastructures essentielles sous réglementation fédérale.

Dans le cas de la partie 2, nous devrons passer par un processus de désignation des fournisseurs de services et systèmes essentiels, ce qui se fera dans le cadre du processus réglementaire. Je ne peux pas dire si les fournisseurs de services de télécommunications qui fournissent des conseils en santé seront visés. Je ne dispose pas de cette information pour l'instant. Ce processus interviendra plus tard.

M. Arbour : Pour continuer sur cette lancée, l'annexe de la partie 2 fait déjà la liste des systèmes et des secteurs de compétence fédérale les plus évidents et les plus clairement visés. Nous sommes impatients d'aller de l'avant — si ce texte reçoit la sanction royale — avec des besoins très clairs, urgents et pressants qui sont sans équivoque de compétence fédérale. Il existe une série d'activités plus coopératives dont les Samis pourraient peut-être aussi parler.

Dans la mesure où il existe des problèmes dans le secteur des télécommunications qui sont liés spécifiquement aux services de télécommunication, il y a une marge de manœuvre. Dans la mesure où ces questions ne sont pas prises en compte, mais qu'elles sont de compétence fédérale, l'annexe peut être modifiée par le gouverneur en conseil. Il n'est pas nécessaire de revenir devant le Parlement, ce qui permet une certaine flexibilité, à condition que cela soit de compétence fédérale.

Le dernier point que je voudrais soulever, c'est qu'il existe des obligations dans le domaine de la protection des renseignements personnels, c'est-à-dire des obligations généralisées pour le secteur privé quand celui-ci relève d'une compétence fédérale. Si vous êtes une entreprise privée — même dans le domaine de la santé —, vous êtes soumis aux dispositions de la Loi sur la protection des renseignements personnels et les documents électroniques et, éventuellement, aux dispositions législatives qui seront mises en œuvre par le projet de loi C-27 afin d'instaurer des pouvoirs élargis pour veiller à ce que le secteur privé assure la protection des renseignements personnels des Canadiens.

M. Khoury : Outre le projet de loi C-26, le Centre pour la cybersécurité du Centre de la sécurité des télécommunications travaille beaucoup avec le secteur des soins de santé. Nous prenons très au sérieux la protection des données médicales des Canadiens, et nous avons malheureusement vu trop d'incidents menacer ces données et les systèmes de santé. Nous sollicitons constamment le milieu des soins de santé pour attirer son

collective bar. We constantly issue advisory alerts providing advice and guidelines on the latest vulnerabilities out there. It could be something on an MRI machine or an electronic medical records system. We are constantly communicating that information at all levels of the health care, both provincial and municipal.

Mr. MacSween: The ministers are on record as saying that Bill C-26, even though it applies to federally regulated sectors, is intended to be a model for other levels of government — provinces, territories and municipalities. We at the official level have done engagements with the provinces and territories, providing advice on the legislation and the requirements therein but also talking about regulatory harmonization so if they ever did go down the road to enact a similar type of legislation, then we would be ready, willing and able to have those conversations about how we can best support that. We have seen some legislative initiatives in Quebec and Ontario. They are novel, but they are trending in this direction.

Senator Duncan: Thank you to the witnesses.

There are significant gaps in Canada's North where communications technology is very limited. The Rangers perform a vital presence in Canada's North, and law enforcement throughout the North is the RCMP. Communications is vital to these two specific areas and the individuals involved. It is health; it is safety; it is personal safety; it's also national security. When communication systems are not available, organizations turn to what is available, and that is perhaps a satellite link that is not provided by Canada or not provided by a Canadian. How will Bill C-26 help that situation? Canada's answer is coming, but it is a way's away, and I am concerned that we're going to be closing the barn door after the horse has left.

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

This issue is a huge priority for my department and for the government. In 2022, Minister Champagne announced the Telecommunications Reliability Agenda, which is that we are going to use every single tool in the toolbox to promote the reliability of the telecommunications system. Bill C-26 is a part of that agenda, but it is one part.

I'll give you a few examples. The Dempster Fibre Line between Dawson and Inuvik was funded by the Connect to Innovate fund with Infrastructure Canada and the Yukon Territory. Another example of this would be a new regulatory

attention sur les dernières menaces que nous voyons émerger et sur la façon de promouvoir la cyberhygiène comme moyen de relever la vigilance collective. Nous publions constamment des alertes qui fournissent des conseils et des lignes directrices sur les plus récentes vulnérabilités. Il peut s'agir d'un appareil d'imagerie par résonance magnétique ou d'un système de dossiers médicaux électroniques. Nous communiquons constamment ces renseignements à tous les échelons des soins de santé, tant au provincial qu'au municipal.

M. MacSween : Les ministres ont déclaré publiquement que, même s'il s'applique aux secteurs réglementés par le gouvernement fédéral, le projet de loi C-26 est destiné à servir de modèle aux autres ordres de gouvernement — provinces, territoires et municipalités. Nous sommes intervenus officiellement auprès des provinces et des territoires en leur fournissant des conseils sur le projet de loi et sur les exigences qu'il contient. Nous avons en outre discuté avec eux de l'harmonisation des règlements, de sorte que si jamais ils se lancent dans l'adoption de mesures législatives similaires, nous serons prêts, disposés et capables d'avoir des discussions sur la façon optimale dont nous pourrions les appuyer. Nous avons vu certaines initiatives législatives au Québec et en Ontario. Elles sont nouvelles, mais elles vont dans le même sens.

La sénatrice Duncan : Merci à nos témoins.

Il y a des lacunes importantes dans le Nord canadien où la technologie des communications est très limitée. Les Rangers assurent une présence vitale dans le Nord canadien, et la GRC est chargée de faire appliquer la loi sur tout ce territoire. Les communications sont vitales pour ces deux domaines particuliers et pour les personnes concernées. C'est une question de santé, de sécurité, de sécurité personnelle et de sécurité nationale. Lorsque les systèmes de communication ne sont pas disponibles, les organisations se tournent vers ce qui est disponible, et c'est peut-être une liaison par satellite qui n'est pas fournie par le Canada ou qui n'est pas fournie par un Canadien. Comment le projet de loi C-26 peut-il améliorer cette situation? La réponse du Canada est imminente, mais il reste encore beaucoup de chemin à faire. Ma crainte est que nous fermions la porte de l'écurie après que le cheval est parti.

M. Arbour : Merci, sénatrice, de cette question.

Ce dossier est une grande priorité pour mon ministère et pour le gouvernement. En 2022, le ministre Champagne a annoncé le programme de fiabilité des télécommunications, aux termes duquel nous allons être en mesure d'utiliser tous les outils de la boîte à outils pour promouvoir la fiabilité du système de télécommunications. Le projet de loi C-26 fait partie de ce programme, mais il n'en est qu'une partie.

Je vais vous donner quelques exemples. La Dempster Fibre Line entre Dawson et Inuvik a été financée par le fonds Brancher pour innover en collaboration avec Infrastructure Canada et le gouvernement du Yukon. Un autre exemple serait le nouveau

regime the department announced that in June to facilitate direct communications between average cellular devices and satellites. Historically, the technology would not allow for that, and you would need a special satellite phone. That's another way to enable communications when you don't have access to the terrestrial network.

In 2023, the government issued a formal policy direction to the Canadian Radio-television and Telecommunications Commission, the CRTC, under the Telecommunications Act. That's a legal instrument on the CRTC. It set out a range of expectations, covering a broad set of issues on competition and consumer protection, but improving resiliency was a core stream of those efforts. The CRTC is looking at how it can best update its rules and programs, such as its broadband fund, to better support resiliency.

In terms of the authorities under Bill C-26, it ensures that security considerations are front and centre in the policy objectives of the act to make it clear that the government can take action. It has a set of tools to be able to do so in a nimble way against a variety of threats. That includes information-collection authorities. If we hear or see concerns about a particular network system that requires further investigation, we can investigate it and, as necessary, impose obligations to mitigate it. That can go so far as an outright prohibition. In the case of high-risk vendor equipment, there are clear examples where the risk cannot be mitigated through less intrusive means, so an outright prohibition is indicated. Sometimes that might mean additional protocols or mechanisms to have that in place. In doing so, we want to make sure that we strike the right balance between what makes sense from an implementation standpoint and a risk-management standpoint, and then abilities to respond. We will never get to a risk level of zero. There will always be a forest fire or some other type of threat. Resilience is about not just having rules up front but also having rules and procedures in place to be able to respond to a crisis so that, when there is an incident, there is an ability to respond.

The memorandum of understanding that Minister Champagne talked about with the telecom operators — and this is an example of that — included voluntary mechanisms. They are just voluntary, but we are starting with, for instance, emergency roaming. When we had the tragic fires around Jasper, that enabled TELUS to have access to the Rogers' network and route its traffic through them.

régime réglementaire que le ministère a annoncé en juin pour faciliter les communications directes entre les appareils cellulaires moyens et les satellites. Jusqu'ici, la technologie ne le permettait pas et il fallait un téléphone satellite spécial. C'est une autre façon de permettre les communications lorsqu'il n'y a pas de réseau terrestre.

En 2023, le gouvernement a donné une instruction officielle au Conseil de la radiodiffusion et des télécommunications canadiennes, ou CRTC, aux termes de la Loi sur les télécommunications. C'était un instrument juridique à l'intention du CRTC. Elle définit une série d'attentes et couvre un large éventail de questions relatives à la concurrence et à la protection des consommateurs. Sauf que l'amélioration de la résilience est au cœur de ces efforts. Le CRTC étudie la meilleure façon de mettre à jour ses règles et ses programmes, tels que le Fonds pour la large bande, afin de mieux soutenir cette résilience.

En ce qui concerne les pouvoirs conférés par le projet de loi C-26, ce dernier garantit que les considérations de sécurité sont au premier plan des objectifs stratégiques de la loi afin qu'il soit clair que le gouvernement peut prendre des mesures. Il dispose d'un ensemble d'outils qui lui permettent d'intervenir en souplesse et contre une diversité de menaces. Il s'agit notamment des autorités chargées de la collecte de renseignements. Si nous entendons parler de préoccupations ou constatons des problèmes qui concernent un système de réseau particulier et nécessitent un examen plus approfondi, nous pouvons enquêter et, le cas échéant, imposer une obligation d'atténuer le risque. Cela peut aller jusqu'à l'interdiction pure et simple d'utiliser l'élément problématique. Dans le cas d'équipements de fournisseurs à haut risque, il existe des exemples clairs où le risque ne peut être atténué par des moyens raisonnablement intrusifs, de sorte qu'une interdiction pure et simple est indiquée. Parfois, cela peut impliquer le recours à des protocoles ou mécanismes de mise en place supplémentaires. En procédant de la sorte, nous voulons nous assurer de trouver le bon équilibre entre ce qui est logique du point de vue de la mise en œuvre et du point de vue de la gestion des risques, et la capacité de réagir. Nous n'arriverons jamais à supprimer le risque complètement. Il y aura toujours un feu de forêt ou un autre type de menace. La résilience ne consiste pas seulement à établir des règles dès le départ, mais aussi à mettre en place des règles et des procédures permettant de répondre à une crise, de sorte qu'en cas d'incident, il soit possible de réagir.

Le protocole d'entente dont le ministre Champagne a parlé avec les fournisseurs de services de télécommunications — et ceci en est un exemple — comprenait des mécanismes offerts sur une base volontaire. Ce ne sont que des mécanismes facultatifs, mais nous commençons, par exemple, par l'itinérance d'urgence. Lors des incendies tragiques qui se sont produits près de Jasper, ce mécanisme a permis à TELUS d'avoir accès au réseau de Rogers et de faire passer son trafic par ce dernier.

Senator M. Deacon: Thank you for being here.

I was encouraged, Mr. Khoury, to hear you talk about operators and sectors, what the threshold is, what the threat is and what it is not, and, of course, determining designated entities.

This is our night. We've opened up a bill here in committee. We've heard from our ministers. There are a whole bunch of people behind you who bring different expertise to support you. We will carry on speaking to and listening to other witnesses next week. My question is, with the wealth of knowledge behind you, is there anything that we have not touched on tonight that your teams bring that we should be hearing from you while you are here? We are asking questions, for sure, but to fill that gap, is there anything that we have not touched on that the folks in the room have expertise on?

Mr. Khoury: I can start and maybe ask my colleagues to chime in.

This bill is super important because it will give us a better pulse of the threat landscape that Canada is facing. Today, incident reporting is voluntary, so we don't have that ability to assess — not just in a particular sector but across sectors — what the threat is. With that incident reporting, it will at least give us more data points so that we can see whether a certain sector is under attack or if, across a sector, there's suddenly a new cybercrime group or a new state-sponsored actor that is going after Canada. We will have those data points.

The threat landscape is getting more and more complex every day. For us, partnership would be very important, not only at the sectoral level. Today, we have good engagement with the various sectors, for example, the banking sector, the telecom sector and the energy sector. We have very good engagement and regular meetings. We talk frankly and openly about what they are seeing.

If we can get into a specific program, I can ask my colleague Mr. Couillard to add more colour commentary on the nature of the partnership that we want to take up with those various sectors.

Daniel Couillard, Director General, Partnerships and Risk Mitigation, Canadian Centre for Cyber Security, Communications Security Establishment Canada: Thank you for your question. It is very surprising for you to ask us to tell

La sénatrice M. Deacon : Je vous remercie de votre présence.

J'ai été encouragé, monsieur Khoury, de vous entendre parler des fournisseurs et des secteurs, de ce qu'est le seuil, de ce qui est une menace et de ce qui n'en est pas une, et, bien sûr, de la nécessité d'établir qui sont les entités désignées.

C'est notre soirée. Le comité s'est attaqué à un projet de loi. Nous avons entendu nos ministres. Il y a toute une série de personnes qui vous soutiennent et qui vous apportent leur expertise. Nous continuerons à parler et à écouter d'autres témoins la semaine prochaine. Ma question est la suivante: compte tenu de la grande connaissance que vous avez à ce sujet, y a-t-il quelque chose que nous n'avons pas abordé et que nous devrions entendre pendant que vous êtes ici, vous et votre équipe? Nous posons des questions, c'est certain, mais pour combler cette lacune, y a-t-il un sujet que nous n'avons pas abordé et à propos duquel les personnes présentes dans la salle ont des connaissances expertes?

M. Khoury : Je peux commencer et, peut-être, demander à mes collègues d'intervenir au besoin.

Ce projet de loi est extrêmement important, car il nous permettra d'avoir un portrait plus précis du profil des menaces qui s'exercent sur le Canada. Aujourd'hui, le signalement des incidents se fait sur une base volontaire, de sorte que nous n'avons pas la capacité d'évaluer — non seulement dans un secteur particulier, mais dans l'ensemble des secteurs — la nature de la menace. À tout le moins, le signalement des incidents nous fournira plus de données pour que nous puissions voir si un certain secteur est attaqué ou si, dans un secteur donné, il y a soudainement un nouveau groupe cybercriminel ou un nouvel acteur parrainé par un État qui s'en prend au Canada. Nous disposerons de ces données.

Le paysage des menaces se complexifie de jour en jour. Pour nous, un partenariat serait très important, et pas seulement dans une optique sectorielle. Aujourd'hui, nous avons une bonne interaction avec les différents secteurs. Pensons entre autres au secteur bancaire, au secteur des télécommunications et à celui de l'énergie. Nous avons une très bonne interaction avec eux et nous les rencontrons sur une base régulière. Nous parlons franchement et ouvertement de ce qu'ils constatent.

Si nous pouvons entrer dans un programme particulier, je peux demander à mon collègue, M. Couillard, d'ajouter des observations plus précises sur la nature du partenariat que nous souhaitons établir avec ces différents secteurs.

Daniel Couillard, directeur général, Partenariats et atténuation des risques, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications Canada : Merci de votre question. Il est très surprenant que

you what to look for. I will pick up on Mr. Khoury's point and try to highlight the big value that Bill C-26 will bring to Canada.

Part of the requirement that will be on designated operators is the creation of a cybersecurity program that will describe their security controls that they are putting in place to address those threats. What we have now is the ability to have a full feedback loop. As Mr. Khoury mentioned, if they see a threat, they will report to us, and if we will see a threat, we can provide advice and guidance on how to mitigate that threat. Once we have all these designated operators reporting to us, we will be able to see if the mitigation we recommend — because that mitigation technically will be implemented by the designated operators and will be reflected in the cybersecurity program that they need to maintain as current. Every year, it needs to be refreshed. We will be able to see the value of the security controls and the advice and guidance we are giving. If it doesn't work, we can change it, so we have will have a feedback loop. Some of our Five Eyes partners don't have that model. They focus on mandatory incident reporting, but they don't have the feedback loop for advice and guidance that they are giving. For me, that's a valuable process to implement.

In Canada, some large designated operators that we will have are obvious. The quantity of designated operators will be to a level that makes it workable for us to actually engage in a meaningful, deeper relationship with those designated operators, ultimately leading to better risk management. I think this aspect of the bill does not come out as much as it maybe can, but it is a fundamental benefit that we would have from this bill.

Senator M. Deacon: Thank you.

Senator Batters: Going back to the question from the Bill C-26 sponsor Senator McNair, law professor Matt Malone has pointed out that the lack of transparency in the secretive court proceedings under Bill C-26 is in direct contrast to the legislation governing creation of the Communications Security Establishment, and he states:

> This diverges markedly from the thrust of the CSE's enabling legislation, which seeks to impose greater accountability over certain conduct through prior authorization and review obligations. For example, under that enabling legislation, when the CSE's spying activities contravene federal law or interfere with the reasonable expectation of privacy of individuals in Canada, the agency must obtain approval from the Office of the Intelligence Commissioner. Last year, the Commissioner fully granted half of such requests (three out of six). The cybersecurity

vous nous demandiez de vous dire ce qu'il faut chercher. Je vais reprendre le point de vue de M. Khoury et essayer de souligner toute la valeur que le projet de loi C-26 apportera au Canada.

Les fournisseurs désignés seront notamment tenus de créer un programme de cybersécurité décrivant les contrôles de sécurité qu'ils mettent en place pour faire face à ces menaces. Ce que nous avons maintenant, c'est la capacité d'avoir une boucle de rétroaction complète. Comme l'a mentionné M. Khoury, s'ils constatent une menace, ils nous la signalent, et si nous constatons une menace, nous pouvons fournir des conseils et des orientations sur la façon de l'atténuer. Une fois que tous ces fournisseurs désignés nous auront fait rapport, nous pourrons voir si les mesures d'atténuation que nous recommandons fonctionnent, attendu qu'elles seront techniquement mises en œuvre par les fournisseurs désignés et qu'elles se retrouveront dans le programme de cybersécurité qu'ils doivent maintenir à jour. Le programme doit être mis à jour tous les ans. Nous serons en mesure de voir la valeur des contrôles de sécurité et des conseils que nous donnons. S'ils ne fonctionnent pas, nous pourrons les modifier, de sorte que nous aurons une boucle de rétroaction. Certains de nos partenaires du Groupe des cinq n'ont pas ce modèle. Ils se concentrent sur la déclaration obligatoire des incidents, mais ils n'ont pas de boucle de rétroaction pour les conseils et l'orientation qu'ils donnent. Pour moi, il s'agit d'un processus de grande valeur qui doit être mis en œuvre.

Au Canada, certains grands fournisseurs désignés sont des choix évidents. Le nombre de fournisseurs désignés sera tel qu'il nous permettra de nouer des relations plus approfondies et plus sérieuses avec eux, ce qui, en fin de compte, permettra une meilleure gestion des risques. Je pense que cet aspect ne ressort pas autant qu'il le pourrait, mais c'est l'un des grands avantages que nous fournit ce projet de loi.

La sénatrice M. Deacon : Je vous remercie.

La sénatrice Batters : Pour revenir à la question du sénateur McNair, l'auteur du projet de loi C-26, le professeur de droit Matt Malone a souligné que le manque de transparence des procédures judiciaires secrètes prévues par le projet de loi C-26 est en contradiction directe avec la loi régissant la création du Centre de la sécurité des télécommunications. Voici ce qu'il soutient :

> Cela s'écarte nettement de l'orientation de la loi d'habilitation du CST, qui cherche à imposer une reddition de comptes accrue à l'égard de certaines conduites en exigeant des autorisations et des examens préalables. Par exemple, en vertu de cette loi habilitante, lorsque les activités d'espionnage du CST contreviennent à la loi fédérale ou portent atteinte aux attentes raisonnables en matière de protection de la vie privée des personnes au Canada, il doit obtenir l'approbation du Bureau du commissaire au renseignement. L'année dernière, le

direction powers in Bill C-26 are subject to no similar kind of review.

Why doesn't Bill C-26 contain those types of review powers?

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

Obviously, one of the amendments that was made by the Standing House of Commons Committee on Public Safety and National Security was the issuance of an advisory to NSIRA and NSICOP because those bodies themselves were set up to ensure transparency and that there were groups that could look at all the classified information and make recommendations on the basis of what they were seeing. The advisories to NSIRA and NSICOP particularly in the case of cybersecurity directions are intended to be measures to ensure transparency and review of those cybersecurity directions if it's required. In the case of both bodies, they do have broad access to all the information holdings at the Communications Security Establishment.

Senator Batters: May I interrupt you? Sorry, I have a limited time here. How do those bodies ensure transparency when they report to the Prime Minister? Their members are appointed to those bodies by the Prime Minister and they report to the Prime Minister, and then the Prime Minister's office could vet those reports and provide to the public what they deem is necessary for the public to see. How does that ensure transparency?

Mr. MacSween: I don't pretend to know the enabling legislation of the review bodies that well. I know that, in the case of NSIRA, they are independent of both the executive level of government and of Parliament. Again, the whole *raison d'être* for those bodies is so that someone can look at classified information and make a determination. I can't speak to the actual appointment process.

On just the protection of classified information, because you asked about that, what is proposed in Bill C-26 is no different than what we could see in other regimes such as the Passenger Protect Program, and it is simply a mechanism to protect classified information from public disclosure. To protect the state's most secretive information, whether it is information shared by an ally, collected by human source or by technical covert means, there does need to be a mechanism to be able to protect that. That is the regime that is set up in the case of Bill C-26 as it relates specifically to the cybersecurity directions.

commissaire a accepté la moitié de ces demandes (trois sur six) dans leur intégralité. Les pouvoirs en matière de directives de cybersécurité que prévoit le projet de loi C-26 ne sont pas soumis à un examen similaire.

Pourquoi le projet de loi C-26 ne contient-il pas ce type de pouvoir en matière d'examen?

M. MacSween : Merci beaucoup de la question.

Évidemment, l'un des amendements apportés par le Comité permanent de la sécurité publique et nationale de la Chambre des communes était l'émission d'un avis à l'intention de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, ou OSSNR, et du Comité des parlementaires sur la sécurité nationale et le renseignement, ou CPSNR, parce que ces organismes eux-mêmes ont été mis sur pied pour assurer la transparence et qu'il y avait des groupes qui pouvaient examiner tous les renseignements classifiés et faire des recommandations sur la base de ce qu'ils voyaient. Les avis adressés à l'OSSNR et du CPSNR, en particulier dans le cas des directives sur la cybersécurité, sont censés être des mesures visant à garantir la transparence et l'examen de ces directives sur la cybersécurité, le cas échéant. Les deux organismes ont effectivement largement accès à tous les renseignements détenus par le Centre de la sécurité des télécommunications.

La sénatrice Batters : Puis-je vous interrompre? Je suis désolée, mais mon temps de parole est limité. Comment ces organismes assurent-ils la transparence lorsqu'ils rendent des comptes au premier ministre? Les membres de ces organismes sont nommés par le premier ministre et rendent des comptes au premier ministre. Ensuite, le cabinet du premier ministre pourrait procéder à un examen approfondi de ces rapports et communiquer au public l'information qu'il juge que le public devrait connaître. En quoi cela garantit-il la transparence?

M. MacSween : Je n'ai pas la prétention de bien connaître la loi habilitante des organismes d'examen. Je sais que, dans le cas du Comité des parlementaires sur la sécurité nationale et le renseignement, ses membres sont indépendants à la fois de l'exécutif du gouvernement et du Parlement. Je le répète, la raison d'être de ces organismes est de permettre à quelqu'un d'examiner des renseignements classifiés et de prendre une décision. Cependant, je ne peux pas parler du processus de nomination proprement dit.

En ce qui concerne la protection des renseignements classifiés, puisque vous avez posé la question, ce qui est proposé dans le projet de loi C-26 n'est pas différent de ce que nous pourrions voir dans d'autres régimes tels que le Programme de protection des passagers. Il s'agit simplement d'un mécanisme visant à protéger les renseignements classifiés contre la divulgation publique. Pour protéger les renseignements les plus secrets de l'État, qu'il s'agisse de renseignements communiqués par un allié, recueillis par une source humaine ou par des moyens techniques clandestins, il faut prévoir un mécanisme qui permet

All of that can be reviewed by the Federal Court. A designated judge in the Federal Court can see all of that information and make their own determinations on the injury to national security and public safety. That's consistent with the regimes we've seen in other administrative proceedings.

Senator Batters: Early in Minister LeBlanc's opening remarks today, he talked about what a major threat ransomware is. Why is Bill C-26 specifically silent on the word "ransomware?" I found no explicit reference to it anywhere in the bill.

Mr. MacSween: Sorry, I missed the question.

Senator Batters: Minister LeBlanc was talking about ransomware and what a major threat it was, but Bill C-26 itself is silent on the very word "ransomware." There is no explicit reference to it anywhere in the bill.

Mr. MacSween: As it relates to the mandatory incident reporting, it is threat agnostic. Regardless of whether it is ransomware or another type of malicious threat activity, that will need to be reported in to the Cyber Centre. The way the legislation is constructed is that we did not want to put specific references to specific threats in the legislation because those can change and evolve on a constant basis. You could see references to that, perhaps, in the regulations or in the cybersecurity programs, but in the legislation itself, if you look at it, it tends to be threat and technology agnostic so that it stands the test of time and does not become outdated.

Senator Batters: There is part of your bill, of course, that is already outdated. Bill C-70, which we passed in the Senate in June, had a portion that has already outdated a certain portion of Bill C-26.

Mr. MacSween: To be honest, I'm not an expert on Bill C-70, but I think the intention there, if I understood the policy intent correctly, was actually to amalgamate the security requirements for administrative proceedings into one piece of legislation under the Canada Evidence Act as opposed to bespoke pieces of legislation like the Passenger Protect Program or Bill C-26.

[*Translation*]

Senator Dagenais: My question is for Mr. MacSween. Mr. MacSween, the impact of some decisions, rulings and orders in telecommunications could go well beyond cybersecurity,

de les protéger. En ce qui concerne les directives de cybersécurité, ce mécanisme sera le régime que le projet de loi C-26 mettra en place. Toute cette information peut être examinée par la Cour fédérale. Un juge désigné de la Cour fédérale peut consulter tous ces renseignements et prendre ses propres décisions quant au préjudice qu'ils pourraient causer à la sécurité nationale et à la sécurité publique. Cela est conforme aux régimes que nous avons vus dans d'autres instances administratives.

La sénatrice Batters : Au début de sa déclaration préliminaire d'aujourd'hui, le ministre LeBlanc a parlé de la menace majeure que représentent les rançongiciels. Pourquoi le projet de loi C-26 ne mentionne-t-il pas le mot « rançongiciel »? Je n'ai trouvé aucune mention explicite de ce terme dans le projet de loi.

M. MacSween : Je suis désolé. Votre question m'a échappé.

La sénatrice Batters : Le ministre LeBlanc parlait des rançongiciels et de la menace importante qu'ils représentent, mais le projet de loi C-26 lui-même ne mentionne pas le mot « rançongiciel ». Il n'y a aucune mention explicite de ce terme dans le projet de loi.

M. MacSween : Les rapports d'incident obligatoire ne tiennent pas compte des types de menaces. Qu'il s'agisse d'un rançongiciel ou d'un autre type d'activités malveillantes, cet incident devra être signalé au centre cybernétique. Lorsque nous avons rédigé la mesure législative, nous n'avons pas voulu mentionner des menaces précises parce qu'elles peuvent changer constamment. Dans les règlements ou les programmes de cybersécurité, on pourrait trouver des allusions à ces menaces, mais la mesure législative elle-même a tendance à ne pas tenir compte des menaces et des technologies, afin de résister à l'épreuve du temps et de ne pas devenir désuète.

La sénatrice Batters : Bien entendu, une partie de votre projet de loi est déjà dépassée. Le projet de loi C-70, que nous avons adopté au Sénat en juin, contient une partie qui rend obsolète une certaine partie du projet de loi C-26.

M. MacSween : Pour être honnête, je ne suis pas un expert en ce qui concerne le projet de loi C-70, mais si j'ai bien compris, je crois que, sur le plan politique, il visait en fait à regrouper les exigences en matière de sécurité pour les poursuites administratives dans un seul texte législatif en vertu de la Loi sur la preuve au Canada, au lieu de créer des textes législatifs particuliers comme le Programme de protection des passagers ou le projet de loi C-26.

[*Français*]

Le sénateur Dagenais : Ma question s'adresse à M. MacSween. Monsieur MacSween, dans l'industrie des télécommunications, certaines décisions, certains jugements et

given Canada's less than harmonious trading relationships with countries like China, India and Russia.

Have you discussed whether the legislation could have an impact on our trading relationships? If so, on what sectors and how will this be managed?

Mr. Arbour: Thank you for your question. With respect to the telecommunications sector, it is of course important to consider potential negative feedback from other countries, but we hold regular discussions with our allies to converge on a policy between us and to protect Canadians in general. The protection of Canadians is the cornerstone of our policy.

This also applies to other economic sectors. Consistent policies among the Five Eyes and with other allied countries make for stronger policies that protect Canadians.

Senator Dagenais: Thank you.

[*English*]

Senator McNair: I had a question on the remote access or connectivity, but it was covered off by Senator Duncan's question.

I just want to say that I liked Senator Deacon's question, the catch-all, which is, what else should we have asked? In response to her question, as I understand it, the answer would be, "Ask us in a year; ask us in two years; ask us in three years." The regulation-making process is not stagnant. It will be ongoing — evergreen, essentially — to make sure the document incorporates feedback you receive — from what you said, we are one exception of the Five Eyes — but the other part is so that it meets the current threat landscape at that time. Is that accurate as far as the process and the regulations?

Mr. MacSween: Yes, senator, I believe that's an accurate description. As you know, the regulation-making process in this case could take anywhere from 18 to 24 months. Obviously, there is a great deal of consultation that will be required, especially in the case of Part 2, to establish the regulatory regime. We will need to be talking with our private sector partners, subnational levels of government, academia and civil society to make sure that what we build is correct and, most importantly, at the end of the day, to make sure that it is do-able by the industry partners as well and achieves the objectives of the legislation.

certains décrets risquent d'avoir une incidence beaucoup plus large que la cybersécurité, étant donné que le Canada a des échanges peu harmonieux avec certains pays, comme la Chine, l'Inde et la Russie.

Avez-vous eu des discussions pour évaluer si l'application de la loi aura des conséquences sur nos relations commerciales? Dans l'affirmative, dans quels secteurs et comment cela sera-t-il géré?

M. Arbour : Merci de la question. Dans le contexte du secteur des télécommunications, il y a bien sûr des considérations en ce qui a trait à une rétroaction négative de certains autres pays, mais nous discutons avec nos alliés régulièrement pour arriver à une politique solide entre nous et pour protéger les Canadiens de façon générale. C'est la protection des Canadiens qui est primordiale dans le contexte de notre politique.

Cela fonctionne de façon semblable dans d'autres secteurs de l'économie. Des politiques constantes par l'entremise du Groupe des cinq ou d'autres pays alliés nous permettront d'arriver à une politique plus solide pour protéger les Canadiens.

Le sénateur Dagenais : Merci.

[*Traduction*]

Le sénateur McNair : J'avais une question à poser au sujet de l'accès à distance ou de la connectivité, mais elle a été abordée lorsque la sénatrice Duncan a posé sa question.

Je voudrais juste dire que j'ai aimé la question fourre-tout que la sénatrice Deacon a posée, c'est-à-dire : « Qu'aurions-nous dû demander d'autre? ». Si j'ai bien compris, la réponse à sa question était la suivante : « Posez-nous la question dans un an, deux ans et trois ans ». Le processus d'élaboration des règlements n'est pas stagnant. Il sera continu — permanent, essentiellement — pour faire en sorte que le document intègre les commentaires que vous recevez — d'après ce que vous avez dit, nous sommes une exception au sein du Groupe des cinq —, mais aussi pour faire en sorte qu'il réponde aux menaces qui seront pertinentes à ce moment-là. Cette description est-elle exacte en ce qui concerne le processus et les règlements?

M. MacSween : Oui, sénateur, je crois que cette description est exacte. Comme vous le savez, le processus de réglementation dans ce cas pourrait prendre de 18 à 24 mois. Il est évident que de nombreuses consultations seront nécessaires, en particulier dans le cas de la partie 2, pour établir le régime réglementaire. Nous devrons discuter avec nos partenaires du secteur privé, les ordres de gouvernement infranationaux, la communauté universitaire et la société civile pour nous assurer que ce que nous établissons est correct et, plus important encore, pour nous assurer en fin de compte que la réglementation peut être respectée par nos partenaires de l'industrie et qu'elle atteint les objectifs de la mesure législative.

We will be learning a lot as we go. Part of the reason we set that up in the regulatory regime is because of the mandatory requirement to do the consultations with those partners as well. For a lot of that, we will absolutely be learning as we go. Another example — I will refer to what my colleague Dan mentioned — is what we see in the cybersecurity program. Part of the objective of this bill is to ensure a baseline level of cybersecurity across the various sectors. As we work with the finance, telecommunications and other sectors, we will be learning about what is in there, what is practical and what is realistic. We will be sharing that information between sectors to help them establish those programs. It will certainly be evolving over time.

Nous apprendrons beaucoup de choses à mesure que nous avancerons. La raison pour laquelle nous avons mis en place ce régime réglementaire est en partie attribuable à l'obligation de mener des consultations avec ces partenaires. À de nombreux égards, nous apprendrons assurément des choses à mesure que nous avancerons. Le contenu du programme de cybersécurité — et je fais allusion à ce que mon collègue, M. Couillard, a mentionné — en est un autre exemple. Une partie de l'objectif du projet de loi est de garantir un niveau de cybersécurité de base dans les différents secteurs. En travaillant avec les secteurs de la finance, des télécommunications et d'autres secteurs, nous apprendrons ce qui existe, ce qui est pratique et ce qui est réaliste. Nous ferons circuler ces informations entre les secteurs afin de les aider à mettre en place ces programmes. La réglementation évoluera certainement au fil du temps.

As you rightly point out, in the case of Part 2, the legislation is deliberately constructed in that manner so that we can learn as we go and be able to adapt to the threats and how the landscape is changing, and also the technology, which is ever evolving.

Comme vous le soulignez à juste titre, dans le cas de la partie 2, la mesure législative est délibérément élaborée de cette manière afin que nous puissions apprendre à mesure que nous avançons et être en mesure de nous adapter aux menaces et à la manière dont elles évoluent, ainsi qu'aux technologies, qui sont en constante évolution.

Senator McNair: Fortunately or unfortunately, there will be never be a "pens down" situation. You will always be working on it.

Le sénateur McNair : Heureusement ou malheureusement, il n'y aura jamais de moment où vous pourrez déposer vos plumes. Vous serez toujours en train de travailler à l'élaboration de cette réglementation.

Mr. MacSween: I will be employable for the next few years.

M. MacSween : Mon emploi devrait être assuré au cours des prochaines années.

Senator McNair: You should be.

Le sénateur McNair : Il devrait l'être.

Senator Kutcher: I must say that I do have a level of discomfort on the health care component. I will try to get my head around that for the next little while, particularly because, as Senator Yussuff pointed out, some of the health care providers are now international. You can go online and get interventions from somebody who is in another country, but you have no idea where that provider is. I will try to get my head around that.

Le sénateur Kutcher : Je dois dire que je suis un peu mal à l'aise par rapport à la question des soins de santé. J'essaierai de saisir les ramifications du projet de loi au cours des prochaines semaines, en particulier parce que, comme l'a souligné le sénateur Yussuff, certains des fournisseurs de soins de santé sont désormais à l'étranger. Vous pouvez aller en ligne et obtenir des interventions auprès de quelqu'un qui se trouve dans un autre pays, mais vous n'avez aucune idée de l'endroit où se trouve ce fournisseur. J'essaierai d'y voir clair bientôt.

My question is for Mr. Khoury. The threat landscape is evolving very, very quickly. Can this bill as written allow us to appropriately mitigate the threat landscape as it evolves?

J'adresse ma question à M. Khoury. Les menaces évoluent très rapidement. Dans sa forme actuelle, le projet de loi peut-il nous permettre d'atténuer de manière appropriée les menaces qui pèsent sur nous à mesure qu'elles évoluent?

Mr. Khoury: Thank you for the question, senator.

M. Khoury : Je vous remercie de votre question, monsieur le sénateur.

Absolutely, it can help us, because once the bill passes and we've finished the establishment of the regulations for those four critical infrastructure sectors on which Canadians depend, we will be able to get a true, accurate picture of the threats they are seeing day to day. Today, we strive to build good working relationships with many of those industries, with many of those

Le projet de loi peut certainement nous aider, car une fois qu'il aura été adopté et que nous aurons terminé de mettre en place la réglementation pour ces quatre secteurs d'infrastructures essentielles dont dépendent les Canadiens, nous serons en mesure d'obtenir une image réelle et précise des menaces qui pèsent sur eux au jour le jour. À l'heure actuelle, nous nous

corporations, but, nevertheless, we still have gaps in our engagements with them. This bill will give us a chance to get that pulse of the Canadian cyber ecosystem and be able to mitigate it and also work with them on mitigation. The bill establishes a framework that probably will sustain the test of time, but it will be on us to keep it alive and to work with the operators when they report an incident to make sure that we are timely in our reaction and that we can share that information with others.

Senator Fridhandler: I will follow on Senator Yussuff's attempt to address the issue of offshore data because I don't think we've got clarity yet. We seem to be able to regulate, to some degree, the import of nefarious equipment and utilization by operators, but does the legislation permit the minister or authorities to issue pre-emptive orders on data location? For example, if an operator decides that the best price for data storage is in North Korea, why would we not stop that just like we stop the import of equipment? Is there an ability under the legislation? If not, I would also like to know, from your expertise, are there disclosure requirements relative to where customers' data might be stored so that they actually have a consumer choice in what's happening? If there is no authority to restrict, whether pre-emptively or in reaction to events, was this even discussed and, if not, why not? Sorry for that mouthful, but I'm trying to get to the bottom line on this because it's always a big concern.

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

In short answer, there absolutely are order-making or regulatory powers that allow for proactive obligations to protect against a full range of threats. The bill was developed with a view to try and anticipate the different threats that could exist, whether they be cyber or natural disaster or other types of bad behaviour. That would allow, within the telecommunications sector, for instance, the imposition of positive obligations on how they govern their networks. That could include both equipment considerations but also human factors or other business processes, if it would protect the Canadian telecommunications system. In looking at that, we will take a risk-management approach in terms of how that could be done. There is a range of different possible considerations in terms of how to best protect that.

efforçons d'établir de bonnes relations de travail avec un grand nombre de ces industries et avec un grand nombre de ces sociétés, mais il y a encore des lacunes dans nos dialogues avec elles. Ce projet de loi nous donnera l'occasion de prendre le pouls de l'écosystème cybernétique canadien et d'être en mesure d'atténuer les menaces et de collaborer avec lui à cette fin. Le projet de loi établit un cadre qui résistera probablement à l'épreuve du temps, mais il nous incombera de le maintenir en vie et de travailler avec les exploitants lorsqu'ils signalent un incident, afin de nous assurer que notre réaction est rapide et que nous pouvons partager ces informations avec d'autres intervenants.

Le sénateur Fridhandler : Je vais poursuivre la tentative du sénateur Yussuff d'aborder la question des données à l'étranger, car je ne crois pas que notre compréhension à cet égard soit claire. Nous semblons pouvoir réglementer, dans une certaine mesure, l'importation d'équipements malveillants et leur utilisation par des exploitants, mais la mesure législative permet-elle au ministre ou aux autorités d'émettre des ordonnances préventives sur l'emplacement des données? Par exemple, si un exploitant décide que le stockage des données le plus économique se trouve en Corée du Nord, pourquoi ne pourrions-nous pas l'empêcher de stocker ses données là-bas, tout comme nous empêchons l'importation d'équipements? La mesure législative le permet-elle? Si ce n'est pas le cas, j'aimerais également savoir, d'après vos connaissances, s'il existe des exigences en matière de divulgation qui sont liées à l'endroit où les données des clients sont peut-être stockées, afin que les consommateurs puissent réellement faire des choix en connaissance de cause. S'il n'y a pas de pouvoir pour limiter ce stockage, que ce soit à titre préventif ou en réaction à des événements, cet enjeu a-t-il même été discuté et, si ce n'est pas le cas, pourquoi ne l'a-t-il pas été? Je m'excuse de cette question tortueuse, mais j'essaie d'aller au fond des choses à cet égard, car cet enjeu est toujours une grande préoccupation.

M. Arbour : Je vous remercie de votre question, monsieur le sénateur.

En bref, il existe certainement des pouvoirs d'ordonnance ou de réglementation qui nous permettent d'imposer des obligations préventives pour nous protéger contre tout un ensemble de menaces. Le projet de loi a été élaboré dans le but d'essayer d'anticiper les différentes menaces qui pourraient exister, qu'il s'agisse de cybermenaces, de catastrophes naturelles ou d'autres types de mauvais comportements. Dans le secteur des télécommunications, cela nous permettrait, par exemple, d'imposer des obligations positives concernant la manière dont ils gèrent leurs réseaux. Cela pourrait inclure à la fois des considérations relatives à l'équipement, mais aussi des facteurs humains ou d'autres processus commerciaux, si cela permet de protéger le système de télécommunications canadien. Pour examiner cet enjeu, nous adopterons une approche de gestion des risques quant à la manière dont ce travail pourrait être fait. Il existe toute une série de facteurs qui pourraient être pris en

The last piece, I would say, is just to circle back to PIPEDA and C-27, which applies more broadly. It is under the trade and commerce head of power, so it applies generally as opposed to being sector-specific. It does have specific obligations for the private sector in terms of the protection of Canadian data. Bill C-27 includes augmented enforcement authorities to ensure that the private sector respects those obligations.

Mr. MacSween: I could probably mention, too, under Part 2 of the act, one of the requirements to which designated operators will be subjected is to identify and mitigate risks from third-party contractors. That's a specific requirement in the act. Those risks will have to be outlined in their cybersecurity program, with the mitigation measures as well. When we say "mitigation measures," we mean what they are doing to minimize likelihood that the risk will materialize or that the risk will happen in the first place. That is a strict obligation under Part 2 for those who are subject to the requirements.

[*Translation*]

Senator Carignan: I have a question about the no compensation clause. In the making of an order, the Governor-in-Council takes into account factors like the financial impact on the telecommunications company. Then, a clause reads:

> 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 under subsection (1).

This could be a really serious matter. Huawei is currently the supplier with the largest financial impact, but other companies once thought to be extremely solid are beginning to show signs of weakness given all the decisions affecting their activities. In fact, it's surprising to see how debt-ridden some companies with a monopoly in the telecoms sector are.

Isn't there a high risk of pushing businesses to the brink of bankruptcy if there's no compensation clause? Is the department thinking of some other form of financial compensation or assistance to prevent hobbling these businesses due to cybersecurity concerns?

Mr. Arbour: Thank you for your question.

Let me give you an example. In the context of telecom regulations, spectrum licensing rules have a huge impact on wireless service offerings. We see the effect on service providers

considération pour déterminer la meilleure façon de protéger ce système.

Je dirais que le dernier élément concerne la LPRPDE et le projet de loi C-27, qui s'applique de manière plus générale. Il relève de la compétence en matière de commerce et d'échanges, alors il s'applique de manière générale et non de manière sectorielle. Il prévoit des obligations particulières pour le secteur privé en matière de protection des données canadiennes. Le projet de loi C-27 prévoit des pouvoirs d'exécution accrus pour veiller à ce que le secteur privé respecte ces obligations.

M. MacSween : Je pourrais probablement mentionner aussi que, dans la partie 2 de la loi, l'une des exigences auxquelles les exploitants désignés seront soumis consistera à déterminer et à atténuer les risques liés aux tiers. C'est une exigence particulière de la loi. Ces risques devront être décrits dans leur programme de cybersécurité, ainsi que les mesures d'atténuation prévues. Par « mesures d'atténuation », nous entendons ce qu'ils font pour minimiser la probabilité que le risque se matérialise ou qu'il se produise en premier lieu. Il s'agit d'une obligation rigoureuse en vertu de la partie 2, qui s'applique à ceux qui sont soumis à ces exigences.

[*Français*]

Le sénateur Carignan : Ma question porte sur la clause de non-indemnisation. Dans les facteurs à prendre en considération pour le décret, le gouverneur en conseil tient compte des facteurs tels que les répercussions financières sur l'entreprise de télécommunications, par exemple. Tout de suite après, une clause dit :

> 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.

Cela peut être extrêmement sérieux. Huawei est le fournisseur qui a actuellement le plus gros impact financier, mais d'autres entreprises qu'on pense extrêmement solides commencent à montrer des signes de fragilité avec l'ensemble des décisions prises qui touchent leurs activités. On est d'ailleurs surpris de constater l'endettement de certaines entreprises ayant un monopole dans le secteur des télécommunications.

N'y a-t-il pas un risque élevé de pousser des entreprises vers la faillite s'il n'y a pas de clause d'indemnisation? Est-ce que le ministère pense à une autre forme de compensation financière ou d'aide, de façon à éviter de nuire à la survie de ces entreprises pour une question de cybersécurité?

M. Arbour : Merci de la question.

Je vous donne un exemple. Dans le contexte de la réglementation du secteur des télécommunications, l'impact des règles, dans l'attribution des licences du spectre, a un impact

on a regular basis, and it's essential to take this into consideration.

For high-risk equipment, the deadlines we set are based on networks' procurement cycles. For example, the cut-off date for 4G equipment is 2027. We'll also be consulting on the drafting of an order for this bill, for this type of impact to be taken into consideration. The aim is to have reliable, yet available, telecommunications services. So, we're already used to operational considerations. To be clearer, there are specific requirements in the bill.

No one is currently entitled to compensation. However, we're not opposed to the idea. If the government wishes to include it in the budget and provide grants to replace equipment, the option would exist, but no one is entitled to this type of compensation at the moment.

Senator Carignan: In the case of industry, businesses, telecommunications companies, cell towers, for example, equipment is approved by Innovation, Science and Economic Development Canada and your department ensures compliance. It's a bit odd that you'd allow a part, which then ends up in the equipment, and two years later, when everything is installed, you say you're removing it without compensation. That's a bit odd.

Mr. Arbour: The impact on industry of any order or regulation taken in the current Telecommunications Act or in the Radiocommunication Act regarding spectrum management is critical. We have a variety of objectives. It's not just about security issues; it's also about increasing access to services in rural and remote areas and increasing competition. For example, with alternative or smaller service providers, there are incentives for the department to take these risks into consideration. To make the House process run more smoothly, amendments were brought so these considerations would be explicit in the bill. This is something that we've been doing for a long time.

[*English*]

Senator Dasko: I will be very brief. I had asked the ministers about sanctions, penalties and remedies in the bill. Obviously, there is mandatory incident reporting, and there are administrative penalties if these are not achieved, but these are for the domestic companies. When it comes to the perpetrators — foreign actors, state actors — does the bill have penalties and sanctions for the perpetrators of these crimes,

énorme sur la capacité d'offrir les services sans fil. Nous constatons l'impact sur les fournisseurs de services régulièrement, et c'est essentiel de le prendre en considération.

Dans le contexte d'équipements à risque élevé, nous avons développé les dates limites qui correspondent au cycle de l'approvisionnement dans les réseaux. Par exemple, la date limite pour ce qui est de l'équipement 4G sera 2027. Nous allons également consulter pour la conception d'un décret sur ce projet de loi, pour pouvoir prendre en considération ce type d'impact. L'objectif est d'avoir des services de télécommunications fiables, mais disponibles. Nous sommes donc déjà habitués à des considérations d'ordre opérationnel. Pour être plus clair, pour avoir plus de confort, il y a des exigences spécifiques dans le projet de loi.

En ce qui concerne la possibilité de compensation ou d'indemnisation, personne n'y a droit. Toutefois, nous ne sommes pas fermés à l'idée. Si le gouvernement souhaite mettre en œuvre un programme dans le budget et subventionner le remplacement d'équipements, cette possibilité existe, mais personne n'a droit à ce type de compensation pour l'instant.

Le sénateur Carignan : Dans le cadre d'industries, de commerces, d'entreprises de télécommunications, de tours de cellulaires, par exemple, tout l'équipement est autorisé par Innovation, Sciences et Développement économique Canada et passe par votre ministère pour assurer la conformité. Cela est donc un peu particulier que vous autorisiez la pièce, qui se retrouve ensuite dans l'équipement, et deux ans plus tard, quand tout est installé, vous dites que vous l'enlevez sans indemnisation. C'est un peu particulier.

M. Arbour : Avec chaque décret ou règle dans la Loi sur les télécommunications actuelle ou la Loi sur la radiocommunication qui traite de la gestion du spectre, l'impact sur l'industrie est une situation très importante. Nous avons une variété d'objectifs. Il ne s'agit pas seulement de questions de sécurité; il s'agit aussi d'augmenter l'accès aux services dans les zones rurales et éloignées et d'augmenter la concurrence. Par exemple, avec les fournisseurs de services alternatifs ou plus petits, il existe des incitatifs pour que le ministère prenne ces risques en considération, mais pour avoir plus de confort dans le processus de la Chambre, on a ajouté des modifications pour rendre ces considérations explicites dans le projet de loi précis. C'est une habitude qui est en place depuis longtemps.

[*Traduction*]

La sénatrice Dasko : Je serai très brève. J'avais interrogé les ministres à propos des sanctions, des pénalités et des recours prévus dans le projet de loi. Il est évident que des rapports d'incident obligatoires sont prévus et que des sanctions administratives sont prévues en cas de non-respect de ces obligations, mais elles concernent les entreprises nationales. En ce qui concerne les auteurs de ces crimes — les acteurs étrangers

and/or is it too difficult to do this because of the nature of who they are and the kinds of entities they are?

Mr. Khoury: Thank you, senator, for the question.

If I step back for a second, the perpetrators of these cyber incidents can be —

Senator Dasko: No. They are crimes.

Mr. Khoury: Some of them I would call crimes, and some of them are cyber incidents. We have the state-sponsored actors, and we have publicly named China, Russia, North Korea and Iran as being in the state-sponsored category. We have cybercriminals who are in it for the money, so they are the perpetrators of ransomware attacks or stealing information to then peddle it on the dark web and make money off of it. Often, the cybercriminal organization — or they are almost organizations, the cyber criminals — hide behind protections afforded by countries like Russia, so they are not within the reach of Canadian law. You can't go and serve a warrant for their arrest in Russia.

Having said that, there are a number of tools that the Canadian government has at its disposal, either cooperating with organizations like INTERPOL and others to extend the reach of the prosecution of these perpetrators, or, at the Cyber Centre at CSE, we also have the authorities to conduct cyber operations to impose a cost on these actors.

Senator Dasko: It's retaliation. Sorry.

Mr. Khoury: I call it cyber operations to impose a cost. Either one is a way by which — and also, we shouldn't forget Global Affairs Canada has the diplomatic tools at its disposal to démarche or otherwise if the attribution points in a certain direction. There are a number of tools available, irrespective of Bill C-26, that the government can avail itself to today to impose a cost of some sort.

Senator Dasko: Thank you.

The Chair: Thank you, Mr. Khoury.

Colleagues, this brings us to the end of this evening's meeting. I have the pleasure of thanking officials from Public Safety Canada; Innovation, Science and Economic Development Canada; and the Communications Security Establishment for being with us today. You have been very generous with your time and advice and the provision of information, including

ou étatiques —, le projet de loi prévoit-il des pénalités et des sanctions à leur intention, ou est-il trop difficile de les appliquer en raison de la nature de ces acteurs et du type d'entités qu'ils représentent?

M. Khoury : Je vous remercie de votre question, madame la sénatrice.

Si je prends du recul pendant une seconde, les auteurs de ces incidents cybernétiques peuvent être...

La sénatrice Dasko : Non. Il s'agit de crimes.

M. Khoury : Je qualifierais certains d'entre eux de crimes, et d'autres d'incidents cybernétiques. Il y a les acteurs parrainés par un État, et nous avons publiquement désigné la Chine, la Russie, la Corée du Nord et l'Iran comme faisant partie de la catégorie des États qui parrainent des acteurs. Il y a aussi les cybercriminels qui cherchent à gagner de l'argent, c'est-à-dire ceux qui lancent des attaques de rançongiciel ou qui volent des renseignements afin de les revendre sur le « Web invisible » et d'en tirer profit. Souvent, l'organisation cybercriminelle — ou ce sont presque des organisations de cybercriminels — se cache derrière les protections offertes par des pays comme la Russie, échappant ainsi à la loi canadienne. Il n'est pas possible de lancer un mandat d'arrêt contre eux en Russie.

Cela dit, le gouvernement canadien dispose d'un certain nombre d'outils, qu'il s'agisse de coopérer avec des organisations comme INTERPOL ou d'autres organisations en vue d'étendre la portée des poursuites engagées contre ces auteurs. De plus, le Centre cybernétique du CST a aussi le pouvoir de mener des cyberopérations pour imposer des coûts à ces acteurs.

La sénatrice Dasko : Il s'agit de représailles. Je suis désolée de l'interruption.

M. Khoury : J'appelle cela des cyberopérations pour imposer des coûts. Dans les deux cas, il s'agit d'un moyen... et il ne faut pas oublier non plus qu'Affaires mondiales Canada dispose d'outils diplomatiques pour entreprendre des démarches ou d'autres mesures si l'attribution de la responsabilité pointe dans une certaine direction. Indépendamment du projet de loi C-26, le gouvernement dispose d'un certain nombre d'outils dont il peut se prévaloir à l'heure actuelle pour imposer des coûts d'une sorte ou d'une autre.

La sénatrice Dasko : Je vous remercie de vos réponses.

Le président : Je vous remercie, monsieur Khoury.

Chers collègues, ceci met fin à la réunion de ce soir. J'ai le plaisir de remercier les hauts fonctionnaires de Sécurité publique Canada, d'Innovation, Sciences et Développement économique Canada et du Centre de la sécurité des télécommunications de s'être joints à nous aujourd'hui. Vous nous avez généreusement offert votre temps, vos conseils et vos informations, y compris

those things that we might have asked but didn't. Thank you for going the extra mile there.

You do hugely important work every day on behalf of us in this room and Canadians. We ask a lot of you, and you operate in an area that we struggle to keep pace with. You appear to be keeping pace with it. I will say that, having travelled around a bit, the CSE and related agencies have a strong reputation — you know this — among our Five Eyes allies and beyond. We thank you for the important work that you do, and we may have further questions for you as we continue our consideration of the bill.

For the time being, colleagues, our next meeting is Monday, November 4, at 4 p.m. Eastern, here in Room C128 at the Senate of Canada Building. I finish by thanking my colleagues for your questions and interventions and for your time and effort in this regard as we study this important bill.

(The committee adjourned.)

celles que nous aurions pu demander, mais que nous n'avons pas demandées. Je vous remercie d'avoir déployé des efforts supplémentaires.

Vous accomplissez chaque jour un travail extrêmement important pour nous, qui siégeons dans la salle, et pour les Canadiens. Nous exigeons beaucoup de vous, et vous travaillez dans un domaine que nous avons du mal à suivre. Cependant, vous semblez ne pas vous laisser distancer. Pour avoir voyagé un peu, je dirais que le CST et les organismes connexes jouissent d'une solide réputation — vous le savez — auprès de nos alliés du Groupe des cinq et au-delà. Nous vous remercions du travail important que vous accomplissez, et nous aurons peut-être d'autres questions à vous poser au cours de la continuation de notre étude du projet de loi.

Pour l'instant, chers collègues, notre prochaine réunion aura lieu le lundi 4 novembre, à 16 heures, heure de l'Est, ici, dans la salle C128 de l'édifice du Sénat du Canada. Je termine en remerciant mes collègues de leurs questions et de leurs interventions, ainsi que du temps et des efforts qu'ils ont consacrés à l'étude de cet important projet de loi.

(La séance est levée.)