EVIDENCE

OTTAWA, Monday, May 25, 2026

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

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

[*English*]

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

I am Marty Deacon, senator from Ontario and chair of this committee. Just before I go to introductions, I want to welcome everyone back today and remind you that this is a pretty stimulating week for defence in Ottawa. I don't know where to start — awards and recognition, people who we are seeing over and over at different events, the Quantum event at the War Museum, CANSEC and defence awards tonight. In honour of our guests, I want to acknowledge that the work matters, and our schedules are full. We have a car going tomorrow morning to view the drone demos, then on Thursday for another session. I know that some of you will be there. I look forward to seeing you there.

Before proceeding to our witnesses today, I would like to offer my colleagues the opportunity to introduce themselves.

Senator Al Zaibak: Mohammad Al Zaibak, senator for Ontario.

Senator Ross: Krista Ross, senator from New Brunswick.

Senator White: Judy White, senator from Newfoundland and Labrador.

Senator Hay: Katherine Hay, Ontario.

[*Translation*]

Senator Youance: Suze Youance from Quebec.

[*English*]

Senator Patterson: Rebecca Patterson, Ontario.

Senator Cardozo: Andrew Cardozo, Ontario.

TÉMOIGNAGES

OTTAWA, le lundi 25 mai 2026

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

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

[*Traduction*]

La présidente : Honorables sénateurs, bienvenue à cette séance du Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants.

Je m'appelle Marty Deacon, sénatrice de l'Ontario et présidente de ce comité. Avant de passer aux présentations, je tiens à souhaiter à nouveau la bienvenue à tout le monde aujourd'hui et à vous rappeler que cette semaine est particulièrement riche en événements dans le domaine de la défense à Ottawa. Je ne sais pas par où commencer entre les remises de prix et les hommages, les différentes manifestations qui nous donnent l'occasion de nous rencontrer, l'événement Quantum au Musée de la guerre, le CANSEC et la cérémonie des prix de la défense ce soir. En l'honneur de nos invités, je tiens à souligner l'importance de ce travail et à rappeler que nos agendas sont bien remplis. Un transport sera offert demain matin pour assister aux démonstrations de drones, et une nouvelle fois jeudi. Je sais que certains d'entre vous seront présents. J'ai hâte de vous y voir.

Avant de passer à l'audition de nos témoins aujourd'hui, je vais demander à mes collègues de bien vouloir se présenter.

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

La sénatrice Ross : Krista Ross, sénatrice du Nouveau-Brunswick.

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

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

[*Français*]

La sénatrice Youance : Suze Youance, du Québec.

[*Traduction*]

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

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

Senator Boehm: Peter Boehm, Ontario.

Senator McNair: John McNair, New Brunswick. Welcome.

[*Translation*]

Senator Carignan: Claude Carignan from Quebec.

[*English*]

The Chair: Thank you. I'd like to welcome Senator Boehm, who is joining us today as we bid farewell to Senator Kutcher during our last session. Thank you, Senator Boehm, for joining us today.

Today, we continue our consideration of Bill C-8, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts. We have the pleasure of welcoming four panels of witnesses today, with representation from business, research entities, law firms and non-governmental organizations. We have a full evening ahead of us.

For our first panel this evening, we are pleased to welcome John de Boer, Vice President, Government Relations, BlackBerry; David Shipley, Chief Executive Officer, Beauceron Security Inc.; and Philip Stupak, Senior Director, ISC2. Thank you all for joining us today and taking the time to be here. Your work certainly matters.

We will begin by inviting you to provide your opening remarks, which will be followed by questions from our members. I remind you that you each have five minutes for opening remarks. We will begin with John de Boer. Please proceed when you are ready.

John de Boer, Vice President, Government Relations, BlackBerry: Thank you, chair.

When Canadians board a train, turn on the lights, access their bank accounts or communicate during an emergency, they trust these systems will work securely and without interruption. That trust is what BlackBerry delivers every day.

Our QNX operating system is embedded in over 275 million vehicles and runs within energy grids, transportation systems and industrial environments where failure is not an option. We also secure the communications governments rely on during a crisis, ensuring decisions can be made safely when seconds matter most. In these environments, cybersecurity is not theoretical. It is about keeping systems operational when they are under pressure.

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

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

[*Français*]

Le sénateur Carignan : Claude Carignan, du Québec.

[*Traduction*]

La présidente : Merci. Je voudrais souhaiter la bienvenue au sénateur Boehm, qui se joint à nous aujourd'hui en remplacement du sénateur Kutcher, à qui nous avons fait nos adieux lors de notre dernière séance. Merci, sénateur Boehm, d'être parmi nous aujourd'hui.

Nous poursuivons aujourd'hui l'examen du projet de loi C-8, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois. Nous avons le plaisir d'accueillir aujourd'hui quatre groupes de témoins, qui représentent le monde des affaires, des organismes de recherche, des cabinets d'avocats et des organisations non gouvernementales. Une soirée bien remplie nous attend.

Dans notre premier groupe de témoins ce soir, nous avons le plaisir d'accueillir John de Boer, vice-président, Relations gouvernementales, chez BlackBerry; David Shipley, directeur général de Beauceron Security Inc.; et Philip Stupak, directeur principal chez ISC2. Merci à vous tous d'avoir pris le temps de vous joindre à nous aujourd'hui. Votre présence est très importante.

Vous êtes d'abord invités à prononcer votre allocution d'ouverture, qui sera suivie des questions des sénateurs. Je vous rappelle que vous disposez chacun de cinq minutes pour votre déclaration liminaire. La parole ira d'abord à John de Boer. Vous pouvez commencer dès que vous êtes prêt.

John de Boer, vice-président, Relations gouvernementales, BlackBerry : Merci, madame la présidente.

Lorsque les Canadiens montent à bord d'un train, allument la lumière, consultent leur compte bancaire ou communiquent entre eux pendant une situation d'urgence, ils ont confiance que les systèmes qu'ils utilisent fonctionneront en toute sécurité et sans interruption. C'est cette confiance que BlackBerry leur apporte chaque jour.

Notre système d'exploitation QNX est intégré à plus de 275 millions de véhicules et fonctionne au sein de réseaux électriques, de systèmes de transport et d'environnements industriels, où la moindre défaillance est inacceptable. Nous assurons également la sûreté des communications sur lesquelles les gouvernements s'appuient en cas de crise, garantissant ainsi que des décisions puissent être prises en toute sécurité lorsque

This is why Bill C-8 matters and why BlackBerry strongly supports its passage.

Canada is behind its peers. Every other G7 country has implemented baseline cybersecurity requirements and mandatory cyber incident reporting for critical infrastructure. At the same time, threats are accelerating, becoming more sophisticated and increasingly focused on disrupting operations, not just stealing data.

We are operating in a world that is less stable, more contested and far less predictable than even a few years ago. As a result, long-held assumptions about efficiency and global sourcing are being re-examined. Decision makers are asking more fundamental questions: Who controls the technology? Where does it run? How is data handled? Will it work when systems are disrupted?

In this environment, trust, resilience and operational control are essential.

Bill C-8 targets four critical sectors — energy, transportation, finance and telecommunications — all of which are increasingly digital, interconnected and exposed to cascading risk.

These risks are evolving. The emergence of post-quantum threats means adversaries are already collecting encrypted data today for future decryption. Without action, sensitive systems risk being exposed retroactively, making it essential that our approach be not only secure today, but future-proof.

Cybersecurity is not just about prevention. It is also about maintaining operations during an incident. We have seen that when coordination breaks down, the impact of an attack worsens significantly. This points to a critical gap with respect to the ability to communicate and coordinate securely in real time.

To that end, Bill C-8 should reinforce continuity of operations; secure, real-time coordination; and the ability to restore services quickly under pressure. Governments, including Canada, are placing increasing emphasis on trusted, sovereign solutions.

chaque seconde compte. Dans ces environnements, la cybersécurité n'est pas une notion théorique. Elle consiste à maintenir l'opérationnalité des systèmes lorsqu'ils sont soumis à des pressions extrêmes.

C'est pour cette raison que le projet de loi C-8 revêt une telle importance et que BlackBerry soutient fermement son adoption.

Le Canada tire de l'arrière par rapport à ses homologues. Tous les autres pays du G7 ont mis en place des exigences de base en matière de cybersécurité et une obligation de signalement des incidents de cybersécurité pour les infrastructures essentielles. Parallèlement, les menaces s'intensifient, gagnent en sophistication et visent de plus en plus à perturber les opérations, et non plus seulement à voler des données.

Nous évoluons dans un monde moins stable, plus contesté et bien moins prévisible qu'il y a encore quelques années. En conséquence, les idées reçues de longue date concernant l'efficacité et l'approvisionnement mondial sont remises en question. Les décideurs se posent des questions plus fondamentales : qui contrôle la technologie? Où est-elle exploitée? Comment les données sont-elles traitées? Fonctionnera-t-elle en cas de perturbation des systèmes?

Dans cet environnement, la confiance, la résilience et le contrôle opérationnel sont essentiels.

Le projet de loi C-8 vise quatre secteurs clés — l'énergie, les transports, les finances et les télécommunications — qui sont tous de plus en plus numériques, interconnectés et exposés à des risques en cascade.

Ces risques évoluent. L'émergence de menaces post-quantiques signifie que des acteurs malveillants collectent déjà des données chiffrées, en vue de leur déchiffrement futur. Si aucune mesure n'est prise, des systèmes sensibles risquent d'être exposés rétroactivement. Il est donc essentiel que notre approche soit non seulement sécuritaire aujourd'hui, mais qu'elle résiste aussi à l'épreuve du temps.

La cybersécurité ne se limite pas à la prévention. Elle consiste également à maintenir les opérations pendant un incident. Nous avons constaté que lorsque la coordination fait défaut, l'impact d'une attaque est considérablement plus grave. Cela fait ressortir une lacune majeure en matière de capacité à communiquer et à se coordonner en toute sécurité et en temps réel.

Dans ce contexte, le projet de loi C-8 devrait renforcer la continuité des activités, garantir une coordination en temps réel et permettre de rétablir rapidement les services en situation de crise. Les gouvernements, y compris celui du Canada, accordent de plus en plus d'importance à des solutions fiables et souveraines.

This reflects a simple reality: Security cannot be separated from trust and control, and systems must function reliably when it matters most.

The same applies across critical infrastructure sectors. Technologies that are security first, independently certified, and deployable in high-assurance environments are essential to long-term resilience.

To strengthen Bill C-8, there are a few practical elements to consider. First, we need clear and consistent definitions of what constitutes a reportable incident. Second, reporting needs to be timely, with a structured, tiered approach for reporting. Third, organizations must have access to secure communications tools so they can coordinate effectively during an incident. Finally, the bill should reinforce continuity of operations and be flexible enough to adapt to evolving threats.

Bill C-8 is a necessary step forward for Canada. It aligns Canada with our allies and strengthens our resilience in a more complex threat environment.

Most importantly, it helps ensure our critical infrastructure can continue to function when it matters most. Thank you.

The Chair: Thank you, Mr. de Boer.

David Shipley, Chief Executive Officer, Beauceron Security Inc.: Thank you, Madam Chair.

Senators, thank you for having me. My name is David Shipley. I'm the CEO and co-founder of Beauceron Security, which is based in Fredericton, New Brunswick. I have worked in cybersecurity for 14 years. I am a Certified Information Security Manager and a public interest technologist. I have been researching, writing and speaking about critical infrastructure cybersecurity for the past nine years. I have testified on cybersecurity policy before, including on Bill C-26, the predecessor to this proposed legislation.

I'm here to say one thing plainly and clearly: Pass Bill C-8.

It isn't perfect, but it is good enough to help protect Canadians from real harm and to help us effectively respond when things go wrong.

The improvements over Bill C-26 are real: a narrower definition of the threats that can trigger government orders, the removal of confidential court submissions, a five-year statutory

Cela reflète une réalité simple : la sécurité ne peut être dissociée de la confiance et du contrôle, et les systèmes doivent fonctionner de manière fiable lorsque cela compte le plus.

Il en va de même pour tous les secteurs d'infrastructures essentielles. Les technologies qui accordent la priorité à la sécurité, qui sont certifiées par des organismes indépendants et qui peuvent être déployées dans des environnements extrêmement sûrs sont essentielles à la résilience à long terme.

Pour renforcer le projet de loi C-8, il convient de prendre en compte plusieurs aspects pratiques. Premièrement, il faut établir des définitions claires et cohérentes de ce qui constitue un incident à signaler. Deuxièmement, les signalements doivent être effectués en temps opportun, selon une approche structurée et à plusieurs niveaux. Troisièmement, les organisations doivent disposer d'outils de communication sécurisés, afin de pouvoir se coordonner efficacement en cas d'incident. Enfin, le projet de loi devrait renforcer la continuité des activités et être suffisamment souple pour s'adapter à l'évolution des menaces.

Le projet de loi C-8 constitue une avancée indispensable pour le Canada. Il permet au pays de s'aligner sur ses alliés et de renforcer sa résilience dans un environnement de menaces de plus en plus complexes.

Qui plus est, il permet de garantir que nos infrastructures essentielles pourront continuer à fonctionner lorsque cela est le plus important. Merci.

La présidente : Merci, monsieur de Boer.

David Shipley, directeur général, Beauceron Security Inc. : Merci, madame la présidente.

Honorables sénateurs, merci de m'accueillir parmi vous. Je m'appelle David Shipley. Je suis le directeur général et le cofondateur de Beauceron Security, une entreprise basée à Fredericton, au Nouveau-Brunswick. Je travaille dans le domaine de la cybersécurité depuis 14 ans. Je suis un gestionnaire certifié de la sécurité de l'information et un technologue d'intérêt public. Depuis neuf ans, je mène des recherches, je rédige des articles et je donne des conférences sur la cybersécurité des infrastructures essentielles. J'ai déjà témoigné sur la politique en matière de cybersécurité, notamment au sujet du projet de loi C-26, qui a précédé le projet de loi proposé aujourd'hui.

Je suis ici pour affirmer catégoriquement qu'il faut adopter le projet de loi C-8.

Il n'est pas parfait, mais il est suffisant pour protéger les Canadiens contre des dangers réels et pour nous permettre d'intervenir efficacement lorsque les choses tournent mal.

Les améliorations apportées par rapport au projet de loi C-26 sont réelles : une définition plus restrictive des menaces pouvant donner lieu à des décrets gouvernementaux, la suppression des

ministerial review and improved clarity that helps protect encryption.

Many of the remaining flaws can be dealt with in regulation. There are two specifically I want to talk about.

First, as my colleague noted, we must define “incident” with precision. Without that, we risk losing valuable insights in a cacophony of reporting. Second, personal liability must follow decision-making authority.

CEOs and CFOs set budgets and risk tolerance. Chief information security officers, or CISOs, do not. As drafted, this bill risks scapegoating the people charged with raising the alarm, while the people who set the spending and risk appetite may not face the appropriate consequences. That will simply cause experienced CISOs in the sectors where we need them most to choose to move to a new sector or, more likely, leave the field altogether.

There have been well-intentioned objections to Bill C-8 from various groups on privacy grounds. I believe the updates from Bill C-26 have gone a significant way to address many of them. Some may still feel otherwise.

However, the idea that Canadians’ data may be caught up in a Bill C-8-related incident filing is truly incidental. While we debate the potential risks of edge cases, criminals and nation-states are deciding whether Canadians get timely, lifesaving health care or safe access to drinking water.

The place we need to have the privacy fight right now is around Bill C-22, should it make its way here without fixing massive fundamental flaws.

So, I support Bill C-8, and not just because Canada is the last G7 country to pass this kind of legislation but because we need to move beyond these bare-bones basics and onto discussions and debates about the role of our national government and our agencies in protecting the other critical infrastructure this bill completely ignores: infrastructure under active threat.

Bill C-8 covers banks, telecommunications, energy transmission and transportation.

mémoires confidentiels présentés aux tribunaux, un examen ministériel prévu par la loi tous les cinq ans et une plus grande clarté qui contribue à protéger le chiffrement.

Bon nombre des lacunes restantes peuvent être comblées par la réglementation. Il y en a deux en particulier dont je voudrais parler.

Premièrement, comme l’a souligné mon collègue, nous devons définir avec précision la notion d’« incident ». Autrement, nous risquons de passer à côté d’informations précieuses dans la confusion d’un signalement. Deuxièmement, la responsabilité personnelle doit découler du pouvoir décisionnel.

Ce sont les PDG et les directeurs financiers qui fixent les budgets et la tolérance au risque. Ce n’est pas le cas des responsables de la sécurité de l’information. Dans sa forme actuelle, ce projet de loi risque de faire porter le chapeau à ceux qui ont pour mission de tirer la sonnette d’alarme, tandis que ceux qui décident des dépenses et de l’appétit pour le risque pourraient ne pas subir les conséquences qui s’imposent. Cela ne fera qu’inciter les responsables de la sécurité de l’information expérimentés, dans les secteurs où nous avons le plus besoin d’eux, à changer de secteur ou, plus probablement, à quitter définitivement la profession.

Divers groupes ont émis des objections bien intentionnées à l’égard du projet de loi C-8, pour des raisons liées à la protection de la vie privée. Je pense que les mises à jour apportées par rapport au projet de loi C-26 ont largement contribué à y répondre. Certains pourraient toutefois ne pas partager cet avis.

Cependant, l’idée que les données des Canadiens puissent être concernées par un signalement lié au projet de loi C-8 est tout à fait accessoire. Alors que nous débattons des risques potentiels liés à des cas limite, des criminels et des États-nations décident si les Canadiens bénéficieront de soins de santé rapides et vitaux ou d’un accès sûr à l’eau potable.

C’est autour du projet de loi C-22 que nous devons mener la bataille pour la protection de la vie privée dès maintenant, s’il venait à être présenté ici sans que ses graves lacunes fondamentales aient été corrigées.

J’appuie donc le projet de loi C-8, non seulement parce que le Canada est le dernier pays du G7 à adopter ce type de législation, mais aussi parce que nous devons aller au-delà des mesures minimales et engager des discussions et des débats sur le rôle de notre gouvernement national et de nos organismes dans la protection des autres infrastructures essentielles que ce projet de loi laisse complètement de côté : les infrastructures qui font l’objet de menaces réelles.

Le projet de loi C-8 concerne les banques, les télécommunications, le transport d’énergie et les transports.

Bluntly, the banks were already well motivated and well regulated prior to this legislation. They are not even remotely my biggest concern. The telecommunications sector at the national level was, on the whole, well prepared and had voluntarily aligned closely with ISED through industry-government collaboration. Energy transmission, specifically pipelines and electrical assets not covered by the North American Electric Reliability Corporation and its regional subsidiaries, is a real concern. Transportation is likely the worst off of the four.

However, those four areas, and any providers closely linked to them, are not nearly enough when it comes to talking about what is truly critical infrastructure.

Let's start with Canadian health care: Newfoundland in 2021, southwestern Ontario in 2023 and many more we never heard about. South of the border, we see much more, and it's bad.

On April 6, Brockton Hospital in Massachusetts sent chemotherapy patients home and diverted ambulances after ransomware took down its systems. Since 2016, peer-reviewed research has documented more than 150 ransomware attacks on U.S. health care facilities that disrupted patient care.

Make no mistake: Canadians have likely died or had their lifespans shortened because of cyberattacks.

Researchers at the University of Minnesota School of Public Health found that ransomware attacks decrease hospitals' ability to handle patient volume by 17% to 24% during the first week of an attack, with recovery taking up to three weeks. Among patients already admitted when an attack begins, in-hospital mortality rises by 34% to 38%.

The same researchers estimate that translates to between 42 and 67 Medicare patient deaths attributable to the impacts of ransomware between 2016 and 2021.

We need to stop hiding behind constitutional jurisdiction lines that were decided before the internet was popularized and get serious about organizing as a country with respect to this national security threat.

Je dirais sans détour que les banques étaient déjà très motivées et bien réglementées avant l'adoption de cette législation. Elles viennent très loin dans mes préoccupations. Au niveau national, le secteur des télécommunications était, dans l'ensemble, bien préparé et s'était volontairement aligné étroitement sur les directives d'Innovation, Sciences et Développement économique, dans le cadre d'une collaboration entre l'industrie et le gouvernement. Le transport d'énergie, en particulier les pipelines et les infrastructures électriques non couverts par la North American Electric Reliability Corporation et ses filiales régionales, constitue une réelle préoccupation. Parmi les quatre secteurs, celui des transports est vraisemblablement le plus mal loti.

Cependant, ces quatre secteurs, ainsi que les fournisseurs qui y sont étroitement liés, sont loin d'être suffisants lorsqu'il s'agit de définir ce qu'est véritablement une infrastructure essentielle.

Commençons par le système de santé canadien : Terre-Neuve en 2021, le sud-ouest de l'Ontario en 2023, et bien d'autres cas dont nous n'avons jamais entendu parler. Au sud de la frontière, la situation est bien pire.

Le 6 avril, l'hôpital de Brockton, dans le Massachusetts, a renvoyé chez eux des patients sous chimiothérapie et a redirigé les ambulances après qu'un rançongiciel a paralysé ses systèmes. Depuis 2016, dans le cadre des travaux de recherche évaluée par les pairs, on a recensé plus de 150 attaques par rançongiciel contre des établissements de santé américains, qui ont provoqué une perturbation de la prise en charge des patients.

Ne vous y trompez pas : des Canadiens ont vraisemblablement perdu la vie ou vu leur espérance de vie raccourcie à cause de cyberattaques.

Des chercheurs de l'École de santé publique de l'Université du Minnesota ont constaté que les attaques par rançongiciel réduisaient de 17 à 24 % la capacité des hôpitaux à prendre en charge des patients au cours de la première semaine suivant l'attaque, le rétablissement pouvant prendre jusqu'à trois semaines. Parmi les patients déjà hospitalisés au moment de l'attaque, la mortalité intra-hospitalière augmente entre 34 et 38 %.

Ces mêmes chercheurs estiment que cela correspond à un nombre de décès de patients couverts par le régime d'assurance-maladie compris entre 42 et 67, imputables aux conséquences des attaques par rançongiciel entre 2016 et 2021.

Nous devons cesser de nous retrancher derrière des limites de compétence constitutionnelles qui ont été établies avant la généralisation d'Internet et nous atteler sérieusement, en tant que pays, à nous organiser face à cette menace pour la sécurité nationale.

Now let's talk about water. This month, Dragos, a cybersecurity firm, published findings on an intrusion at a water utility serving Monterrey, Mexico's third-largest city —

The Chair: Thank you, Mr. Shipley. We can incorporate that into the question period.

Mr. Shipley: Sure.

The Chair: Thank you.

Philip Stupak, Senior Director, ISC2: Good afternoon, Madam Chair and members of the committee. Thank you for the opportunity to appear before you today. My name is Philip Stupak, and I serve as Senior Director of Advocacy at ISC2, the membership association for cybersecurity professionals. Prior to joining ISC2, I had the privilege of serving in the Biden-Harris administration as the Assistant National Cyber Director at the White House.

ISC2 is the world's largest association dedicated to cybersecurity professionals, representing more than 265,000 members globally. Our third-largest membership base is here in Canada, where we have over 14,800 members. We offer nine professional certifications, the most recognized of which is Certified Information Systems Security Professional, or CISSP. It is widely regarded by employers as the gold standard for cybersecurity expertise.

I appear today on behalf of that global membership to express the cybersecurity profession's strong support for Bill C-8, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts.

We live in an era of great contrasts. Our technology affords us a level of connectivity our forbears never could have imagined; our digital assets also enable foreign actors to shut off the power without ever setting foot on North American soil. At no other time in history have we been able to share information so fast nor have our schools been so easily shuttered by a thief a world away. It is a world of impressive capabilities, endless possibilities and dizzying vulnerabilities.

Not too long ago, using that same connectivity, the People's Republic of China, or PRC, exploited one of those vulnerabilities to infiltrate telecommunications companies around the world.

Parlons maintenant de l'eau. Ce mois-ci, Dragos, une société spécialisée dans la cybersécurité, a publié les conclusions d'une enquête sur une intrusion au sein d'un service des eaux desservant Monterrey, la troisième plus grande ville du Mexique…

La présidente : Merci, monsieur Shipley. Nous pourrons aborder cela pendant la période des questions.

M. Shipley : Bien sûr.

La présidente : Merci.

Philip Stupak, directeur principal, ISC2 : Bonjour, madame la présidente et honorables sénateurs. Je vous remercie de me donner l'occasion de m'adresser à vous aujourd'hui. Je m'appelle Philip Stupak et j'occupe le poste de directeur principal de la défense des droits au sein de l'ISC2, l'association professionnelle des spécialistes de la cybersécurité. Avant de rejoindre l'ISC2, j'ai eu le privilège de servir au sein de l'administration Biden-Harris, en tant que directeur adjoint de la cybersécurité nationale à la Maison-Blanche.

L'ISC2 est la plus grande association mondiale dédiée aux professionnels de la cybersécurité, et elle représente plus de 265 000 membres à travers le monde. C'est ici, au Canada, que nous comptons notre troisième plus grande base d'adhérents, avec plus de 14 800 membres. Nous proposons neuf attestations professionnelles, dont la plus reconnue est celle de professionnel certifié en sécurité des systèmes d'information, qui est considérée dans une large mesure comme l'étalon de référence en matière d'expertise en cybersécurité par les employeurs.

Je m'adresse à vous aujourd'hui au nom de l'ensemble de nos membres à travers le monde, afin d'exprimer le soutien sans réserve de la profession de la cybersécurité au projet de loi C-8, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois.

Nous vivons à une époque de grands contrastes. La technologie dont nous disposons nous offre un niveau de connectivité que nos ancêtres n'auraient jamais pu imaginer, mais nos actifs numériques font également en sorte que des acteurs étrangers sont en mesure de couper l'électricité, sans même avoir mis les pieds sur le sol nord-américain. À aucun autre moment de l'histoire, nous n'avons été capables de partager des informations aussi rapidement, et jamais auparavant nos écoles n'ont pu être mises à l'arrêt aussi facilement par un pirate informatique situé à l'autre bout du monde. C'est un monde aux capacités impressionnantes, aux possibilités infinies et aux vulnérabilités vertigineuses.

Il n'y a pas si longtemps, la République populaire de Chine a exploité l'une de ces failles pour infiltrer des entreprises de télécommunications à travers le monde, en tirant parti de cette même connectivité.

Simultaneously, they began pre-positioning digital assets — that's a polite way of saying weapons — within civilian critical infrastructure. This is Salt Typhoon and Volt Typhoon.

This is why the most recent National Cyber Threat Assessment highlighted that the PRC's expansive and aggressive cyber program presents the most sophisticated and active state cyber-threat to Canada today.

The PRC is not alone. Threat actors around the world are trying to disrupt, degrade and interfere with Canada's telecommunications system and everything connected to it. ISC2's 14,800 Canadian members are trying to stop them. Our members keep us safe and secure in our shared online environments. They also ensure that we have power for surgeries, water for drinking, gas for driving and heat for living.

The bill before you sends two unambiguous messages: First, to our shared adversaries, pre-positioning cyber weapons in civilian critical infrastructure will not be tolerated. Second, to all of Canada's cyber defenders, you are not alone. The Canadian government will answer the call to help you keep us safe.

By passing Bill C-8, you are meeting this moment of heightened uncertainty and protecting Canadians against the next threat.

My experience has afforded me the understanding that the arduous and slow process of passing cyber legislation means we need to respond to both the crisis of the moment and the unknown ones of the next 20 years. Bill C-8 provides the flexibility to adapt as the digital world evolves. This flexibility matters. It enables Canadians to defend against the threats and adversaries of today and tomorrow.

Bill C-8 also maximizes Canadians' privacy rights. The Canadian Centre for Cyber Security has a long operational history of simultaneously protecting Canadians' security and their privacy. They know how to do this, and they do it well.

The biggest, most persistent threat to privacy comes not from the Canadian government but from all the governments Canadians do not elect. Foreign adversaries can exploit vulnerabilities to gain access to your calls, emails and text messages. Bill C-8 shuts down that privacy violation by giving the government the tools it needs to secure the telecommunications sector, and it does so by expressly adding privacy-enhancing language to this security bill.

Parallèlement, elle a commencé à prépositionner des actifs numériques — une façon polie de parler d'armes — au sein d'infrastructures civiles essentielles, dans le cadre des opérations Salt Typhoon et Volt Typhoon.

C'est pourquoi, lors de la plus récente Évaluation des cybermenaces nationales, on a souligné que le programme cybernétique étendu et agressif de la République populaire de Chine constitue aujourd'hui la cybermenace étatique la plus sophistiquée et la plus active à laquelle le Canada est confronté.

La République populaire de Chine n'est pas seule. Des acteurs malveillants du monde entier tentent de perturber et de dégrader le système de télécommunications canadien et tout ce qui y est connecté, ou de s'y immiscer. Les 14 800 membres canadiens de l'ISC2 s'efforcent de les en empêcher. Nos membres assurent notre sécurité dans les environnements numériques que nous partageons. Ils s'assurent aussi que nous avons l'électricité nécessaire pour les chirurgies, de l'eau potable, de l'essence pour nos déplacements et du chauffage pour vivre confortablement.

Le projet de loi qui vous est soumis envoie deux messages sans équivoque, c'est-à-dire à nos adversaires communs d'abord, à savoir que le prépositionnement d'armes cybernétiques dans les infrastructures civiles essentielles ne sera pas toléré, et à tous ceux qui assurent la cyberdéfense du Canada ensuite, à savoir qu'ils ne sont pas seuls et que le gouvernement canadien répondra à leur appel pour vous aider à assurer notre sécurité.

En adoptant le projet de loi C-8, vous réagissez à cette période d'incertitude accrue et vous protégez les Canadiennes et Canadiens contre la prochaine menace.

Mon expérience m'a permis de comprendre que le processus ardu et lent d'adoption de la législation cybernétique implique que nous devons répondre à la fois à la crise du moment et à celles inconnues des 20 prochaines années. Le projet de loi C-8 offre la souplesse nécessaire pour s'adapter à l'évolution du monde numérique, et cette souplesse est importante. Elle permettra aux Canadiennes et Canadiens de se défendre contre les menaces et les adversaires d'aujourd'hui et de demain.

Le projet de loi C-8 maximise aussi les droits à la vie privée des Canadiennes et Canadiens. Le Centre canadien pour la cybersécurité a une longue expérience opérationnelle de la protection de la sécurité et de la vie privée des Canadiennes et Canadiens. Ses responsables savent quoi faire, et ils le font bien.

La plus grande menace persistante à la vie privée ne vient pas du gouvernement canadien, mais de tous les gouvernements que les Canadiennes et Canadiens n'élisent pas. Des adversaires étrangers peuvent exploiter des failles pour accéder à vos appels, vos courriels et vos messages textes. Le projet de loi C-8 met fin à cette atteinte à la vie privée en donnant au gouvernement les moyens nécessaires pour sécuriser le secteur des télécommunications, et ce, en ajoutant expressément des

Bill C-8 is much more than a compliance or regulatory exercise. This legislation impacts daily life. Yes, Bill C-8 is about critical infrastructure, but it is also about everything that infrastructure enables: how we work; how we stay cool this summer and warm next winter; how we pay our bills; and how we get to work and visit our friends and family. That is what this bill is really about.

Protecting critical infrastructure from cyberattacks protects our way of life. I am proud to lend the voices of ISC2's 265,000 global members in support of Bill C-8. On behalf of our future members, thank you for the flexibility to safeguard that way of life over the next 20 years.

Thank you for your time. I am pleased to answer any questions you may have.

The Chair: Thank you. I'd like to take this moment to welcome Senator Donna Dasko from Ontario. Thank you for joining us.

We will now proceed to questions. Our guests will be here with us until 4:55 p.m. We will do our best to allow time for each member to ask a question during this time. With this in mind, four minutes will be allotted to each question, including the answer, so hopefully we will be able to keep our questions succinct in an effort to get this work done. I would like to offer the first question to our deputy chair, Senator Al Zaibak.

Senator Al Zaibak: Thank you to all of our witnesses today. My first question is directed to you all.

What is the single biggest cyber vulnerability Canada must address immediately if we want to strengthen national resilience against hostile state actors and sophisticated criminal networks?

Mr. de Boer: The biggest vulnerability is a systemic risk, where we have legacy infrastructure that was not meant to be connected to the internet that is now being connected to the internet.

The challenge there is that there are no patches that can be run. There is a rip-and-replace process that needs to happen. That is the legacy infrastructure that covers rail and energy, though not so much banking and telecommunications. As an exporting country, if that breaks down, our entire economy will break down. There will be a lack of public trust, and it will be a national security incident as well.

dispositions favorisant la protection de la vie privée dans ce projet de loi sur la sécurité.

Le projet de loi C-8 est bien plus qu'un simple exercice de conformité ou de réglementation. Cette loi a un impact sur la vie quotidienne. Certes, le projet de loi C-8 porte sur les infrastructures essentielles, mais il concerne aussi tout ce que ces infrastructures rendent possible : notre façon de travailler; comment nous restons frais l'été et au chaud l'hiver; comment nous payons nos factures; et comment nous nous rendons au travail et nous visitons nos amis et notre famille. Voilà ce dont il est réellement question dans ce projet de loi.

La protection des infrastructures essentielles contre les cyberattaques protège notre mode de vie. Je suis fier de porter la voix des 265 000 membres mondiaux de l'ISC2 pour appuyer le projet de loi C-8. Au nom de nos futurs membres, merci de nous offrir la souplesse nécessaire pour protéger ce mode de vie au cours des 20 prochaines années.

Merci de votre temps. Je serai heureux de répondre à toutes vos questions.

La présidente : Merci. Je profite de cette occasion pour souhaiter la bienvenue à la sénatrice Donna Dasko, de l'Ontario. Merci de vous joindre à nous.

Nous allons maintenant passer aux questions. Nos invités resteront avec nous jusqu'à 16 h 55. Nous ferons de notre mieux pour permettre à chaque membre de poser une question durant ce temps. Dans cette optique, quatre minutes seront allouées à chaque question, réponse comprise, afin que nous puissions être succincts et accomplir notre travail. Je cède la parole pour la première question à notre vice-président, le sénateur Al Zaibak.

Le sénateur Al Zaibak : Merci à tous nos témoins aujourd'hui. Ma première question s'adresse à vous tous.

Quelle est la principale vulnérabilité cybernétique que le Canada doit corriger immédiatement pour renforcer la résilience nationale face aux acteurs étatiques hostiles et aux réseaux criminels sophistiqués?

M. de Boer : La principale vulnérabilité est un risque systémique qui est lié aux infrastructures existantes qui n'étaient pas destinées à être connectées à Internet et le sont désormais.

Le problème vient du fait qu'il n'existe aucun correctif à appliquer. Il faut procéder à un remplacement complet. Il s'agit d'infrastructures existantes dans les secteurs ferroviaires et énergétiques, mais pas vraiment dans le secteur bancaire et dans celui des télécommunications. Comme nous sommes un pays exportateur, si cela se détraque, notre économie tout entière s'effondrera. La confiance du public sera ébranlée, et cela constituera aussi un incident de sécurité nationale.

Mr. Shipley: From my perspective, cyber means people in control of technology. The people expect our government to be able to react and act. We are not properly equipped with the laws, tools, experience and practice to respond to what John just said. This legislation gives us some of those tools.

Mr. Stupak: We frequently think about cybersecurity as information security. The challenge is that it is so much more now.

Nation-states and criminals have penetrated the cyber-physical barrier time and again. When you ask me what the biggest vulnerability is, it's water. David was right: It is 100% water.

The difference between where finance and health care are is even greater than between health care and water.

Senator Al Zaibak: Thank you.

Senator Cardozo: Mr. Stupak, I have a couple of questions. Can you say more about water? What do you mean by that?

I sense that Canadians are sometimes more concerned about having privacy from the government than having privacy from other actors. Can you talk about that?

Mr. de Boer, on the question of digital sovereignty, we have very little of that. Most of our infrastructure is in the U.S. Could you talk about what that means for cybersecurity?

Mr. Stupak: First, on water, when I was in the White House, the absolute worst critical infrastructure sector we had for preparedness in cybersecurity was water. It remains water today.

Senator Cardozo: What does that mean?

Mr. Stupak: That means that there are almost no physical protections for cybersecurity within the water sector.

Senator Cardozo: Okay.

Mr. Stupak: Fundamentally, people are unwilling to pay an extra five cents per gallon for cybersecurity protection on their water. We need a movement for that market in order to build out cybersecurity protections within the water sector.

Senator Cardozo: Do you mean somebody poisoning the water?

M. Shipley : De mon point de vue, par cybernétique, on entend les gens qui maîtrisent la technologie. Les citoyens attendent du gouvernement qu'il soit en mesure de réagir et d'agir. Nous ne disposons pas des lois, des outils, de l'expérience et de la pratique adéquats pour réagir face à ce que M. de Boer vient de décrire. Ce projet de loi nous donne certains de ces outils.

M. Stupak : On pense souvent à la cybersécurité comme à la sécurité de l'information. Le problème vient du fait qu'aujourd'hui elle va bien au-delà de cela.

Les États-nations et les criminels ont maintes fois franchi la barrière cyber-physique. Si vous me demandez quelle est la plus grande vulnérabilité, je dirais que c'est l'eau. M. Shipley a raison : c'est sans contredit l'eau.

L'écart entre les secteurs des finances et de la santé est encore plus grand que celui entre la santé et l'eau.

Le sénateur Al Zaibak : Merci.

Le sénateur Cardozo : Monsieur Stupak, j'ai quelques questions. Pouvez-vous nous parler davantage de l'eau? Que voulez-vous dire exactement?

J'ai le sentiment que les Canadiennes et Canadiens sont parfois plus préoccupés par la protection de leur vie privée face au gouvernement que face à d'autres acteurs. Pouvez-vous nous en dire plus à ce sujet?

Monsieur de Boer, pour ce qui est de la souveraineté numérique, nous en avons très peu. La majeure partie de nos infrastructures se trouvent aux États-Unis. Pouvez-vous expliquer ce que cela signifie pour la cybersécurité?

M. Stupak : Tout d'abord, pour ce qui est de l'eau, lorsque j'étais à la Maison-Blanche, le secteur des infrastructures essentielles le moins bien préparé pour la cybersécurité était celui de l'eau. Cela reste vrai aujourd'hui.

Le sénateur Cardozo : Qu'est-ce que cela signifie?

M. Stupak : Cela signifie qu'il n'y a presque aucune protection physique contre les cyberattaques dans le secteur de l'eau.

Le sénateur Cardozo : D'accord.

M. Stupak : Fondamentalement, les gens ne sont pas prêts à payer cinq cents de plus par gallon pour une protection contre les cyberattaques de leur approvisionnement en eau. Il faut que ce marché réagisse, afin de développer des protections cybernétiques dans le secteur de l'eau.

Le sénateur Cardozo : Voulez-vous dire que quelqu'un pourrait empoisonner l'eau?

Mr. Stupak: Absolutely. We have already seen it. Iranian actors were able to breach a water sector in Florida and alter chemical balances.

On the privacy point, this is an excellent point that the United States and Canada share, which is a desire to have greater protection of privacy from government than necessarily businesses or anyone else. I understand that.

I believe this act, at this point, has nine separate protections for privacy, and six of those reinforce the existing law. I think that is adequate protection from government misuse.

But a fundamental point is this: We cannot hamstring government's ability to keep us all safe and keep our data — your data in Canada — away from other foreign actors because of a possibility that one small piece of personally identifiable information, or PII, might be in some record that's shared somewhere. I understand the concern, but I think the bill adequately addresses it.

Mr. de Boer: In terms of digital sovereignty, there are a number of fundamental aspects. The Canadian government is now recognizing what those are: the ability to control infrastructure and data; ensuring the availability of access to that infrastructure; and also accountability when things go wrong.

Canada has not nurtured that infrastructure. It's obviously evolved significantly over the past 10 years. It hasn't nurtured it because the priority was efficiency. The priority was cost efficiency and scale. That has changed. Now governments are realizing we need to control.

Now we can do something about it. We have great Canadian tech companies. We've got emerging investments in satellite and space communications that can help control our telecommunications sector. As well, banking is attuned to this sovereignty question.

You see both industry and government being alive to the issue of ensuring that the data resides in Canada, that the infrastructure actually exists here and that we can control it.

Senator Cardozo: Thank you. Could you say more about that? Is that about having more data centres in Canada? How do we get those companies, which are usually American, to keep their information on Canadian soil?

M. Stupak : Absolument. Cela est déjà arrivé. Des acteurs iraniens ont réussi à infiltrer un réseau d'approvisionnement en eau en Floride et à modifier l'équilibre chimique.

Pour ce qui est de la vie privée, les États-Unis et le Canada ont quelque chose en commun, à savoir la volonté que leur vie privée soit mieux protégée face au gouvernement, que face aux entreprises ou à quiconque d'autre. Je comprends cela.

Je crois que cette loi prévoit à ce jour neuf protections distinctes pour la vie privée, dont six qui renforcent la loi existante. Je pense que c'est une protection adéquate contre les abus gouvernementaux.

Toutefois, il existe un point fondamental : nous ne pouvons pas entraver la capacité du gouvernement à assurer notre sécurité à tous et à protéger nos données — vos données au Canada — contre les acteurs étrangers, simplement à cause de la possibilité qu'un petit élément d'information personnelle identifiable se trouve dans un dossier faisant l'objet d'un partage. Je comprends cette inquiétude, mais je pense que le projet de loi la traite adéquatement.

M. de Boer : Pour ce qui est de la souveraineté numérique, plusieurs aspects fondamentaux sont en jeu. Le gouvernement canadien les reconnaît désormais : la capacité de contrôler les infrastructures et les données, ainsi que de garantir la disponibilité de l'accès à ces infrastructures et la responsabilité en cas de défaillance.

Le Canada n'a pas favorisé le développement de ces infrastructures. Ces dernières ont évidemment beaucoup évolué au cours des dix dernières années, mais elles n'ont pas été développées parce que la priorité était l'efficacité, la réduction des coûts et la portée. Cela a changé. Les gouvernements réalisent maintenant qu'un contrôle est nécessaire.

Nous sommes maintenant en mesure d'agir. Nous avons d'excellentes entreprises technologiques au Canada. Des investissements émergents dans les communications par satellite et dans le domaine spatial peuvent nous aider à maîtriser notre secteur des télécommunications. Le secteur bancaire est lui aussi conscient de cette question de souveraineté.

On voit que l'industrie et le gouvernement sont attentifs à la nécessité de s'assurer que les données demeurent au Canada, que les infrastructures nécessaires sont réellement en place ici, et que nous pouvons en avoir le contrôle.

Le sénateur Cardozo : Merci. Pouvez-vous nous en dire davantage à ce sujet? Voulez-vous dire qu'il faut avoir davantage de centres de données au Canada? Comment peut-on inciter les entreprises, souvent américaines, à conserver leurs informations au Canada?

Mr. de Boer: Yes, it means data centres in Canada. It also means having cloud infrastructure here in Canada, if you're using cloud infrastructure. It also means incentivizing companies to invest in on-premises installations.

It also means being conscious about the kinds of applications we're using. Many of the applications being used to exchange critical information are consumer-grade apps, the texts and voice messages we commonly use. They were not built for government or for critical infrastructure. We need to invest in technologies that were purpose-built for that.

Senator Cardozo: Thank you.

The Chair: Next is Senator McNair, the sponsor of the bill.

Senator McNair: Thank you to the panellists for being here today.

Todd Warnell, Chief Information Security Officer, Bruce Power, stated before this committee on May 4, 2026:

> . . . Bill C-8 is not an end state; it is a foundation. However, in a world defined by greater volatility and uncertainty, establishing that foundation is urgent. The threat environment has evolved faster than our policy framework, and this legislation is an essential step toward closing that gap.

I think I know where you all stand on whether you agree with those comments, but I'm curious if you can expand on the threat environment evolving faster than we thought.

Mr. Shipley: Sure. Starting with AI, what I didn't get a chance to talk about is Monterrey, Mexico, and the first documented AI attack on critical infrastructure. The perpetrators used tools to try to jump from the business network to mess with the water system.

In this case, they were unsuccessful. However, this happened the same week we learned that five water treatment plants in Poland had been compromised by traditional methods, so the gap is closing. That's the speed at which we're seeing it.

John mentioned that we designed these systems way before we ever thought of plugging them into a network. We've plugged them in haphazardly, in a rush, often during the pandemic.

M. de Boer : Oui, cela veut dire des centres de données au Canada. Cela signifie aussi avoir une infrastructure infonuagique ici, au Canada, si c'est une telle infrastructure qui est utilisée. Cela signifie également inciter les entreprises à investir dans des installations sur site.

Cela veut également dire qu'il faut faire attention aux types d'applications que nous utilisons. Nombre des applications utilisées pour échanger des informations critiques sont des applications grand public, les messages textes et les messages vocaux que nous utilisons couramment. Ces applications n'ont pas été conçues pour les gouvernements ni pour les infrastructures essentielles. Nous devons investir dans des technologies spécifiquement conçues à cet effet.

Le sénateur Cardozo : Merci.

La présidente : Nous passons maintenant au sénateur McNair, le promoteur du projet de loi.

Le sénateur McNair : Je remercie les témoins d'être parmi nous aujourd'hui.

Todd Warnell, directeur de la sécurité de l'information chez Bruce Power, disait ceci devant ce comité, le 4 mai 2026 :

> … le projet de loi C-8 n'est pas une fin en soi; c'est une base. Toutefois, dans un monde marqué par une volatilité et une incertitude accrues, il est urgent d'établir cette base. Le contexte des menaces a évolué plus rapidement que notre cadre politique, et ces dispositions législatives sont une étape essentielle pour combler l'écart entre les deux.

Je crois connaître votre position concernant ces commentaires, mais je suis curieux de savoir si vous pouvez nous en dire plus sur l'évolution plus rapide que prévu du contexte des menaces.

M. Shipley : Bien sûr. Pour ce qui est de l'IA, je n'ai pas eu le temps de parler de Monterrey, au Mexique, où a eu lieu la première attaque documentée par IA contre une infrastructure essentielle. Les responsables de cette attaque ont utilisé des outils pour passer par le réseau d'affaires pour perturber l'approvisionnement en eau.

Ils ont échoué dans ce cas, mais cela s'est produit la même semaine où nous avons appris que cinq stations d'épuration en Pologne avaient été compromises par des méthodes classiques. C'est donc dire que l'écart se réduit. Nous pouvons constater à quelle vitesse la situation évolue.

M. de Boer a mentionné que ces systèmes ont été conçus bien avant que l'on envisage de les relier à un réseau, ce que nous avons fait n'importe comment, à la hâte, souvent pendant la pandémie.

Many Canadian municipalities hooked their water systems to the internet so people could remotely manage them from home. Those vulnerabilities were never remediated properly.

We have rushed, ill prepared, into a world that was never designed to be secure, and we have built a house of cards.

Mr. de Boer: Cybersecurity threats thrive on asymmetry, particularly in an interconnected world where all the infrastructure — such as banking infrastructure — depends on electricity or, the weakest link, telecommunications. We often focus on AI, and that is absolutely accelerating the threat. The one after that will be quantum technologies.

But what most people suggest is that we will get 95% there if we do basic cyber hygiene. Todd Warnell's points are so important. We need to get there. Then we can be better placed to deal with the threats that come.

Finally, Philip mentioned Salt Typhoon. There are already pre-positioned threats in our networks. Our Canadian telecommunications networks were also exposed. Metadata, voice communications — all that is in the network today. We must also be able to protect against threats that are already present.

Mr. Stupak: There is a reason why adversaries are targeting water. Yes, it is because of life and limb. We all need water to survive and live.

But the other reason why they are targeting it is this: If you look back to the 20th century, we all competed in steel manufacturing. If you had steel, it meant you had good jobs. You could build buildings and battleships. That was a national security imperative.

Today, it's not steel; it's AI. When we look at the preconditions for AI, they are power and water. You need more data centres for data to stay in Canada. Those shut down without water because they need water for cooling. When an adversary can turn off your data centres at a time and place of their choosing, it means you can be made vulnerable at a time and place of their choosing. That is the evolution of the threat we are seeing: away from information and toward physical, real-life impacts.

Mr. Shipley: Also, we had the first attack against a health care provider in the U.S. as part of the Iran conflict. They didn't ask for a ransom; they just crippled everything in there. They didn't want money. They just wanted to shut the hospital down and to hurt people.

Plusieurs municipalités canadiennes ont relié leurs réseaux d'eau à Internet pour que les usagers puissent les gérer à distance de chez eux. Ces vulnérabilités n'ont jamais été corrigées correctement.

Nous nous sommes précipités, sans préparation, dans un monde qui n'avait pas été conçu pour être sécurisé, et nous avons construit un château de cartes.

M. de Boer : Les menaces cybernétiques tirent parti d'une asymétrie, particulièrement dans un monde interconnecté où toutes les infrastructures — comme celles des banques — dépendent de l'électricité ou, ce qui est leur maillon faible, les télécommunications. Il est souvent question de l'intelligence artificielle, qui accélère indéniablement cette menace. La suivante sera la technologie quantique.

Mais la plupart des gens estiment que 95 % des risques pourraient être évités si l'on appliquait simplement les règles de base de l'hygiène cybernétique. Les propos de Todd Warnell sont très importants. Nous devons y parvenir et nous serons ainsi mieux équipés pour faire face aux menaces à venir.

Enfin, M. Stupak a mentionné Salt Typhoon. Des menaces sont déjà prépositionnées dans nos réseaux. Nos réseaux de télécommunications canadiens ont également été exposés. Les métadonnées, les communications vocales : tout ce qui est présent aujourd'hui dans le réseau. Nous devons également être capables de nous protéger contre ces menaces déjà présentes.

M. Stupak : Si les adversaires prennent l'eau pour cible, c'est qu'il en va de la vie et de l'intégrité physique des personnes. Nous avons tous besoin d'eau pour vivre et survivre.

Il y a une autre raison : au XX^{e} siècle, nous étions tous en concurrence dans la production d'acier. Posséder de l'acier, c'était avoir des emplois de qualité. On pouvait construire des édifices et des cuirassés. C'était un impératif de sécurité nationale.

Aujourd'hui, l'IA a remplacé l'acier. Si on veut avoir des centres d'IA, il faut avoir de l'électricité et de l'eau. Si nous voulons que les données restent au Canada, il nous faut davantage de centres de données. S'il n'y a pas d'eau, les centres ferment, car il faut de l'eau pour les refroidir. Si on peut mettre les centres de données de son adversaire hors service quand et là où on veut, il devient vulnérable quand et où on le veut. C'est là l'évolution de la menace que nous observons. Elle ne porte plus tant sur l'information que sur l'impact physique et concret.

M. Shipley : Par ailleurs, nous avons assisté à la première attaque contre un fournisseur de soins de santé aux États-Unis pendant le conflit avec l'Iran. Les pirates n'ont pas demandé de rançon; ils ont simplement paralysé tout le système. Ils ne voulaient pas d'argent. Ils voulaient simplement mettre l'hôpital à l'arrêt et causer un préjudice aux patients.

Senator McNair: Mr. Shipley, is there anything else you want to add to put on the record about water?

Mr. Shipley: It is not in the scope of this legislation. I am not looking for the Senate to amend the legislation to deal with that. I am looking for us to move beyond this legislation and study the issue.

The United States is ahead of us in health care because they have laws that hold health care accountable through HIPAA. We are not there. We are very much at risk on the health care side and on the water side, and we're not having these conversations because we can't even protect the four areas we have clear jurisdiction over and that we've stumbled on legislation around since 2022.

Senator Ross: My question is for Mr. Shipley. You've made the recommendation loud and clear that we pass Bill C-8 without trying to make any amendments, despite the fact that it may have some flaws that you feel could be fixed in regulations.

However, making observations is a tool that committees have when providing reports back to the Senate. Say you were a member of the National Security, Defence and Veterans Affairs Committee and wanted to add observations to the report to draw attention to a deficiency in this bill. What would be one or two key observations that you would recommend adding to the report that this committee will provide to the Senate?

Mr. Shipley: Specifically, one of the two areas I noted was ensuring that the regulations are as clear as possible as to what exactly an incident is. Some countries' legislation was so unclear that they were drowned out in the noise of security events versus actual incidents that merited investigation.

The other goes back to CISO liability. I've talked to national critical infrastructure CISOs, who looked at the fines when they were $1 million and said, "That is my entire net worth. I am out when this bill passes." Even at $500,000, I know CISOs of power utilities who believe it is not worth it for them to stay in their jobs. They are just not there, so if we are going to have personal liability, it should be on the boards of directors or the senior officers who actually make the decisions. That could be dealt with in regulation.

Senator Ross: Thank you.

Le sénateur McNair : Monsieur Shipley, avez-vous autre chose à ajouter au sujet de l'eau?

M. Shipley : Le projet de loi ne porte pas là-dessus. Je ne demande pas au Sénat de modifier la loi pour s'attaquer à cette question. Je souhaite que nous allions au-delà du projet de loi pour étudier le fond du problème.

Les États-Unis ont une longueur d'avance sur nous en matière de santé, car ils ont légiféré pour obliger le secteur de la santé à rendre des comptes aux termes de la Health Insurance Portability and Accountability Act. Nous n'en sommes pas là. Nous courons de sérieux risques en ce qui concerne aussi bien la santé que l'eau, et nous n'en discutons pas, car nous ne parvenons même pas à protéger les quatre domaines qui relèvent clairement de notre compétence et, depuis 2022 environ, nous n'arrivons pas à légiférer.

La sénatrice Ross : Ma question s'adresse à M. Shipley. Vous avez clairement recommandé que nous adoptions le projet de loi C-8 sans chercher à y apporter des amendements, bien qu'il puisse comporter des lacunes. Celles-ci, selon vous, pourraient être corrigées par voie réglementaire.

Les comités peuvent cependant formuler des observations lorsqu'ils font rapport au Sénat. Si vous étiez membre du Comité de la sécurité nationale, de la défense et des anciens combattants et souhaitiez ajouter des observations au rapport afin d'attirer l'attention sur une lacune du projet de loi, quelles seraient, selon vous, une ou deux observations clés qu'il serait souhaitable d'ajouter au rapport que le comité remettra au Sénat?

M. Shipley : Plus précisément, l'un des deux points que j'ai soulevés concernait la nécessité de veiller à ce que la réglementation définisse aussi clairement que possible ce qu'est au juste un incident. La législation de certains pays était si floue que les autorités se perdaient dans le brouhaha de tout ce qui est lié à la sécurité, au détriment des incidents réels qui méritaient une enquête.

L'autre point concerne la responsabilité des RSSI, les responsables de la sécurité des systèmes d'information. J'ai discuté avec des RSSI d'infrastructures critiques nationales. Lorsqu'ils ont pris connaissance des amendes qui s'élevaient à 1 million de dollars, ils ont déclaré : « Cela représente la totalité de ma valeur nette. Je démissionnerai dès que le projet de loi sera adopté. » Même à 500 000 $, je connais des RSSI de compagnies d'électricité qui estiment qu'il ne vaut pas la peine de rester en poste. Ils ne seront tout simplement pas là; par conséquent, si nous devons prévoir une responsabilité personnelle, celle-ci devrait incomber aux conseils d'administration ou aux cadres supérieurs qui prennent réellement les décisions. Cela pourrait se régler par voie réglementaire.

La sénatrice Ross : Merci.

Senator Boehm: Thank you, witnesses, for being with us today. This is my first recent meeting of this committee. However, I was on this committee two years ago when we were discussing Bill C-26. Much of the discussion is similar, but I wanted to probe a little bit.

Mr. Shipley, you mentioned that this bill is narrower and cleaner and that the government has benefited from a two-year interval to focus on and take account of developments both internationally and domestically in that context. You also mentioned that a lot can be achieved in the regulatory process, and that is something, of course, parliamentarians don't often see. We look at the legislation but do not look at all the regulatory underpinnings.

I'm wondering whether you can provide some examples of how you see that evolving.

Mr. Shipley: As mentioned, the specificity around the definition of "incident" and who should be held personally liable when we decide to pierce the corporate veil is important.

Another important component of this legislation is the designation of critical providers to these sectors. That's where we can broaden the scope to say we really depend on Google, Microsoft, Amazon, et cetera, for running the cloud services that now power some of our energy utilities and distribution grids, so I think a fair amount can be dealt with on that side.

Overall, the legislation takes a risks-based framework approach and talks about the bars that organizations have to clear to prove they have done due diligence.

The only other thing in regulation that could be wrestled with, and it is something we have debated back and forth, is liability for telecommunications providers if the government does a 90-degree turn on policy and says, "We don't like this country anymore. Your equipment is coming out."

One of the changes was that it was moved from a hard position of saying, "You're not entitled to compensation," to a softer position of saying, "It can be evaluated at the time." They need to find a way to be clearer about that in the regulations because, let's not kid ourselves, the rate payer is going to pay if they have to do this. Someone is going to pay.

Those are the major things I have thought about.

Le sénateur Boehm : Merci aux témoins d'être là. C'est la première fois depuis peu que je participe à une réunion du comité. J'en faisais partie il y a deux ans, lorsque nous avions étudié le projet de loi C-26. Les débats sont en grande partie similaires, mais je souhaiterais approfondir quelque peu la question.

Monsieur Shipley, vous avez dit que le projet de loi était plus ciblé et plus précis, et que le gouvernement avait eu deux ans pour s'intéresser aux développements intervenus aux niveaux tant international que national dans ce contexte et en tenir compte. Vous avez également souligné qu'on pouvait faire beaucoup de choses par voie réglementaire, ce que nous, parlementaires, avons rarement l'occasion de constater. Nous étudions le texte de loi, mais non ses règlements d'application.

Pouvez-vous donner quelques exemples pour expliquer comment, selon vous, la situation va évoluer?

M. Shipley : Comme je l'ai déjà dit, il est important de définir de manière précise le terme « incident » et de déterminer qui doit être tenu personnellement responsable lorsqu'on décide de lever le voile de la personnalité morale.

Un autre élément important du projet de loi est la désignation des fournisseurs essentiels de ces secteurs. C'est là que nous pouvons élargir le champ d'application pour reconnaître que nous dépendons réellement de Google, Microsoft, Amazon, etc., pour les services d'informatique en nuage sur lesquels comptent désormais certains de nos services publics d'énergie et de nos réseaux de distribution. Je pense donc qu'on peut faire beaucoup sur ce plan par voie réglementaire.

Dans l'ensemble, la législation adopte une approche fondée sur les risques et définit les critères que les organisations doivent respecter pour prouver qu'elles ont fait preuve de diligence raisonnable.

Le seul autre aspect qui pourrait être abordé par voie réglementaire, et c'est un sujet dont nous avons longuement débattu, concerne la responsabilité à l'égard des fournisseurs de services de télécommunications si le gouvernement opérait un revirement radical et déclarait : « Nous n'aimons plus ce pays-là. Vos équipements sont retirés. »

L'un des changements a consisté à passer d'une position intransigeante, écartant toute indemnisation, à une position plus souple, consistant à dire que la question pourrait être évaluée le moment venu. Il faut trouver le moyen de préciser ce point dans la réglementation car, ne nous leurrons pas, ce sont les contribuables qui finiront par payer si on en arrive là. Quelqu'un devra bien payer.

Voilà les principaux éléments qui me sont venus à l'esprit.

Senator Boehm: It would seem to me that, in looking at the regulatory process, we would also want to look at what other jurisdictions and countries are doing. You have all mentioned the G7. Well, we sit beside the "G1" geographically. There might be a lot of prospects there for osmosis in terms of ideas and approaches, but I would think the same is true with the Europeans, where there are certain similarities in terms of not only the threats and the malign actors behind the threats but also the different regulatory environments. This is open to the panel if I still have time, chair.

Mr. Shipley: One of the things that John and I and others have advocated is to harmonize with the American timelines. Many of our critical infrastructure providers are cross-border, so we suggest that we don't have two different sets of instant definitions or timelines. Let's try to be as unified in this as we can be on that side, which makes sense.

Mr. de Boer: I'd add two things.

One of the key lessons from other jurisdictions, in Europe and the U.S., has been public-private collaboration. Those systems are now being put in place in Canada. You are seeing that more. In Canada, we have something called the Canadian Forum for Digital Infrastructure Resilience, where you have companies from across the spectrum contributing to that. It's chaired by ISED. You also have a new cyberdefence collective being set up by Public Safety and CSE. We are learning from the U.S. Joint Cyber Defense Collaborative, with all its faults, but having public-private collaborations is important because the time to respond is important.

The second lesson that we have learned at ISC2, which is in Europe, is that there was too much — maybe not too much, but the sole focus was on reporting cyber incidents after they happened, without an understanding of what to do during the attack.

How do you communicate securely? How do you establish standards to ensure that the information about that incident gets to the reporting authority in a way that is not compromised, not over consumer-grade apps, et cetera? Setting that up and being mindful of security and continuity of operations are also important.

[*Translation*]

Senator Youance: My question is for Mr. Shipley.

You mentioned that if you were a designated operator and this bill were passed, your company would be bankrupt. Did I understand correctly?

Le sénateur Boehm : À propos du processus réglementaire, il me semblerait utile de voir ce qui se fait dans d'autres administrations ou pays. Vous avez tous parlé du G7. Or, géographiquement, nous sommes voisins du « G1 ». Il pourrait y avoir là de nombreuses possibilités d'osmose au plan des idées et des approches, mais il en va de même avec les Européens, avec qui il existe certaines similitudes non seulement au sujet des menaces et des acteurs malveillants qui sont derrière, mais aussi des contextes réglementaires. Tous les témoins peuvent répondre, pour peu que j'aie encore du temps, madame la présidente.

M. Shipley : M. de Boer, moi-même et d'autres avons notamment préconisé un alignement sur les délais américains. Bon nombre de nos fournisseurs d'infrastructures essentielles ont leurs activités hors de nos frontières; nous proposons donc de ne pas avoir deux séries distinctes de définitions ou de délais. Essayons d'être aussi cohérents que possible sur ce point, ce qui est tout à fait logique.

M. de Boer : J'ajouterais deux choses.

L'un des principaux enseignements tirés de pays européens et des États-Unis concerne la collaboration entre les secteurs public et privé. Elle est en train de se mettre en place au Canada. On observe de plus en plus ce phénomène. Au Canada, nous avons le Forum canadien sur la résilience des infrastructures numériques, auquel participent des entreprises de tous les secteurs. Il est présidé par Innovation, Sciences et Développement économique Canada, ou ISDE. Sécurité publique Canada et le Centre de la sécurité des télécommunications sont en train de créer un nouveau collectif de cyberdéfense. Nous tirons des enseignements du Joint Cyber Defense Collaborative américain, malgré toutes ses failles, mais il est important de mettre en place des collaborations public-privé, car le délai de réaction est crucial.

Le deuxième enseignement que nous avons tiré de l'ISC2, qui s'est tenu en Europe, est qu'on accordait trop d'importance — ou peut-être pas trop, mais en tout cas qu'on se concentrait uniquement sur le signalement des cyberincidents après coup, sans comprendre comment réagir pendant l'attaque.

Comment communiquer en toute sécurité? Comment établir des normes pour garantir que les informations relatives à l'incident parviennent à l'autorité compétente sans être compromises, sans passer par des applications grand public, etc.? Il est également important de mettre cela en place tout en veillant à la sécurité et au maintien des activités.

[*Français*]

La sénatrice Youance : Ma question s'adresse à M. Shipley.

Vous avez mentionné que si vous étiez un exploitant désigné et si l'on adoptait ce projet de loi, votre compagnie serait en faillite. Ai-je bien compris?

[*English*]

Mr. Shipley: Thank you. No. The legislation has the ability to hold individuals liable, so it pierces the legal protection that normally exists for corporations. Therefore, certain individuals could be held personally liable for failure to adhere to elements of the legislation.

That personal liability has caused a number of what are called certified information security officers, or CISOs, the most senior professionals with the most experience that we want at the helm, to re-evaluate whether they want to stay in the profession. This is a profession where over 50% of people want to quit already. So, if they could be personally ruined — or if that's the perception — it's going to make our problem even worse. My colleague may be able to speak to that as well.

[*Translation*]

Senator Youance: To what extent could the coming into force disrupt operators' daily operations? Apart from personal responsibility, are there other factors that might lead all those responsible to leave?

[*English*]

Mr. Shipley: My company is not currently in scope, though it could be made a designated operator because we provide services to critical infrastructure. I'm not worried about adhering to the legislation. I think it makes sense. I think these are things we already do today.

I do worry about the utility CISOs.

[*Translation*]

Senator Youance: Thank you.

Could the Canadian Centre for Cyber Security or another federal entity provide support to designated operators?

What observation could be added to the bill to avoid this negative impact?

[*English*]

Mr. Shipley: I don't think there is anything that can be amended in the bill to allay the concern. I don't think that there needs to be. In the regulations — I don't mind holding CEOs accountable if they make bad decisions, but I believe it should be directed to either the board of directors or the CEO. When I

[*Traduction*]

M. Shipley : Merci. Non. La législation prévoit la possibilité de tenir des personnes physiques responsables, ce qui lève la protection juridique dont bénéficient normalement les entreprises. Par conséquent, certaines personnes physiques pourraient être tenues personnellement responsables en cas de non-respect de certaines dispositions de la loi.

Cette responsabilité personnelle a conduit un certain nombre de responsables de la sécurité de l'information certifiés, ou RSSI — les professionnels les plus chevronnés et les plus expérimentés que nous souhaitons avoir à la tête de nos équipes — à se demander s'ils souhaitent rester dans la profession. Il s'agit d'un secteur où plus de 50 % des personnes souhaitent déjà démissionner. Ainsi, s'ils risquent de se ruiner personnellement — ou si c'est du moins l'impression qu'ils ont —, cela ne fera qu'aggraver le problème. Mon collègue pourra peut-être également s'exprimer à ce sujet.

[*Français*]

La sénatrice Youance : Dans quelle mesure l'entrée en vigueur pourrait-elle perturber les activités quotidiennes des exploitants? Mis à part la responsabilité personnelle, y aurait-il d'autres éléments qui feraient en sorte que tous les responsables partiraient?

[*Traduction*]

M. Shipley : Mon entreprise n'est pas visée pour l'instant, même si elle risque d'être considérée comme exploitant désigné, car elle offre des services à des infrastructures essentielles. Je ne m'inquiète pas de l'application de la loi. Je trouve cela logique. Ce sont des choses que nous faisons déjà aujourd'hui.

Je m'inquiète pour les responsables de la sécurité informatique des services publics.

[*Français*]

La sénatrice Youance : Merci.

Est-ce que le Centre canadien pour la cybersécurité ou une autre entité fédérale pourrait fournir un soutien aux exploitants désignés?

Quelle observation pourrait-on ajouter au projet de loi afin d'éviter cet impact négatif?

[*Traduction*]

M. Shipley : Il ne me semble pas possible d'amender le projet de loi pour dissiper ces inquiétudes. Je ne pense pas que ce soit nécessaire. À propos de réglementation, j'accepte que les premiers dirigeants soient tenus responsables s'ils prennent de mauvaises décisions, mais j'estime que la responsabilité devrait

talked to the drafters of the law, their intent was to get executives to care.

Senator Al Zaibak: My question is directed to Mr. de Boer.

In your opening remarks, you identified four areas for improving the bill. It wasn't clear to me whether you were suggesting amending the bill or are supporting the bill as is and, like Mr. Shipley, leaving it to the regulations to take care of those areas. Could you clarify, please?

Mr. de Boer: BlackBerry supports the bill and wants it passed. The elements of a clearer definition, timelines of reporting, continuity of operations and secure communications procedures can all be clarified in regulations.

Senator Al Zaibak: Thank you.

With respect to BlackBerry, it has evolved over the years and is very focused in cybersecurity protection. Where does it stand now among the major international players in this field?

Mr. de Boer: We specialize in securing mission-critical systems. We are 100% a software company now, and people trust us because of the "security first" approach that we take. We are a Canadian company; thus, we guarantee data sovereignty, and not just here. We are one of the few that ensure on-premise installations — that data where we work resides in those places. That is why governments come to us.

As I mentioned, we secure 275 million vehicles on the road today. For the majority of them, as they become more software defined, important BlackBerry's operating system becomes more important. Nuclear power stations, missile guidance systems — all the software used in these systems relies on BlackBerry. Why? Because it is secure.

We have transitioned our emphasis on hardware security into software security because that scales the most. And Canada is a leader in this space. People trust Canadian technology, as well. BlackBerry is really proud to work with the Canadian government and other Canadian technology companies to advance that.

Senator Al Zaibak: Thank you.

revenir au conseil d'administration ou au dirigeant principal. Je retiens de mes échanges avec les rédacteurs du texte que leur intention était d'amener les dirigeants à prendre la chose au sérieux.

Le sénateur Al Zaibak : Ma question s'adresse à M. de Boer.

Dans votre exposé liminaire, vous avez énuméré quatre points à améliorer dans le projet de loi. Je n'ai pas bien compris si vous proposiez de l'amender ou si vous le souteniez tel quel et, à l'instar de M. Shipley, si vous comptiez sur le processus réglementaire pour régler ces questions. Auriez-vous l'obligeance de préciser?

M. de Boer : BlackBerry soutient le projet de loi et en souhaite l'adoption. Les éléments relatifs à une définition plus claire, aux délais de signalement, à la continuité des activités et aux procédures de communication sécurisées peuvent tous être précisés dans la réglementation.

Le sénateur Al Zaibak : Merci.

BlackBerry a évolué au fil des ans et se concentre désormais principalement sur la cybersécurité. Quelle est sa position actuelle parmi les principaux acteurs internationaux dans ce domaine?

M. de Boer : Nous sommes spécialisés dans la sécurisation des systèmes essentiels à la mission. Nous sommes désormais une entreprise qui s'occupe uniquement de logiciels, et nos clients nous font confiance grâce à notre approche axée sur « la sécurité avant tout ». En tant qu'entreprise canadienne, nous garantissons la souveraineté des données, et pas seulement sur notre territoire. Nous sommes l'une des rares entreprises à proposer des installations sur site, ce qui signifie que les données auxquelles nous travaillons sont conservées sur place. C'est pourquoi les gouvernements font appel à nous.

Comme je l'ai dit, nous assurons la sécurité de 275 millions de véhicules actuellement en circulation. Pour la plupart d'entre eux, à mesure qu'ils s'appuient de plus en plus sur des solutions logicielles, le système d'exploitation de BlackBerry prend une importance croissante. Qu'il s'agisse de centrales nucléaires ou de systèmes de guidage de missiles, tous les logiciels utilisés dans ces systèmes s'appuient sur BlackBerry. Pourquoi? Parce qu'il est sûr.

Nous avons réorienté nos efforts de la sécurité matérielle vers la sécurité logicielle, car c'est ce domaine qui offre le plus grand potentiel de croissance. Et le Canada est un chef de file dans ce secteur. On fait également confiance à la technologie canadienne. BlackBerry est très fier de collaborer avec le gouvernement du Canada et des entreprises technologiques canadiennes pour faire progresser ce domaine.

Le sénateur Al Zaibak : Merci.

Senator Hay: Thank you all for being here. I might now store some water in my home.

I just want to pick up the thread on the mission-critical piece and data sovereignty, as well as a bit of what Senator Cardozo was talking about.

Professor Janice Stein said recently that it is not so much about control, because end-to-end data sovereignty really isn't possible in its entirety, but it is free from coercion, and that is probably the more important thing. When I think of BlackBerry and mission critical being very sovereign, based on BlackBerry's positioning, that isn't all data in Canada, though. Data travels, so it could boomerang through the United States before it lands. Please comment on that but also with respect to data centres and foreign clouds. It is more about cloud sovereignty than it is data sovereignty — or it is the same thing.

Please comment on that a bit.

If it's being free from coercion that we're striving for, how do we worry about state adversaries like China? Our trade situation with our ally south of the border and supply chains are potentially at risk right now.

Speak about those things — the U.S. CLOUD Act and our vulnerabilities there. I guess I'm looking at you, Mr. de Boer, because you did say that BlackBerry was fully sovereign. However, that is not the only place that holds our data.

Mr. de Boer: Thank you for that question.

When I say "sovereign," I mean it is truly sovereign — all data and the applications that we provide, and there are a number of them. One is a secure, government-grade voice and text system. It is similar to WhatsApp or Signal but resides fully here in Canada. In fact, it is installed in government data centres.

Senator Hay: And you're not governed, then, by the U.S. CLOUD Act or anything like that, right?

Mr. de Boer: If it is an on-premises installation, it doesn't even go through BlackBerry servers. We don't even see the data. It is fully sovereign. The Government of Canada has full control. Some other clients have full control, as well.

All our solutions were designed to be implemented and deployed that way. They can also be deployed to the cloud if consumers choose to do so. The difference between

La sénatrice Hay : Merci à tous d'être là. Je vais peut-être commencer à stocker un peu plus d'eau chez moi.

Je voudrais en revenir à la question des éléments essentiels pour la mission et de la souveraineté des données, ainsi qu'à certains propos du sénateur Cardozo.

Janice Stein a dit récemment qu'il ne s'agissait pas tant d'une question de contrôle, car la souveraineté des données de bout en bout n'est en réalité pas possible complètement, mais plutôt d'une absence de coercition, ce qui est probablement plus important. Je songe à BlackBerry et au fait que les systèmes essentiels à la mission sont très souverains, selon le positionnement de l'entreprise. Cela ne signifie toutefois pas que toutes les données se trouvent au Canada. Les données voyagent. Elles pourraient donc faire un détour par les États-Unis avant d'arriver à destination. Quel est votre avis à ce sujet et que pensez-vous des centres de données et des services en nuage? Il s'agit davantage de souveraineté du nuage que de souveraineté des données — ou est-ce la même chose?

Pourriez-vous nous en dire un peu plus à ce sujet?

Si notre objectif est de nous affranchir de la coercition, comment devons-nous nous prémunir contre des adversaires étatiques comme la Chine? Notre situation commerciale avec notre allié au sud de la frontière et nos chaînes d'approvisionnement sont peut-être à risque en ce moment.

Parlez-nous de ces questions — la loi américaine CLOUD Act et nos vulnérabilités à cet égard. Je m'adresse à vous, monsieur de Boer, car vous avez affirmé que l'entreprise BlackBerry était pleinement souveraine. Cependant, ce n'est pas le seul endroit où nos données sont hébergées.

M. de Boer : Merci de cette question.

Quand je dis « souverain », je veux dire vraiment souverain — pour toutes les données et les applications que nous fournissons, et elles sont nombreuses. L'une d'elles est un système sécurisé de communication vocale et textuelle de niveau gouvernemental. Il est similaire à WhatsApp ou Signal, mais il est entièrement hébergé ici, au Canada. En fait, il est installé dans les centres de données du gouvernement.

La sénatrice Hay : Vous n'êtes donc pas soumis à la loi américaine CLOUD Act ni à aucune autre disposition de ce type. Est-ce exact?

M. de Boer : S'il s'agit d'une installation sur site, les données ne transitent même pas par les serveurs de BlackBerry. Nous ne voyons même pas ces données. La souveraineté est complète. Le gouvernement du Canada en a le contrôle total. Certains autres clients en ont également le contrôle total.

Toutes nos solutions ont été conçues pour être mises en œuvre et déployées de la sorte. Elles peuvent aussi être déployées dans le nuage si les clients le souhaitent. La différence entre le modèle

BlackBerry's model and a lot of other entities is that they went cloud first and cloud only, and they stopped providing customers with the ability to control their data and to deploy it on-premises because it is more expensive, more specialized and more niche.

Two years ago, if people had told me that governments are going to start going back to on-premises as opposed to the cloud, I would have questioned them, but, today, that is the norm. That is why governments come to BlackBerry and others that provide those kinds of on-premises services.

Senator Hay: Mr. Shipley and Mr. Stupak, please talk a bit about non-BlackBerry sovereignty because that is a big conversation around our AI strategy, for example, in Canada and building data centres. BlackBerry is the Canadian success story; we know that.

Mr. Shipley: We are the only Canadian company left that does security awareness education at scale. We have 1,800 customers, including a number of our largest banks, all three national telecommunications providers and more. Everybody else has been bought. It's an interesting place to be.

We rely upon Microsoft infrastructure here in Canada, but we also have our own control over the encryption. There are some elements in terms of questions about where the U.S. CLOUD Act could come into this, but we're the closest we can be in our sector. To your point, there are elements. Sometimes, with some capabilities, as BlackBerry demonstrated, and at some value points — as there are significant costs to doing this — you can do it. That is the big thing. You can do full sovereignty if you are willing to pay the bill for it. Thus far, none have been unwilling to pay the bill.

Senator Hay: There are few countries that can do end-to-end sovereignty. So you're saying that the trade-off is worth it when you're working with hyperscalers like Microsoft and Amazon — it is the only way to do it.

Mr. Shipley: It has been. For us to compete against some of the extraordinarily funded American-based AI competitors now, we have to use every advantage we can. We're proudly Canadian, but if we weren't using hyperscaler cloud infrastructure, we would be dead in the water.

The Chair: We are running out of time and still have senators who wish to ask questions. Then we will see if we can get answers or a bit of homework out of it.

de BlackBerry et celui de nombreux autres fournisseurs, c'est que ceux-ci ont adopté une approche qui consiste à donner la priorité ou l'exclusivité aux services informatiques en nuage et ont cessé d'offrir à leurs clients la possibilité de contrôler leurs données et de les déployer sur site, car c'est plus coûteux, plus spécialisé et plus adapté à un créneau donné.

Il y a deux ans, si quelqu'un m'avait dit que les gouvernements allaient recommencer à privilégier l'hébergement sur site plutôt que l'informatique en nuage, j'aurais remis ce choix en question, mais aujourd'hui, c'est la norme. C'est pourquoi les gouvernements se tournent vers BlackBerry et d'autres fournisseurs qui offrent le service sur site.

La sénatrice Hay : Messieurs Shipley et Stupak, pourriez-vous parler un peu de la souveraineté hors des services de BlackBerry? C'est un grand débat autour de notre stratégie en IA, par exemple, ici au Canada, et de la construction de centres de données. BlackBerry est une réussite canadienne, nous le savons.

M. Shipley : Nous sommes la seule entreprise canadienne qui offre encore à grande échelle des formations en sensibilisation à la sécurité. Nous comptons 1 800 clients, y compris plusieurs de nos plus grandes banques, les trois fournisseurs nationaux de télécommunications et d'autres entités. Toutes les autres entreprises ont été rachetées. Nous occupons une position intéressante.

Nous nous appuyons sur l'infrastructure de Microsoft au Canada, mais nous gardons notre propre contrôle sur le chiffrement. Il y a des questions quant à l'application éventuelle de la loi américaine CLOUD Act, mais nous sommes le plus près possible dans notre secteur. Comme vous l'avez souligné, il faut tenir compte de certains éléments. Parfois, avec certaines capacités, comme l'a montré BlackBerry, et à certains niveaux de valeur — car cela a un coût important —, c'est possible. C'est la grande chose. On peut avoir une souveraineté totale si on est disposé à en assumer le coût. Jusqu'à présent, personne n'a refusé de payer.

La sénatrice Hay : Peu de pays peuvent assurer une souveraineté de bout en bout. Vous dites donc que le compromis en vaut la peine quand on travaille avec des fournisseurs à très grande échelle comme Microsoft et Amazon — que c'est la seule façon de faire.

M. Shipley : C'est le cas. Pour affronter certains concurrents américains en IA, extraordinairement bien financés, nous devons utiliser tous les avantages possibles. Nous sommes fiers d'être canadiens, mais si nous n'utilisions pas l'infrastructure informatique en nuage des fournisseurs à très grande échelle, nous serions voués à l'échec dès le départ.

La présidente : Le temps presse, et il reste des sénateurs qui souhaitent poser des questions. Nous verrons ensuite si nous pouvons obtenir des réponses ou un complément d'information.

Senator Cardozo: I will cut it down to one question.

Mr. Stupak, can you talk to us about what the Americans are doing in this regard and what lessons we must learn? With your experience in the White House, what was the level of openness from government to taking these measures?

Senator Ross: My question is for Mr. Shipley. You mentioned health infrastructure and the security of health services.

Given that it is not covered in the bill, can you give us some insight on how that can be included, as it is not necessarily federal jurisdiction?

Mr. Stupak: From the American perspective, when I was in government — highlighting that I have been out of government since January 17, 2025 — information sharing is one of the more important things that we've been doing, and we are starting to almost get there with the Joint Cyber Defense Collaborative, or JCDC, for example. It is an area where this bill could go further in regulations: enabling information sharing among critical infrastructure providers so they can share vulnerabilities back and forth to protect themselves. That goes far.

The other piece I would highlight is we did not focus on data sovereignty — and I understand this is an unpopular opinion — as data sovereignty is something of a mirage. We focused on encryption and ensuring our data was encrypted at rest and in transit, as well as measuring every agency in the federal government against that standard so that I knew how good they were at encrypting everything they had.

Mr. Shipley: To answer Senator Ross's question, the reason why I am so adamant about passing this legislation is so we can turn to the study of how we will wrestle with health care. Remember, our incentives in Canada are not aligned to invest in security. Every Canadian wants to hear how many more doctors, nurses, X-ray technologists or hospitals are being opened or how wait times are being reduced. No politician in this country is incented to invest in security, and the outcomes reflect that, so we need to have a serious conversation.

If we can tie federal funding to orthopaedic surgical wait times, we can tie federal funding to achieving baseline security standards; we can mandate formal cooperation with the Canadian Centre for Cyber Security.

Le sénateur Cardozo : Je vais m'en tenir à une seule question.

Monsieur Stupak, que font les Américains à cet égard? Quels enseignements faut-il en tirer? D'après votre expérience à la Maison-Blanche, dans quelle mesure le gouvernement était-il ouvert à prendre ces mesures?

La sénatrice Ross : Ma question s'adresse à M. Shipley. Vous avez parlé de l'infrastructure en matière de santé et de la sécurité des services de santé.

Étant donné que cet aspect n'est pas visé par le projet de loi, pourriez-vous nous donner des indications sur la manière dont il pourrait y en être tenu compte, étant donné que ce n'est pas nécessairement de compétence fédérale?

M. Stupak : Du point de vue américain? Lorsque je faisais partie du gouvernement — je précise que j'ai quitté mes fonctions le 17 janvier 2025 —, la communication d'informations était l'une des choses les plus importantes, et nous y sommes presque, notamment grâce à la Joint Cyber Defense Collaborative, ou JCDC. C'est un domaine dans lequel le projet de loi pourrait aller plus loin par la voie réglementaire : permettre la communication de renseignements entre fournisseurs d'infrastructures essentielles afin qu'ils échangent des renseignements sur leurs vulnérabilités pour se protéger mutuellement. Cela peut aller loin.

L'autre point que je soulignerais, c'est que nous n'avons pas mis l'accent sur la souveraineté des données — et je sais que c'est une opinion peu populaire —, car la souveraineté des données est en quelque sorte un mirage. Nous nous sommes concentrés sur le chiffrement et avons veillé à ce que nos données soient chiffrées au repos et en transit, et nous avons évalué chaque entité du gouvernement fédéral en fonction de cette norme afin de savoir à quel point chacune était efficace pour chiffrer tout ce qu'elle détenait.

M. Shipley : Pour répondre à la question de la sénatrice Ross, je dirai que si je tiens tant à l'adoption du projet de loi, c'est que nous pourrons alors étudier comment nous allons gérer le domaine des soins de santé. Rappelez-vous, les incitatifs au Canada ne favorisent pas l'investissement en sécurité. Chaque Canadien veut savoir combien il y a de médecins, d'infirmières, de techniciens en radiologie, combien d'hôpitaux supplémentaires sont ouverts ou comment on réduit les temps d'attente. Aucun politique au Canada n'est incité à investir en sécurité, et les résultats le montrent. Une discussion sérieuse s'impose donc.

Si nous pouvons lier le financement fédéral aux temps d'attente en chirurgie orthopédique, nous pouvons aussi le lier au respect de normes fondamentales de sécurité; nous pouvons prévoir une coopération formelle avec le Centre canadien pour la cybersécurité.

We never received a full accounting of what happened in Newfoundland because the lawyers were there, because of the concerns there and because of politics. We need to treat a health care incident like an airplane crash, meaning we need to learn everything we can as fast as possible to prevent the next one. That is a conversation we can't get to if we can't even pass this bill.

The Chair: Thank you. This brings us to the end of our time with this panel. Thank you very much, Mr. de Boer, Mr. Shipley and Mr. Stupak. Your testimony was very helpful, and thank you for the work you're doing in this lane. We obviously need it very much; it is very timely.

Welcome to Senator Yussuff, who has joined us.

For the next panel, we are pleased to welcome Kate Robertson, Senior Research Associate, Citizen Lab, at the University of Toronto; Christian Leuprecht, Professor, Royal Military College and Queen's University; and Matt Malone, Balsillie Scholar, Balsillie School of International Affairs in Waterloo. Thank you for joining us today.

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

Kate Robertson, Senior Research Associate, University of Toronto, Citizen Lab: Good evening. My name is Kate Robertson. I am a lawyer and, currently, a researcher at the University of Toronto's Citizen Lab.

My comments today draw on our research on cybersecurity and telecommunications, as well as constitutional law analysis I submitted in a brief to this committee. My brief set out five amendments to address constitutional deficits and cybersecurity risks in the bill.

A series of important amendments were made to Bill C-8 in the House of Commons earlier this year. However, this committee is still left with an unfortunate irony: that the most significant constitutional vulnerability remains in the bill, which is the imbalance between the bill's privacy-impacting powers and the contrasting absence of judicial oversight.

Judicial oversight amendments were implemented in the study by the committee but were subsequently ruled out of scope in the House. As a result, Bill C-8 remains highly vulnerable on constitutional grounds. Given its importance, this matter should not be disposed of for procedural reasons in Parliament.

Nous n'avons jamais obtenu de rapport complet sur ce qui s'est passé à Terre-Neuve à cause de la présence des avocats, des préoccupations locales et de la politique. Nous devons traiter un incident en matière de santé comme un accident d'avion, c'est-à-dire apprendre le maximum au plus vite pour éviter que cela ne se reproduise. C'est une discussion que nous ne pourrons pas avoir si nous n'adoptons même pas le projet de loi.

La présidente : Merci. Voilà qui met un terme à la période réservée à l'audition du groupe de témoins. Merci beaucoup, monsieur de Boer, monsieur Shipley et monsieur Stupak. Vos témoignages ont été très utiles et merci pour le travail que vous accomplissez dans ce domaine. Nous en avons manifestement grand besoin; c'est très opportun.

Bienvenue au sénateur Yussuff, qui se joint à nous.

Voici les témoins suivants. Nous sommes heureux d'accueillir Kate Robertson, associée de recherche principale au Citizen Lab de l'Université de Toronto; Christian Leuprecht, professeur au Collège militaire royal et à l'Université Queen's; Matt Malone, chercheur-boursier Balsillie à la Balsillie School of International Affairs de Waterloo. Merci de vous joindre à nous.

Pour commencer, les témoins sont invités à livrer leur exposé liminaire. Viendront ensuite les questions des membres du comité. Je rappelle aux témoins qu'ils ont cinq minutes pour faire leur exposé.

Kate Robertson, associée de recherche principale, Université de Toronto, Citizen Lab : Bonsoir. Je m'appelle Kate Robertson. Je suis avocate et actuellement chercheuse au Citizen Lab de l'Université de Toronto.

Mes observations d'aujourd'hui s'appuient sur nos recherches en cybersécurité et télécommunications, ainsi que sur l'analyse constitutionnelle que j'ai proposée dans un mémoire soumis au comité. Ce mémoire propose cinq amendements au projet de loi pour pallier les failles constitutionnelles et les risques en matière de cybersécurité.

Une série d'amendements importants ont été apportés au projet de loi C-8 à la Chambre des communes plus tôt cette année. Malgré tout, le comité est toujours placé devant un paradoxe regrettable : la vulnérabilité constitutionnelle la plus significative demeure présente dans le projet de loi, à savoir le déséquilibre entre les pouvoirs portant atteinte à la vie privée et l'absence de contrôle judiciaire.

Les amendements relatifs au contrôle judiciaire ont été approuvés lors de l'étude du comité, mais ils ont ensuite été considérés à la Chambre des communes comme dépassant la portée du projet de loi. En conséquence, le projet de loi C-8 demeure très vulnérable sur le plan constitutionnel. Vu son importance, cette question ne devrait pas être écartée pour des raisons de procédure parlementaire.

My brief further outlines how the absence of independent oversight also destabilizes Canada's existing national security framework, which faces precarious challenges at present even without the complications of Bill C-8. I recommend this committee find these constitutional risks are too significant to leave hanging over important public interest legislation. Addressing this imbalance should be a priority.

My brief also recommends mitigating amendments that are also important, particularly in the absence of judicial oversight.

First, we should clarify clause 15.2 to ensure that it also excludes the interception of metadata as well as clarify that it cannot be used to require telecommunications providers to adopt intercept capabilities.

We should stipulate that where personal or de-identified information is obtained from telecom providers, it should only be used by government agencies for cybersecurity and information assurance purposes.

Finally, clarification is needed on a new clause that was added by the House Standing Committee on Public Safety and National Security; in particular, the provision within clause 15.2 now stipulates that the powers cannot be used to decode encrypted private communications. This is good, but a correction is needed to include protection for encryption and technical safeguards in telecom generally, not just the specific type that attaches to private communications.

In the committee's clause by clause, all members and parties were of the view that an amendment was needed for encryption. Several versions were tabled. Ultimately, the version that received majority support was around the theory that the verbiage that's now in the bill expressly references the concept of encryption, which is laudable. However, this has the incidental problem of excluding important encryption technologies in Canada's networks that don't specifically attach to private communications, and this should be remedied.

Telecom networks are composed of many layers. Encryption is important in those layers generally. My brief proposes specific language on this. There are other options. Officials had expressed resistance during clause by clause about alternative phrasing, in particular the concept of "confidentiality, integrity and availability," suggesting that was vague. I find that surprising. It is one of the most widespread, authoritative terms to describe cybersecurity. Ultimately, that's something we see being proposed with respect to the controversial equivalent clause in Bill C-22, which is unfolding today. Those words are not vague, but I've also given another option in my brief.

Mon mémoire explique également comment l'absence de contrôle indépendant déstabilise davantage le cadre national de sécurité du Canada, déjà précaire, même sans les complications liées au projet de loi C-8. Je recommande au comité de conclure que ces risques constitutionnels sont trop importants pour être tolérés dans un projet de loi d'intérêt public aussi crucial. Corriger ce déséquilibre devrait être une priorité.

Mon mémoire recommande aussi des amendements importants pour atténuer les problèmes, surtout en l'absence de contrôle judiciaire.

Premièrement, nous devrions préciser l'article 15.2 pour assurer qu'il exclut aussi l'interception de métadonnées et dire qu'il ne peut être utilisé pour obliger les fournisseurs de télécommunications à se doter de capacités d'interception.

Il faudrait disposer que, lorsque des informations personnelles ou anonymisées sont obtenues auprès des fournisseurs de télécommunications, elles doivent être utilisées uniquement par les organismes gouvernementaux à des fins de cybersécurité et d'assurance de l'information.

Enfin, une clarification s'impose sur une nouvelle clause ajoutée par le Comité permanent de la sécurité publique et nationale; en particulier, la disposition de l'article 15.2 indique maintenant que les pouvoirs ne peuvent être utilisés pour déchiffrer les communications privées. C'est positif, mais une correction s'impose pour inclure la protection du chiffrement et des mesures techniques dans les télécommunications en général, et non uniquement le type spécifique lié aux communications privées.

Au cours de l'étude article par article, tous les membres et partis ont estimé qu'un amendement sur le chiffrement était nécessaire. Plusieurs versions ont été proposées. Au bout du compte, celle qui a reçu l'appui de la majorité reposait sur la théorie voulant que le libellé actuel du projet de loi fasse expressément référence à la notion de chiffrement, ce qui est louable. Cependant, cela pose le problème accessoire de l'exclusion des technologies de chiffrement importantes dans les réseaux canadiens qui ne sont pas expressément liées aux communications privées. Il faudrait que ce soit corrigé.

Les réseaux de télécommunications comportent plusieurs couches. Le chiffrement est important à ces niveaux en général. Mon mémoire propose un libellé précis à ce propos. Il existe d'autres options. Pendant l'étude article par article, les représentants gouvernementaux ont eu des réticences au sujet de formulations de rechange, notamment le concept de « confidentialité, intégrité et disponibilité », estimé trop vague. Ce qui m'étonne. C'est l'un des termes les plus répandus et qui font le plus autorité en cybersécurité. Enfin, ces termes sont proposés dans la disposition équivalente, controversée, du projet de loi C-22, qui est en cours d'examen. Ces mots ne sont pas vagues, mais j'ai aussi proposé une autre option dans mon mémoire.

Ultimately, this is not a riddle or a conundrum. Government experts undoubtedly know that encryption is in multiple layers of telecom networks and not just for private communications. I've included a 2024 report from Canada's cyber authorities that describes this.

Australian legislation uses language that is broader than Bill C-8 in this regard. Even the much-criticized Bill C-22 recognizes that electronic protections include both encryption and authentication.

We need a more inclusive scope of protection.

Thank you very much for your attention. I would be happy to provide more context and discussion in the question-and-answer stage.

The Chair: Thank you.

[*Translation*]

Christian Leuprecht, Professor, Royal Military College and Queen's University, As an individual: Thank you for the invitation. I'll speak in English, but please feel free to ask your questions in the official language of your choice.

[*English*]

Thank you for having me back at the Senate to testify. My objective is going to, maybe, change the perspective on this bill.

Canada is under constant attack from hybrid and grey-zone activities intent on espionage, sabotage, subversion and outright destruction of data and networks below NATO's Article 5 threshold.

Malign state, state-tolerated and non-state actors are not just going after vulnerabilities across Canada's cyber systems; their ultimate objective is abusing and undermining society's trust.

How do adversaries go after trust? They undermine our resilience. When an attack happens, how we respond has an implication for how our governments are perceived. Attacks are designed to make our state look weak. Citizens need to have trust in a state's competence, which is a core part of Bill C-8.

Citizens need to have trust in the legitimacy of the Canadian state. Adversaries build up misinformation campaigns; you can witness it in the controversy over lawful access. The adversary's narrative purports that all forms of surveillance are somehow illegitimate.

En fin de compte, ce n'est pas une énigme ou un casse-tête. Les experts gouvernementaux savent que le chiffrement se trouve dans plusieurs couches des réseaux de télécommunications et pas uniquement pour les communications privées. J'ai joint un rapport publié en 2024 par des autorités canadiennes en cybersécurité qui l'explique.

La législation australienne utilise un vocabulaire plus général que le libellé du projet de loi C-8 à cet égard. Même le très critiqué projet de loi C-22 reconnaît que les protections électroniques incluent à la fois le chiffrement et l'authentification.

Nous avons besoin d'une protection plus inclusive.

Merci beaucoup de votre attention. Je serai heureuse d'expliquer davantage le contexte et de poursuivre la discussion durant la période de questions.

La présidente : Merci.

[*Français*]

Christian Leuprecht, professeur, Collège militaire royal et Université Queen's, à titre personnel : Je vous remercie de l'invitation. Je vais m'exprimer en anglais, mais n'hésitez pas à poser vos questions dans la langue officielle de votre choix.

[*Traduction*]

Je vous remercie de m'avoir invité à nouveau au Sénat pour témoigner. Mon objectif est peut-être de faire évoluer le point de vue sur le projet de loi.

Le Canada est constamment ciblé par des activités hybrides et relevant de la « zone grise », portant sur l'espionnage, le sabotage, la subversion et la destruction pure et simple de données et de réseaux, sans pour autant atteindre le seuil prévu par l'article 5 de l'OTAN.

Les acteurs malveillants, qu'ils soient étatiques, tolérés par l'État ou non étatiques, ne se contentent pas d'exploiter les failles des systèmes informatiques du Canada. Leur objectif ultime est d'abuser de la confiance de la société et de la saper.

Comment les adversaires s'attaquent-ils à la confiance? Ils sapent notre résilience. Lorsqu'une attaque se produit, la riposte a des répercussions sur la façon dont nos gouvernements sont perçus. Les attaques visent à faire passer notre État pour faible. Les citoyens doivent pouvoir avoir confiance dans la compétence de l'État, ce qui est un élément essentiel du projet de loi C-8.

Les citoyens doivent avoir confiance dans la légitimité de l'État canadien. Les adversaires mènent des campagnes de mésinformation; on le constate notamment dans la controverse sur l'accès légal. Le récit de l'adversaire laisse entendre que toutes les formes de surveillance sont, d'une manière ou d'une autre, illégitimes.

Hybrid warfare thus intends to conjure up friction that calls into question the legitimacy and competency of the Canadian state. Bill C-8 remedies some of these deficiencies.

Adversaries target social cohesion. They aim to fracture society. Bill C-8 also helps with that.

Citizens need to trust one another and Canada's allies. Cohesion and solidarity in society are indispensable to a vibrant democracy, and I believe Bill C-8 does important work in shoring up cohesion.

Finally, what are the facts? What is right? What is real? How do we discern that? AI is further exacerbating uncertainty. Adversaries want our citizens to accuse the Canadian state of being authoritarian so as to weaken our defences. Bill C-8 provides important defences for the Canadian societal framework.

Bill C-8 addresses key weaknesses in Canada's cyber ecosystem that adversaries have been exploiting at scale to undermine Canadian security, prosperity and democracy. Yet investments needed to shore up Canada's resilience are actually fairly modest.

Bill C-8 is ultimately about building trust. For too long have government and society abdicated collective responsibility. Bill C-8 is part of a suite of measures to create and reinforce resilience and trust to sustain ourselves through political turmoil.

Bill C-8 provides a long-overdue legal framework to require designated operators across the finance, telecommunications, energy and transport sectors to enhance their cybersecurity strategies.

The legislation prioritizes resiliency and the ability of organizations to withstand an incident and to prohibit Canadian telecommunications companies using products or services that originate with the same high-risk suppliers whose countries of origin are intent on overturning the rules-based international order and thus pose an existential threat to our way of life. Protecting against these sorts of devices is essential.

Bill C-8 also introduces the critical cyber systems protection act, or CCSPA, which provides a comprehensive framework for ensuring the cyber systems that support Canada's vital services and systems.

La guerre hybride vise donc à susciter des tensions qui remettent en cause la légitimité et la compétence de l'État canadien. Le projet de loi C-8 comble certaines de ces lacunes.

Les adversaires s'attaquent à la cohésion sociale. Ils cherchent à diviser la société. Le projet de loi C-8 est également utile à cet égard.

Il faut que les citoyens se fassent confiance les uns aux autres et fassent confiance aux alliés du Canada. La cohésion et la solidarité au sein de la société sont indispensables à une démocratie dynamique, et le projet de loi C-8 joue un rôle important dans le renforcement de cette cohésion.

En fin de compte, quels sont les faits? Qu'est-ce qui est juste? Qu'est-ce qui est réel? Comment le déterminer? L'IA ne fait qu'aggraver l'incertitude. Nos adversaires veulent que nos citoyens accusent l'État canadien d'autoritarisme afin d'affaiblir nos défenses. Le projet de loi C-8 offre des moyens de défense essentiels pour le cadre sociétal canadien.

Le projet de loi C-8 vise à remédier aux principales faiblesses de l'écosystème cybernétique canadien, que des acteurs malveillants exploitent à grande échelle pour nuire à la sûreté, à la prospérité et à la démocratie du Canada. Pourtant, les investissements nécessaires pour renforcer la résilience du Canada sont en réalité assez modestes.

Le projet de loi C-8 vise avant tout à instaurer la confiance. Depuis trop longtemps, le gouvernement et la société se sont désengagés de leur responsabilité collective. Le projet de loi C-8 s'inscrit dans un ensemble de mesures visant à créer et à renforcer la résilience et la confiance afin de nous permettre de traverser les turbulences politiques.

Le projet de loi C-8 établit un cadre juridique qui n'a que beaucoup trop tardé afin d'obliger les exploitants désignés des secteurs de la finance, des télécommunications, de l'énergie et des transports à renforcer leurs stratégies en matière de cybersécurité.

Le projet de loi accorde la priorité à la résilience et à la capacité des organisations d'affronter un incident, et vise à interdire aux entreprises canadiennes de télécommunications d'utiliser des produits ou des services provenant de fournisseurs à haut risque dont les pays d'origine cherchent à renverser l'ordre international fondé sur des règles et constituent ainsi une menace existentielle pour notre mode de vie. Il est essentiel de se prémunir contre ce type de dispositifs.

Le projet de loi C-8 propose également la Loi sur la protection des cybersystèmes essentiels, la LPCE, qui établit un cadre complet visant à garantir la sécurité des cybersystèmes qui soutiennent les services et les systèmes critiques du Canada.

Importantly, the CCSPA would increase the sharing of information on cyber-threats by requiring the reporting of cybersecurity incidents above certain thresholds. Greater visibility on vulnerabilities by way of mandatory reporting by regulated entities is absolutely imperative. Canada's key allies already have similar frameworks and requirements in place, and some of them have for years. In the age of global conflict and great power competition, Bill C-8 is not just essential for the integrity of Canada's own cyber ecosystem but also an important signal to allies that Canada is serious about cyber because the allied cyber ecosystem is only as good as its weakest link.

That Canada is perceived as a weak link across myriad security issues by our closest ally is not lost on anyone here. On cyber, Canada has fared comparatively well. Bill C-8 is essential to maintain the trust and confidence Canada has built because Canadian vulnerabilities have cascading continental, allied and global consequences not just for Canada's cyber ecosystem but for Canada's reputation.

Guns and butter aren't what they used to be. Technology, hybrid threats, total defence, conventional capabilities, state-of-the-art modern warfare technology, dual-use technology, cyber disruptions and airspace incursions are today's guns. The butter is the freedom to have access to reliable and stable transport and energy, not to be disrupted in cyber or have medical devices weaponized. Today's butter is to defend, deter, react and prevent. That is the purpose of Bill C-8.

The Chair: Thank you.

Matt Malone, Balsillie Scholar, Balsillie School of International Affairs, as an individual: Thank you very much for the invitation and the opportunity to speak today. We were saying it felt like Groundhog Day coming back here, so it's fun to see everyone again.

My name is Matt. I am a scholar at the Balsillie School of International Affairs, and today I am speaking in a personal capacity. These are just my views.

To start with, on an optimistic note, I will make a general comment about the benefits of the bill.

Many of the changes this bill introduces, as my esteemed co-panellists shared, are welcome, including the requirements for certain actors to take cybersecurity more seriously, to develop programs, to mitigate risks and to report certain incidents.

Il est important de noter que la LPCE renforcerait l'échange de renseignements sur les cybermenaces en imposant le signalement des incidents de cybersécurité dépassant certains seuils. Une meilleure visibilité des vulnérabilités, grâce à l'obligation de signalement imposée aux entités assujetties à la réglementation, est absolument indispensable. Les principaux alliés du Canada ont déjà mis en place des cadres et des exigences similaires, et certains d'entre eux l'ont fait il y a des années. À l'ère des conflits mondiaux et de la rivalité entre grandes puissances, le projet de loi C-8 est non seulement essentiel à l'intégrité du cyberécosystème canadien, mais il constitue également un signal important adressé aux alliés, leur montrant que le Canada prend la cybersécurité au sérieux, car le cyberécosystème allié n'est pas plus solide que son maillon le plus faible.

Personne ici n'ignore que notre plus proche allié considère le Canada comme un maillon faible pour une multitude de questions de sûreté. En matière de cybersécurité, le Canada s'en est relativement bien sorti. Le projet de loi C-8 est essentiel pour préserver la confiance que le Canada a su bâtir, car les vulnérabilités canadiennes ont des répercussions en cascade à l'échelle du continent, au sein de l'alliance et à l'échelle mondiale, non seulement sur l'écosystème cybernétique du Canada, mais aussi sur sa réputation.

Les armes et le beurre ne sont plus ce qu'ils étaient. La technologie, les menaces hybrides, la défense totale, les capacités conventionnelles, les technologies de guerre modernes de pointe, les technologies à double usage, les perturbations cybernétiques et les incursions dans l'espace aérien constituent les armes d'aujourd'hui. Et le beurre, c'est la liberté d'avoir accès à des transports et à une énergie fiables et stables, sans subir de perturbations cybernétiques ni voir les matériels médicaux instrumentalisés. Le beurre d'aujourd'hui, c'est défendre, dissuader, réagir et prévenir. Tel est l'objectif du projet de loi C-8.

La présidente : Merci.

Matt Malone, chercheur-boursier Balsillie, Balsillie School of International Affairs, à titre personnel : Grand merci de m'avoir invité et de me donner l'occasion de prendre la parole. Nous disions que revenir ici nous donnait l'impression de revivre *Le jour de la marmotte*. C'est donc un plaisir de vous revoir tous.

Je m'appelle Matt Malone. Je suis chercheur-boursier à la Balsillie School of International Affairs, et c'est à titre personnel que j'interviens. Je n'exprimerai que mes opinions à moi.

Pour commencer, sur une note optimiste, je voudrais faire une remarque générale sur les avantages du projet de loi.

Comme l'ont souligné les éminents témoins qui sont là avec moi, bon nombre des changements proposés dans le projet de loi sont les bienvenus, notamment les obligations faites à certains acteurs de prendre davantage au sérieux la cybersécurité,

Minor changes would also help achieve these objectives, too, including, in my opinion, shortening the reporting period; expanding the list of "vital services and systems" already at this stage to include vital services and systems like space and data centres; and expanding ransomware reporting obligations so that actors that fall through the cracks of the law, who aren't covered by the law, would be required to report those too. Ransomware is the greatest cyber-threat facing average Canadians. Also, use an automatic, size-cap approach, as Europe does with its cybersecurity legislation, rather than a registration- or order-based system, as is contained in this one.

Des modifications mineures contribueraient également à la réalisation de ces objectifs. À mon avis, on pourrait notamment abréger le délai de signalement; allonger la liste des « services et systèmes critiques » dès à présent afin d'y inclure des services et systèmes essentiels tels que l'espace et les centres de données; élargir les obligations de signalement des attaques par rançongiciel afin que les acteurs qui passent entre les mailles du filet, et qui ne sont pas visés par la loi, soient également tenus de les signaler. Les attaques par rançongiciel constituent la plus grande cybermenace à laquelle sont confrontés les simples citoyens au Canada. Il conviendrait aussi d'adopter une approche automatique avec plafonnement, comme le fait l'Europe dans sa législation sur la cybersécurité, plutôt qu'un système basé sur l'enregistrement ou des décrets, comme il est prévu dans le projet de loi à l'étude.

I'm happy to talk about these ideas in detail, but the focus of the remainder of my opening remarks will be on two issues related to oversight and review.

Je serai ravi d'aborder ces idées plus en détail, mais le reste de mon exposé liminaire portera principalement sur deux questions liées au contrôle et à la révision.

When it comes to oversight, I agree with my colleague from the Citizen Lab: This bill has serious flaws. The administrative standards in Parts 1 and 2 for issuing orders and directions are quite low, and the threshold is simply whether the Governor-in-Council or the minister, in relevant part, believes on reasonable grounds that it is necessary to issue either an order or a direction, and the language is quite expansive. It's a low bar that could stretch to cover an enormous range of activity, and those orders or directives could be wrapped in a high level of secrecy, which I find particularly concerning.

En matière de contrôle, je partage l'avis de ma collègue du Citizen Lab : le projet de loi présente de graves lacunes. Les normes administratives prévues aux parties 1 et 2 pour la prise de décrets et de directives sont très peu contraignantes, et le seuil à atteindre se résume simplement à savoir si le gouverneur en conseil ou le ministre, selon le cas, croit, pour des motifs raisonnables, qu'il est nécessaire de prendre un décret ou d'émettre une directive, et la formulation est très large. Il s'agit d'un seuil très bas qui pourrait s'étendre à un vaste domaine d'activités, et ces ordres ou directives pourraient être entourés d'un niveau élevé de confidentialité, ce que je trouve particulièrement préoccupant.

Accompanying those order-making and direction-giving powers are information-gathering powers under clause 15.4 of Part 1 and clause 29 of Part 2, which Intelligence Commissioner Simon Noël has expressly warned might permit warrantless surveillance.

Ces pouvoirs de prise de décrets et de directives s'accompagnent de pouvoirs de collecte de renseignements prévus à l'article 15.4 de la première partie et à l'article 29 de la deuxième, au sujet desquels le commissaire au renseignement, Simon Noël, a expressément lancé une mise en garde en disant qu'ils pourraient permettre une surveillance sans mandat.

It is not a coincidence that the bill expressly bypasses the Intelligence Commissioner, in my opinion.

À mon avis, ce n'est pas un hasard si le projet de loi contourne expressément le commissaire au renseignement.

It is also worrying that Parts 1 and 2 permit wide latitude in the sharing of information that is obtained through these powers, both within organizations that have multiple mandates but also to foreign states, and perhaps there is a conversation there that you should be having.

Il est également préoccupant que les parties 1 et 2 accordent une grande latitude au sujet de l'échange de renseignements obtenus grâce à ces pouvoirs, tant au sein d'organisations ayant plusieurs mandats qu'avec des États étrangers; il y a peut-être là un sujet dont vous devriez discuter.

As with oversight, when it comes to review, there are some serious issues with the bill. This is after the fact as opposed to before the fact. What passes for review in Parts 1 and 2 are the obligations to notify the National Security and Intelligence Committee of Parliamentarians, or NSICOP, and the National

Quant au contrôle, le projet de loi présente de sérieux problèmes en matière d'examen. Il s'agit ici d'un examen a posteriori, et non a priori. Ce qui passe pour un examen dans les parties 1 et 2, ce sont les obligations d'informer le Comité des parlementaires sur la sécurité nationale et le renseignement, le

Security and Intelligence Review Agency, or NSIRA, when orders or directions are issued.

However, as I'm sure everyone in this room knows, those organizations face some real constraints in doing their review work.

NSICOP has produced phenomenal reports about the cybersecurity practices of the government itself. Those reports have largely had mixed success. NSICOP has made a number of recommendations that have not been taken up, and cyber has struggled to do its job as well. I wrote an article in January called "6 years on, Canada's intelligence watchdog says it still struggles to access government documents," highlighting how NSIRA repeatedly said in its annual reports that it was having trouble getting records from institutions it's supposed to oversee, like CSE. This is despite provisions in NSIRA's enabling law that says it can access any information it needs.

One of the most difficult federal institutions they're experiencing this with is the CSE, whose powers will be expanded in this law.

Also, NSIRA has said openly that it is not performing some reviews simply due to budgetary constraints. At the same time that CSE has seen its budget double in recent years, NSIRA is part of the 15% cuts across the board.

The measures in the bill complement what we've seen in Bill C-4 and Bill C-22, as well as what I read as what is in the upcoming reforms to the Access to Information Act and Privacy Act, which all indicate we are heading toward further erosion of Canadians' privacy rights.

The committee should treat these issues seriously and recognize that privacy and data security affect the health and security of our democracy. When it comes to privacy and data security, it is at the oversight and review stages where the rubber meets the road. Parliamentarians should carefully consider the concerns about potential harm from a lack of oversight and/or review.

In sum, I am not an opponent of the bill. I believe this is an important bill and we should have cybersecurity for critical infrastructure, but the bill could use refinements and needs better oversight and review and a lot less secrecy.

CPSNR, et l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, l'OSSNR, lorsque des décrets sont pris ou des directives sont données.

Or, comme personne ici ne l'ignore, ces instances sont aux prises avec de réelles contraintes dans l'exercice de leurs missions d'examen.

Le CPSNR a publié des rapports remarquables sur les pratiques du gouvernement en matière de cybersécurité. Ils ont généralement reçu un accueil mitigé. Le comité a formulé un certain nombre de recommandations qui n'ont pas été retenues, et le service chargé de la cybersécurité a lui aussi eu du mal à remplir sa mission. J'ai rédigé en janvier un article disant que « six ans plus tard, l'organisme de surveillance des services de renseignement du Canada affirme qu'il a toujours du mal à accéder aux documents gouvernementaux », et soulignant que l'OSSNR avait signalé à plusieurs reprises dans ses rapports annuels qu'il avait du mal à obtenir des documents auprès des établissements qu'il est censé superviser, comme le CST, soit le Centre de la sécurité des télécommunications. Et ce, malgré les dispositions de la loi habilitante de l'OSSNR qui prévoient qu'il peut accéder à tout renseignement dont il a besoin.

L'une des institutions fédérales avec lesquelles l'office éprouve le plus de difficultés à cet égard est le CST, dont les compétences seront élargies dans le cadre de la loi à l'étude.

Par ailleurs, l'OSSNR a déclaré ouvertement qu'il ne menait pas certaines évaluations simplement à cause de contraintes budgétaires. Alors que le budget du CST a doublé ces dernières années, l'OSSNR est visé par les coupes budgétaires générales de 15 %.

Les mesures prévues dans le projet de loi viennent compléter celles que proposaient les projets de loi C-4 et C-22, et celles, je crois comprendre, que préconiseront les réformes à venir de la Loi sur l'accès à l'information et de la Loi sur la protection des renseignements personnels, ce qui indique clairement que nous nous dirigeons vers une nouvelle érosion des droits à la vie privée des Canadiens.

Le comité devrait prendre ces questions au sérieux et reconnaître que la protection de la vie privée et la sécurité des données ont une incidence sur la santé et la sécurité de notre démocratie. À propos de la protection de la vie privée et de la sécurité des données, ce sont le contrôle et l'examen qui sont la pierre de touche. Les parlementaires devraient examiner attentivement les préoccupations relatives aux préjudices qui peuvent découler d'un manque de contrôle ou d'examen.

En résumé, je ne suis pas opposé au projet de loi. C'est un texte important et il est nécessaire d'assurer la cybersécurité des infrastructures essentielles, mais il pourrait être amélioré, prévoir un meilleur contrôle et un examen plus sérieux, et beaucoup moins de secret.

As parliamentarians, you have done important work on this bill, including Senator McNair catching drafting errors in its previous iteration. I applaud you for that work.

I hope you will continue this impressive work by strengthening the oversight and review provisions in the bill this time around. Thank you for the invitation to speak today.

The Chair: Thank you, Mr. Malone. We will now proceed to questions with the same restrictions as our last panel. Our guests will be with us until 5:55. I would like to offer the first question to our deputy chair.

Senator Al Zaibak: My first question goes to Ms. Robertson. In your opening remarks, you addressed the vulnerability of this bill to legal challenges. I'm going to ask you, from the Citizen Lab's perspective, about the vulnerability of Canadian institutions, including parliamentarians, diaspora communities, journalists and researchers, to foreign cyber-enabled intimidation and surveillance. I would appreciate your concerns about the legal aspects of that when we come back to it.

Ms. Robertson: The Citizen Lab has multiple areas of research that are engaged by the scope of your question, and I will do my best to address the most important pieces as it relates to this bill.

Undoubtedly, expansive surveillance powers and security vulnerabilities often have the potential to impact the most vulnerable people in our communities, including from both domestic and foreign surveillance actors. Some of those surveillance actors are authorized; some of them are unauthorized and gain access by unlawful intrusions.

On the last occasion that I was here to testify with respect to Bill C-26, I spoke about what at the time was the recently unfolding public awareness of the Salt Typhoon attack, which is now — some months later — understood to be one of the most expansive cyber-espionage attacks in history.

That attack was facilitated by some of the vulnerabilities in telecom networks that we very much hope the Government of Canada and those around the world will take a more proactive role in remedying. However, in the absence of sufficient safeguards in this legislation, which carry a constitutional risk as well as a cybersecurity risk, we fear that we will see the efforts of some within government who view surveillance as a more important priority than the security of everyone, including by compromising some of the very safeguards that would prevent us from experiencing some of the Salt Typhoon attacks of the future.

Vous, parlementaires, avez accompli un travail important sur le projet de loi, notamment le sénateur McNair qui a repéré des erreurs de rédaction dans la version précédente. Je vous félicite de ce travail.

J'espère que vous poursuivrez ce travail remarquable en renforçant, cette fois-ci, les dispositions relatives au contrôle et à l'examen prévues dans le projet de loi. Merci de m'avoir invité à prendre la parole.

La présidente : Merci, monsieur Malone. Nous allons maintenant passer aux questions. Les restrictions sont les mêmes que pour le dernier groupe de témoins. Les témoins sont là jusqu'à 17 h 55. Le vice-président posera la première question.

Le sénateur Al Zaibak : Ma première question s'adresse à Mme Robertson. Dans votre exposé, vous avez évoqué la vulnérabilité du projet de loi aux contestations judiciaires. Selon le Citizen Lab, les institutions canadiennes, ce qui englobe les parlementaires, les diasporas, les journalistes et les chercheurs, sont-elles exposées à l'intimidation et à la surveillance exercées depuis l'étranger par des moyens informatiques? Je voudrais connaître votre avis sur les aspects juridiques relatifs à tout cela, quand nous y reviendrons.

Mme Robertson : Le Citizen Lab mène des recherches dans maints domaines touchés par votre question, et je ferai de mon mieux pour aborder les aspects les plus importants sous l'angle du projet de loi.

Il ne fait aucun doute que les pouvoirs de surveillance étendus et les failles de sécurité sont souvent susceptibles de toucher les éléments les plus vulnérables de nos communautés, que ce soit du fait d'acteurs nationaux ou étrangers du domaine de la surveillance. Certains de ces acteurs sont autorisés. D'autres, en revanche, agissent sans autorisation et accèdent aux données par des intrusions illégales.

La dernière fois que j'ai comparu pour témoigner au sujet du projet de loi C-26, j'ai évoqué la sensibilisation publique, alors récente, à l'attaque Salt Typhoon, qui est aujourd'hui, quelques mois plus tard, considérée comme l'une des attaques de cyberespionnage les plus vastes de l'histoire.

Cette attaque a été rendue possible par certaines vulnérabilités des réseaux de télécommunications, et nous espérons vivement que le gouvernement du Canada et les gouvernements du monde entier joueront un rôle plus proactif pour y remédier. Toutefois, en l'absence de mesures de sécurité suffisantes dans le projet de loi, qui comporte un risque constitutionnel ainsi qu'un risque pour la cybersécurité, nous craignons de voir des membres du gouvernement, qui considèrent la surveillance comme une priorité plus importante que la sûreté de tous, compromettre certaines des mesures de sécurité qui nous éviteraient de subir à l'avenir des attaques semblables à celle de Salt Typhoon.

Senator Al Zaibak: Are you proposing specific amendments to this bill for our consideration?

Ms. Robertson: Yes, my brief has five specific amendments. The first is that there be judicial authorization with respect to the very expansive information-collection powers. Corresponding amendments were, in fact, made by the Standing Committee on Public Safety and National Security on the other side but were voted as out of order in the House. Those should be brought back to address this constitutional problem.

I also outlined in my remarks corresponding clarifications to restrain the scope of what government surveillance actors may seek to use this bill for if it's not explicitly made clear that they cannot do so. I really urged recognition that there is legislation going through Parliament under Bill C-22 that is explicitly a technical capability regime, but this bill could very well act as a technical capability regime if we don't expressly make it not so. That's what my amendments include.

Senator Al Zaibak: Thank you.

The Chair: Also, we did receive your information on Friday. At this moment, some of our colleagues may not have seen it because it's in translation. I would encourage us to have a good, fulsome look at it when they have received it. Thank you.

Senator Cardozo: I'll carry on the questioning that Senator Al Zaibak started.

Ms. Robertson, could you just provide more detail? We have you here, so maybe I can ask you to explain the clause you were looking at amending. Was it clause 15.2?

Ms. Robertson: The fifth recommendation relating to encryption relates to subclause 15.2(2.1), which references as an interpretive matter the stipulation that the powers in subclause 15.2 cannot be used to decode private communications. This is what I recommend be expanded to ensure that it doesn't inadvertently exclude all forms of encryption and critical safeguards that are part of modern telecommunications.

Senator Cardozo: Can you explain that more? What would it include and what would it exclude?

Ms. Robertson: Certainly.

Right now, this stipulation is specifically there to prevent private communications from being decrypted when they're wrapped in a form of encryption technology. However, there are

Le sénateur Al Zaibak : Proposez-vous des amendements précis que nous pourrions étudier?

Mme Robertson : Oui, mon mémoire comporte cinq amendements précis. Dans le premier, il est prévu qu'une autorisation judiciaire soit requise pour l'exercice de ces pouvoirs très étendus en matière de collecte de renseignements. Des amendements correspondants avaient d'ailleurs été adoptés par le Comité permanent de la sécurité publique et nationale à l'autre chambre, mais ils ont été jugés irrecevables par la Chambre des communes. Il faudrait les réintroduire afin de remédier à ce problème constitutionnel.

J'ai également exposé dans mon intervention les précisions nécessaires pour limiter la portée de l'utilisation que les acteurs de la surveillance gouvernementale pourraient vouloir faire de ce projet de loi si on ne le leur changé pas explicitement. J'ai vivement insisté pour que l'on reconnaisse qu'un texte de loi en cours d'examen au Parlement, le projet de loi C-22, est explicitement un régime de capacités techniques, mais que ce projet de loi pourrait très bien agir comme un régime de capacités techniques si nous ne précisons pas expressément que ce n'est pas le cas. C'est ce que visent mes amendements.

Le sénateur Al Zaibak : Merci.

La présidente : Par ailleurs, nous avons bien reçu vos renseignements vendredi. Pour l'instant, certains de nos collègues ne les ont peut-être pas encore consultés, car ils sont en cours de traduction. J'aimerais que nous les examinions attentivement et en détail dès qu'ils les auront reçus. Merci.

Le sénateur Cardozo : Je vais poursuivre dans la veine des questions du sénateur Al Zaibak.

Madame Robertson, pourriez-vous nous donner plus de détails? Puisque vous êtes ici, je pourrais peut-être vous demander d'expliquer la disposition que vous souhaitiez modifier. S'agissait-il de l'article 15.2?

Mme Robertson : La cinquième recommandation concernant le chiffrement porte sur le paragraphe 15.2(2.1), qui porte, à titre d'interprétation, sur la stipulation selon laquelle les pouvoirs prévus à l'article 15.2 ne peuvent servir à décoder des communications privées. C'est cette disposition que je recommande d'élargir afin de garantir que ne soient pas exclues par inadvertance toutes les formes de chiffrement et les mesures de protection essentielles qui font partie intégrante des télécommunications modernes.

Le sénateur Cardozo : Pourriez-vous développer un peu plus? Qu'est-ce qui serait inclus et qu'est-ce qui ne le serait pas?

Mme Robertson : Bien sûr.

À l'heure actuelle, cette stipulation vise en particulier à empêcher le décodage des communications privées lorsqu'elles sont protégées par une technologie de chiffrement. Cependant, il

many layers of telecommunications networks, and there are critical forms of encryption technology that apply to other elements of telecom technology in 5G — and 6G technology someday — that are really important to protect data generally, as it flows through telecom networks. That could include traffic and device identity or authentication.

This is ultimately a technical arena. I've included in my brief some illustrations as to why, from a cyber-expertise perspective — when I look at the guidance that Canada's Cyber Security Centre has issued, for example — it's urged for end-to-end encryption to be applied to all traffic.

This provision, in and of itself, is much narrower than that framing. We have language that I've put in the brief, but previous language that was discussed at the House Standing Committee on Public Safety and National Security referenced the concept of "confidentiality, integrity and availability," often called the "CIA triad." It's a term of art to reference the three major pillars of cybersecurity, and it's something that federal agencies already use in their official capacity.

Senator Cardozo: What are the three pillars?

Ms. Robertson: Confidentiality, integrity and availability. "CIA triad" is a term used to describe the way that strong cybersecurity shows up at a technical level in telecom systems.

Senator Cardozo: With regard to the amendment you had that was ruled out of order or out of scope, could you say more about that and where that would go?

Ms. Robertson: An amendment was made to Bill C-8 that would have specifically applied to ministerial orders and orders-in-council that would be issued under either clause 15.1 or clause 15.2. Those are some of the very expansive capability-making powers that are at the heart of Part 1 of Bill C-8. A Federal Court authorization was included by way of amendment in the House Standing Committee on Public Safety and National Security to ensure that the Federal Court continues to have oversight over something as significant as these types of orders.

I would also note that clause 15.4 would be what would enable the minister to basically request any information from telecom providers. I agree with the Intelligence Commissioner in his previous remarks: This warrantless power has no apparent justification, and it's difficult to envision how that would not be struck down under the Charter or saved under section 1 of the Charter.

y a plusieurs couches dans les réseaux de télécommunications, et il existe des technologies de chiffrement essentielles qui s'appliquent à d'autres éléments des technologies de télécommunications dans la 5G — et, un jour, dans la 6G — qui sont vraiment importantes pour protéger les données en général, au fur et à mesure qu'elles transitent par les réseaux de télécommunications. Cela pourrait inclure notamment le trafic ainsi que l'identité ou l'authentification des appareils.

C'est en fin de compte un domaine technique. J'ai inclus dans mon mémoire quelques illustrations expliquant pourquoi, du point de vue de l'expertise en cybersécurité — lorsque je me réfère aux directives émises, par exemple, par le Centre canadien pour la cybersécurité — il est recommandé d'appliquer un chiffrement de bout en bout à tout le trafic.

Cette disposition, en soi, est nettement plus restrictive que ce cadre. J'ai inclus un libellé dans le mémoire, mais dans le libellé antérieur discuté au Comité permanent de la sécurité publique et nationale, il était question du concept de « confidentialité, intégrité et disponibilité », souvent appelé la « triade C-I-D ». C'est un terme technique pour désigner les trois piliers majeurs de la cybersécurité, et c'est un concept déjà employé en contexte officiel par des organismes fédéraux.

Le sénateur Cardozo : Quels sont ces trois piliers?

Mme Robertson : Confidentialité, intégrité et disponibilité. La « triade C-I-D » est un terme utilisé pour décrire la manière dont une cybersécurité robuste se manifeste techniquement dans les systèmes de télécommunications.

Le sénateur Cardozo : Concernant l'amendement que vous aviez proposé et qui a été déclaré irrecevable ou hors sujet, pourriez-vous en dire plus et préciser où il aurait été intégré?

Mme Robertson : Un amendement au projet de loi C-8 aurait expressément concerné les arrêtés ministériels et les décrets pris en vertu de l'article 15.1 ou de l'article 15.2. Il s'agit de certains des pouvoirs très étendus conférant des capacités qui sont au cœur de la partie 1 du projet de loi C-8. Une autorisation de la Cour fédérale avait été introduite par amendement au Comité permanent de la sécurité publique et nationale de la Chambre des communes afin de garantir que la Cour fédérale continue d'exercer un contrôle sur des mesures aussi importantes que ces arrêtés.

Je voudrais aussi souligner que c'est l'article 15.4 qui permettrait au ministre de demander essentiellement tout renseignement aux fournisseurs de services de télécommunications. Je partage l'avis du commissaire au renseignement exprimé dans ses remarques antérieures, à savoir que ce pouvoir non mandaté ne semble aucunement justifié, et il est difficile de concevoir qu'il pourrait résister à un examen au regard de la Charte, ou qu'il soit validé en vertu de l'article 1 de la Charte.

So, you have an opportunity to include authorization, in particular, for that information-collecting ability.

Senator Dasko: One of my questions has been answered, but I'll get to the scope topic in a moment.

First, I want to ask Professor Leuprecht something that he raised that I hadn't really known about and find quite interesting. You said that, so far, the cyber-threats that we've experienced have fallen below the NATO threshold. I was not aware that NATO could actually be engaged in a cyber-threat operation.

Could you explain what you meant by that?

Mr. Leuprecht: Sure.

Article 5 applies to any provision where allies might perceive themselves to be under an attack where they would call in the collective defence provisions.

Our adversaries, in terms of the asymmetric capacities they deploy, quite deliberately use tactics, means and methods that keep their attacks below a threshold where Canada or any other member of the alliance might be able to invoke or might need to invoke Article 5. However, they come very close to pushing that threshold across a wide range of capabilities.

One of the challenges, of course, in this environment is that, while I empathize with the need to have proper safeguards in place — I did a whole book on Five Eyes accountability review and oversight — at the same time, this is an environment that moves extremely fast, where we often need governments to make critical decisions in a very timely fashion.

Part of the objective of Bill C-8, as I see it, is to give government the ability to be more dynamic and agile in responding to this very rapidly evolving environment where the adversarial capabilities are expanding exponentially.

Senator Dasko: I assume that no one has ever invoked Article 5 around cyber-threats. Has anyone got close to it? Have there been situations where that threshold might have been reached? I haven't heard about it before, so I'm quite interested.

Mr. Leuprecht: In this country, we have expanded the mandate of CSE and have included both active and offensive operations.

Vous avez donc l'occasion d'inclure une autorisation, notamment en ce qui a trait à cette capacité de collecte de renseignements.

La sénatrice Dasko : Je viens d'avoir la réponse à l'une de mes questions, mais je reviendrai sous peu sur la question de la portée.

Tout d'abord, je voudrais interroger M. Leuprecht sur un point qu'il a soulevé et dont je n'avais pas vraiment connaissance, mais que je trouve particulièrement intéressant. Vous avez dit que, jusqu'à présent, les cybermenaces que nous avons connues sont restées en dessous du seuil de l'OTAN. Je ne savais pas que l'OTAN pouvait être directement impliquée dans une opération liée à une cybermenace.

Pourriez-vous m'expliquer ce que vous entendiez par là?

M. Leuprecht : Bien sûr.

L'article 5 s'applique à toute circonstance où les alliés pourraient se considérer comme étant attaqués et invoqueraient alors les dispositions relatives à la défense collective.

Nos adversaires, par le déploiement de leurs capacités asymétriques, utilisent intentionnellement des tactiques, moyens et méthodes qui maintiennent leurs attaques sous le seuil à partir duquel le Canada ou tout autre membre de l'alliance pourrait invoquer — ou être contraint d'invoquer — l'article 5. Toutefois, ils se rapprochent fortement de ce seuil dans un large éventail de capacités.

L'un des défis dans cet environnement, bien sûr, est que, tout en comprenant la nécessité d'avoir des mesures de protection appropriées — j'ai écrit un livre sur l'examen redditionnel et la surveillance des « Five Eyes » —, c'est aussi un environnement qui évolue extrêmement rapidement, où les gouvernements doivent souvent prendre des décisions cruciales dans des délais très courts.

Selon moi, l'un des objectifs du projet de loi C-8 est de permettre au gouvernement de réagir avec plus de dynamisme et d'agilité dans un contexte où les capacités adverses évoluent de manière exponentielle.

La sénatrice Dasko : Je suppose que personne n'a encore invoqué l'article 5 à l'occasion d'une cybermenace. Est-ce qu'on s'en est déjà approché? Y a-t-il eu des situations où ce seuil aurait pu être atteint? Comme je n'en avais jamais entendu parler, c'est un sujet qui m'intéresse beaucoup.

M. Leuprecht : Ici, nous avons élargi le mandat du Centre de la sécurité des télécommunications, le CST, pour inclure à la fois des opérations actives et offensives.

We've provided ourselves with the ability to engage in active operations, precisely to be able to neutralize as needed adversarial capabilities that might pose significant threats to the integrity, for instance, of critical infrastructure.

We also have offensive capabilities. It is rather improbable that those would be used by a country such as Canada because they would be classic warfare capabilities. But all major members of the alliance now have active capabilities in recognition of the fact that adversarial actors exist and that simply playing defence is not an option. So you need to be actively engaged. Think about, for instance, the Hunt Forward teams that both the United States and several other allies now deploy in terms of looking for pre-positioned payloads in networks.

The state has visibility in this domain that private sector actors don't, so what this bill, in part, allows the state to do with the intelligence it has is act in a timely fashion on often rapidly evolving challenges. Take, for instance, Volt Typhoon, where the vulnerabilities were so significant that, at the time, the FBI received warrants to be able to engage in mitigating vulnerabilities in critical infrastructure systems because they were afraid their CISOs would not be able to act fast enough.

Time is of the essence here. Part of the balance in terms of the privacy elements is that we need to make sure we have the right balance in terms of where the pendulum swings in an environment where our adversarial actors and the asymmetric capabilities they have are becoming much more aggressive and brazen and pose a much greater risk to our critical infrastructure systems. We have a telecommunications company in this country through which, due to a software update, many of your phones would have not worked for three days.

I always say that if you want to destroy Western civilization, take out Microsoft. We have, sometimes by design, sometimes inadvertently, created significant vulnerabilities. Now we are catching up on how we mitigate those, since these are existential, vital systems for 21st-century society.

Senator Yussuff: Thank you, witnesses, for being here. Thank you for all your perspective and your important briefs.

Ms. Robertson, I will come to you. There have been many concerns raised about Bill C-26. It seems like déjà vu. It was a similar bill, but some of the improvements were critical in the context of those hearings.

Nous nous sommes dotés de la capacité de mener des opérations actives, précisément afin de neutraliser, au besoin, des capacités adverses susceptibles de représenter une menace importante pour l'intégrité, par exemple, des infrastructures essentielles.

Nous avons aussi des capacités offensives. Il est assez improbable que ces capacités soient utilisées par un pays comme le Canada, car elles relèvent de la guerre classique. Mais tous les membres majeurs de l'alliance ont désormais des capacités actives, reconnaissant que des acteurs hostiles existent et que se cantonner à la défense n'est pas une option. Il faut donc s'engager activement. Pensez, par exemple, aux équipes de chasse en avant que les États-Unis et plusieurs autres alliés déploient maintenant pour détecter des charges de virus prépositionnées dans les réseaux.

L'État a une visibilité dans ce domaine que le secteur privé ne possède pas, et ce projet de loi lui permet, en partie, d'agir rapidement avec les renseignements dont il dispose face à des défis qui évoluent souvent très rapidement. Si l'on prend l'exemple de « Volt Typhoon », les vulnérabilités étaient tellement importantes qu'à l'époque, le FBI a obtenu des mandats pour intervenir et atténuer les vulnérabilités des systèmes d'infrastructures essentielles, craignant que ses responsables de la sécurité informatique ne puissent pas réagir assez vite.

Il n'y a pas une minute à perdre dans de telles circonstances. L'équilibre à trouver en matière de protection de la vie privée consiste à assurer le bon dosage de protection dans un environnement où nos adversaires et leurs capacités asymétriques deviennent plus agressifs et audacieux, posant un risque bien plus grand à nos infrastructures essentielles. Il y a dans ce pays une entreprise de télécommunications à cause de laquelle, à la suite d'une mise à jour logicielle, bon nombre de vos téléphones n'auraient pas fonctionné pendant trois jours.

Je dis toujours que si l'on veut détruire la civilisation occidentale, il suffit de s'en prendre à Microsoft. Nous avons créé, parfois volontairement et parfois involontairement, d'importantes vulnérabilités. Nous rattrapons maintenant notre retard en matière d'atténuation, car ce sont des systèmes existentiels, essentiels à la société du XXIe siècle.

Le sénateur Yussuff : Merci aux témoins d'être présents aujourd'hui. Merci pour vos points de vue et vos mémoires importants.

Madame Robertson, ma question est pour vous. De nombreuses préoccupations ont été soulevées concernant le projet de loi C-26. Il y a comme un sentiment de déjà-vu. C'était un projet de loi similaire, mais certaines améliorations s'étaient avérées cruciales dans le cadre de ces audiences.

I think my colleagues in the House of Commons did tremendous work in trying to address as many as they could to make the bill better, as did Senator McNair, who very aptly pointed out there were some challenges in how the bill was drafted that needed to be corrected.

Would you acknowledge that Parliament has substantially improved the bill from the last bill we had in Bill C-26?

Ms. Robertson: I was saying before the hearing began that my brief with respect to this legislation has changed a lot, but my focused remarks verbally have changed very little, because I have been urging that the priority issues to address are to ensure that we don't have a piece of very important legislation that is dragged into the swamp of constitutional litigation.

We also don't want the provisions, which are intended to make our systems more secure, to become over time the vehicle for undermining those systems for surveillance purposes. As I noted, that type of approach is what's coming, perhaps, at some point, even to this very committee. It is not in the bill. This bill should be about cybersecurity and not surveillance.

Unfortunately, right now, we are at risk from how broad the framing is. It's a blurred mandate, and we've seen this in past complex pieces of legislation like this, where agencies come before the Senate and testify as to how they interpret their mandate vis-à-vis powers of this kind.

Review agencies like the National Security and Intelligence Review Agency, or NSIRA, have actually documented how agencies like CSIS have changed their position after the legislation was implemented. We don't want that here because we want these powers to make our systems more secure, not more compromised.

Networks like 5G and 6G ones have the important potential to help us mitigate some of the harms we are seeing, including cyber-fraud attacks that are all too easy to facilitate through telecommunications vulnerabilities. We hope those tasked with this legislation will implement it to address some of the legacy issues in telecommunications networks.

However, right now, we are seeing too much resistance to even the very basic premise that this bill shouldn't be about surveillance and encryption breaking, and when the amendment actually came through a few months ago, it was quite technical and narrow, which is concerning in itself.

Je pense que mes collègues de la Chambre des communes ont fait un travail remarquable en s'efforçant de corriger autant de points que possible afin d'améliorer le projet de loi, tout comme l'a fait le sénateur McNair, qui a souligné très justement qu'il y avait quelques problèmes liés à la rédaction du projet de loi qui devaient être corrigés.

Reconnaissez-vous que le Parlement a substantiellement amélioré le projet de loi par rapport à la dernière mouture, le projet de loi C-26?

Mme Robertson : Je disais avant le début de l'audience que mon mémoire sur ce projet de loi a beaucoup changé, mais que mes observations de vive voix ont très peu changé, car j'insiste depuis toujours sur le fait que la priorité est de veiller à ce qu'un texte législatif aussi important ne soit pas entraîné dans le bourbier des litiges constitutionnels.

Nous ne voulons pas non plus que les dispositions, qui visent à rendre nos systèmes plus sécuritaires, finissent par devenir, au fil du temps, un outil pour miner ces mêmes systèmes à des fins de surveillance. Comme je l'ai souligné, ce type d'approche pourrait, à un moment donné, apparaître même devant ce comité. Ce n'est pas dans le projet de loi. Ce projet de loi devrait concerner la cybersécurité, et non la surveillance.

Malheureusement, actuellement, le cadre est trop large, ce qui nous expose à des risques. Le mandat est flou, et nous avons déjà vu la même chose dans des textes législatifs complexes semblables dans le passé, quand des représentants d'organismes sont venus témoigner devant le Sénat au sujet de l'interprétation de leur mandat en lien avec ce type de pouvoirs.

Des organismes de contrôle, comme l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, l'OSSNR, ont effectivement documenté comment des organismes comme le Service canadien du renseignement de sécurité, le SCRS, ont modifié leur position après l'entrée en vigueur de la loi. Nous ne voulons pas que cela se produise ici, car nous souhaitons que ces pouvoirs renforcent la sécurité de nos systèmes, pas qu'ils la compromettent.

Les réseaux comme la 5G et la 6G ont le potentiel important de nous aider à atténuer certains des méfaits observés, y compris les cyberattaques frauduleuses, qui sont beaucoup trop faciles à commettre en exploitant les vulnérabilités des réseaux de télécommunications. Nous espérons que les responsables de cette loi la mettront en œuvre dans l'optique de régler certains problèmes hérités des réseaux de télécommunications.

Pour l'instant toutefois, nous observons une résistance trop forte même à la prémisse de base selon laquelle ce projet de loi ne devrait pas concerner la surveillance ni le décodage du chiffrement, et quand l'amendement a finalement été adopté il y a quelques mois, il était très technique et restreint, ce qui en soi est préoccupant.

Senator Yussuff: Referring to the point you made earlier that the House committee did bring forth an amendment that was ruled out of scope in the other place. That would be the same challenge we will face here. If we put forward an amendment that is out of scope, it will be out of scope. We can't do so.

The dilemma is that you can't fix something that is out of scope because of the way the drafter drafted this piece of legislation. I do acknowledge the point you're making, but the reality is, of course, that they already ruled in the other place that it is out of scope. We don't have the luxury of simply ignoring some of the realities that already happened, pretending we are going to do our own thing and disregarding the House of Commons ruling on this.

Ms. Robertson: Brighter minds than mine would have to help me understand how adding the most important safeguard that section 8 of the Charter of Rights and Freedoms affords is out of the scope of the principle of the legislation.

I don't understand that legal position. I've testified today that I don't think that something so important should be addressed and disposed of by matter of a procedure like this. But I would note, as well, that I'm not the only witness to testify at this stage before this committee on this bill.

The Intelligence Commissioner also testified about the availability of review by his office and his position, and that is not an amendment that has been ruled out of scope. I don't believe that either form of authorization should be ruled out of scope, but that is ultimately not for me to determine.

Senator Yussuff: Thank you very much for your work and for being here.

Senator Boehm: Thank you very much, witnesses, for being here. As Mr. Malone said, there is a sense of not just déjà vu but also Groundhog Day to this in terms of the work we did two years ago on Bill C-26, where you were also witnesses.

I recognize the value of civil society input. In the previous panel, we heard from practitioners from industry about the need to push forward. With any legislation that comes from the House of Commons to this place, there is always a need to push forward quickly.

I looked with some interest, Ms. Robertson, at your five proposed amendments. There is a lot that can be put into regulations and the regulatory aspect to a law, and those can be changed at almost any time, depending on circumstances. My

Le sénateur Yussuff : Pour revenir au point que vous avez soulevé tout à l'heure, à savoir que le comité de la Chambre des communes a bien adopté un amendement qui a été déclaré irrecevable à l'autre chambre, c'est exactement le même problème que nous rencontrerons ici. Si nous présentons un amendement irrecevable, il sera jugé comme tel. Nous ne pouvons pas procéder ainsi.

Le dilemme, c'est que l'on ne peut corriger ce qui est irrecevable à cause de la façon dont le rédacteur a conçu ce texte législatif. Je comprends votre point, mais la réalité est que l'autre chambre a déjà statué que l'amendement était irrecevable. Nous n'avons pas le luxe d'ignorer purement et simplement certaines réalités déjà établies, en prétextant pouvoir faire la sourde oreille et ne pas tenir compte de la décision de la Chambre des communes à ce sujet.

Mme Robertson : Il faudrait que des esprits plus brillants que le mien m'aident à comprendre comment le fait d'ajouter la mesure de protection la plus importante prévue à l'article 8 de la Charte des droits et libertés pourrait échapper à la portée du principe de la loi.

Je ne comprends pas cette position juridique. J'ai déclaré aujourd'hui que je ne pense pas qu'une question aussi importante doive être traitée et réglée dans le cadre d'une procédure comme celle-ci. Mais je tiens également à souligner que je ne suis pas la seule à avoir témoigné à ce stade devant ce comité au sujet de ce projet de loi.

Le commissaire au renseignement a également témoigné concernant la possibilité d'un examen par son bureau et sa position, et il ne s'agit pas là d'un amendement qui a été jugé irrecevable. Je pense qu'aucune de ces deux formes d'autorisation ne devrait être jugée irrecevable, mais ce n'est pas à moi de le déterminer en fin de compte.

Le sénateur Yussuff : Merci beaucoup pour votre travail et pour votre présence.

Le sénateur Boehm : Merci beaucoup aux témoins d'être ici. Comme l'a dit M. Malone, nous avons non seulement une impression de déjà-vu, mais aussi l'impression de vivre le jour de la marmotte, compte tenu du travail que nous avons accompli il y a deux ans au sujet du projet de loi C-26, pour lequel vous aviez également été appelés à témoigner.

Je reconnais l'importance de la contribution de la société civile. Dans le groupe de témoins précédent, des spécialistes du secteur nous ont fait part de la nécessité d'aller de l'avant. Chaque fois qu'un projet de loi passe de la Chambre des communes à cette chambre, il faut toujours avancer rapidement.

J'ai examiné avec un certain intérêt, madame Robertson, les cinq amendements que vous proposez. Les règlements et les dispositions réglementaires d'une loi peuvent couvrir de nombreux aspects, et ceux-ci peuvent être modifiés à tout

question to both you and Mr. Malone is this: Would any of your concerns be fixed or ameliorated by regulatory changes?

Mr. Malone: I think the ability to amend what a "vital system or service" is enables the Governor-in-Council to make those changes and bring in industries that are excluded right now. I think that would be a benefit.

Ms. Robertson: Your question specifically referenced the amendments that I recommended in my brief. I actually think it would be quite a problem if they were left for regulation because they are a matter of statutory interpretation. If I could just use one example, right now, the bill references the lack of authority in clause 15.2 to order the intercept of private communication.

I recommended that should be inclusive of intercepting metadata as well. As a matter of statutory interpretation, Parliament's intent will be divined from the clause that right now, as it stands, does not include metadata. There will be inferences drawn as to whether Parliament very much intended to enable the interception of metadata.

Similarly, I recommended an amendment to ensure that the bill doesn't interfere with the encryption surrounding other layers of telecom that would protect people against, for example, geolocation surveillance that is unauthorized. Right now, it only explicitly protects encryption of private communications. Again, inferences will be drawn by that narrow definition.

Senator Boehm: Thank you. I wanted to get your metadata comment on the record, and that is specifically what I was referring to.

Senator Al Zaibak: Ms. Robertson, as a business matter, how accessible are Citizen Lab services to citizens, enterprises and businesses in practice?

Ms. Robertson: The Citizen Lab is an academic research lab based at the University of Toronto's Munk School of Global Affairs, and it is engaged with research that is supervised by its director, Professor Ron Deibert. Its methods are entirely subject to the research and ethics protocols of the University of Toronto. It has no mandate to provide public services; it does public interest research.

Senator Al Zaibak: Thank you.

moment, selon les circonstances. Ma question s'adresse à vous et à M. Malone : est-ce que des modifications réglementaires permettraient de résoudre les problèmes ou d'atténuer l'une ou l'autre de vos préoccupations?

M. Malone : Je pense que la possibilité de redéfinir ce qu'est un « service critique ou système critique » permet au gouverneur en conseil d'apporter ces modifications et d'inclure des secteurs qui en sont actuellement exclus. Je pense que ce serait un avantage.

Mme Robertson : Votre question renvoie expressément aux modifications que j'ai recommandées dans mon mémoire. Je pense en effet que ce serait un véritable problème si ces questions étaient laissées à la discrétion du pouvoir réglementaire, car elles relèvent de l'interprétation de la loi. Pour ne citer qu'un exemple, le projet de loi fait actuellement référence à l'absence de pouvoir à l'article 15.2 permettant d'ordonner l'interception de communications privées.

J'ai recommandé que cela inclue également l'interception des métadonnées. En matière d'interprétation législative, l'intention du Parlement sera déduite de la disposition qui, dans sa version actuelle, n'inclut pas les métadonnées. On voudra déterminer si le Parlement avait réellement l'intention d'autoriser l'interception des métadonnées.

De même, j'ai proposé un amendement visant à garantir que le projet de loi n'affecte pas le chiffrement utilisé dans d'autres domaines des télécommunications, qui protège les citoyens contre, par exemple, la surveillance géolocalisée non autorisée. À l'heure actuelle, il ne protège explicitement que le chiffrement des communications privées. Une fois encore, cette définition restrictive donnera lieu à certaines interprétations.

Le sénateur Boehm : Merci. Je tenais à ce que votre remarque concernant les métadonnées figure au compte rendu, et c'est précisément de cela que je parlais.

Le sénateur Al Zaibak : Madame Robertson, d'un point de vue pratique, dans quelle mesure les services du Citizen Lab sont-ils accessibles aux citoyens et aux entreprises?

Mme Robertson : Le Citizen Lab est un laboratoire de recherche universitaire rattaché à la Munk School of Global Affairs de l'Université de Toronto. Ses travaux de recherche sont supervisés par son directeur, le professeur Ron Deibert. Ses méthodes sont entièrement soumises aux protocoles de recherche et d'éthique de l'Université de Toronto. Il n'a pas pour mission de fournir des services publics; il mène des recherches d'intérêt public.

Le sénateur Al Zaibak : Merci.

Mr. Malone, you suggested in your opening remarks expanding the scope of the bill to include space and data centres. Aren't they included as a matter of fact in the telecommunications sector?

Mr. Malone: Certain telecommunications companies might be included, but the ability to amend these through regulation is one of the examples I provided to the other question — there is flexibility here.

One of the problems is how slowly this bill has moved through Parliament. I think this was introduced when ArriveCAN was still mandatory, so it has been four years now. It goes to show the drawbacks that registration-based systems or systems where we rely on regulations to be issued to make the changes come with.

These laws get passed and then are laws for decades. The Privacy Act was passed in 1983, and we're doing a modernization right now for the first time. The Access to Information Act, PIPEDA — there are so many examples of this. I support the bill, but it is worth positing other approaches. One of the approaches that has a lot of merit is the European approach. After trying a registration-based system, NIS 1, they used a size-cap approach and disseminated these obligations for cybersecurity programs, mitigation efforts and reporting obligations based on the size of a company.

If Parliament draws these inferences, I share the concern that some of these law enforcement, national security and national intelligence agencies will read this language very carefully to utilize things like clause 15.4 in Part 1 and clause 29 in Part 2, the information-gathering powers that both the Intelligence Commissioner and the Privacy Commissioner have said will enable warrantless surveillance. However, the private sector will draw its own inferences too, and if they don't have to follow these obligations, they won't.

That is where size cap is a good model. It automates those things. It is like a trigger, and then private sector actors need to follow.

There is merit in other approaches. As much as there is an urgency to pass the law, which I recognize, the reality is that once we have the legislation, it is likely to be there for a long time.

Monsieur Malone, vous avez suggéré, dans votre intervention liminaire, d'élargir le champ d'application du projet de loi afin d'y inclure l'espace et les centres de données. Ne font-ils pas déjà partie du secteur des télécommunications?

M. Malone : Certaines entreprises de télécommunications pourraient être incluses, mais la possibilité de modifier ces dispositions par voie réglementaire est l'un des exemples que j'ai cités en réponse à l'autre question; il y a ici une certaine souplesse.

L'un des problèmes réside dans la lenteur avec laquelle ce projet de loi a été examiné par le Parlement. Je crois qu'il a été déposé à une époque où l'application ArriveCAN était encore obligatoire, et cela fait maintenant quatre ans. Cela met en évidence les inconvénients propres aux systèmes fondés sur l'enregistrement ou à ceux qui reposent sur la publication de règlements pour mettre en œuvre les changements.

Ces lois sont adoptées, puis restent en vigueur pendant des décennies. La Loi sur la protection des renseignements personnels a été adoptée en 1983, et c'est la première fois que nous procédons à sa modernisation. La Loi sur l'accès à l'information, la Loi sur la protection des renseignements personnels et les documents électroniques, ou LPRPDE; les exemples ne manquent pas. Je soutiens le projet de loi, mais il vaut la peine d'envisager d'autres approches. L'une de celles qui présentent de nombreux avantages est l'approche européenne. Après avoir essayé un système basé sur l'enregistrement, la directive NIS-1, les Européens ont adopté l'approche du plafonnement en fonction de la taille et ont réparti ces obligations en matière de programmes de cybersécurité, de mesures d'atténuation et de signalement en fonction de la taille de l'entreprise.

Si le Parlement tire ces conclusions, je partage la crainte que certains de ces organismes d'application de la loi, de la sécurité nationale et du renseignement national interprètent très attentivement ces dispositions afin de recourir à des dispositions comme l'article 15.4 de la partie 1 et l'article 29 de la partie 2, ces pouvoirs de collecte de renseignements au sujet desquels le commissaire au renseignement comme le commissaire à la protection de la vie privée ont déclaré qu'ils permettraient une surveillance sans mandat. Cependant, le secteur privé tirera également ses propres conclusions, et s'il n'est pas tenu de s'acquitter de ces obligations, il ne le fera pas.

C'est dans ce contexte que le plafonnement en fonction de la taille constitue un bon modèle. Il automatise ces processus. C'est comme un déclencheur, après quoi les acteurs du secteur privé doivent suivre le mouvement.

D'autres approches ont leurs mérites. Même si je reconnais qu'il est urgent d'adopter cette loi, la réalité est qu'une fois qu'elle sera en place, elle restera vraisemblablement en vigueur pendant longtemps.

Senator Al Zaibak: Thank you.

Senator Cardozo: I want to pursue that question in terms of passing the bill in its current form and making amendments or not. You don't feel that the issues you've raised can be dealt with in regulation.

Given that we have taken so long to get here and that last time we had a couple of very technical errors that we sent back and a year and a half later we're still here, would you consider that we should pass the bill as is and fix some of those things in a subsequent bill?

Ms. Robertson: I acknowledge it has been some time since I was here last, but I recall one of your colleagues on this committee had expressed some hesitancy around amendments because at that time there was a concern as to what would happen if the bill were to return to the House of Commons.

I don't gather that it is as front and centre in the thinking of this committee. That would be my inference.

Senator Cardozo: It is a more stable government now than the last time you came here in terms of what was happening in the other place versus here.

Ms. Robertson: Even with that different opportunity available, I still testified on the last occasion — and I would repeat — that this is long-term cybersecurity. It is an approach that may be replicated at the provincial level. When you have something as precedent setting as this, you absolutely want its compass points pointed in the right direction.

I'll repeat myself that there is surveillance capability legislation going through the House of Commons, and undoubtedly — or hopefully — parliamentarians will be attentive to the correspondingly significant safeguards that would need to accompany capabilities of that kind.

Right now, because this bill hasn't been positioned as surveillance capability powers, it doesn't have the corresponding safeguards.

This is not something we should be afraid of fixing. By the government's own description, it's not supposed to be surveillance legislation, and this committee should ensure that it is not.

Senator Cardozo: I read an article by you in *The Walrus*, "Trump Wants to Tap Your Phone. Ottawa Might Let Him,"

Le sénateur Al Zaibak : Merci.

Le sénateur Cardozo : Je voudrais approfondir cette question pour savoir s'il convient d'adopter le projet de loi tel quel ou d'y apporter des modifications. Vous ne pensez pas que les problèmes que vous avez soulevés puissent être réglés par voie réglementaire.

Étant donné qu'il nous a fallu tant de temps pour en arriver là et que, la dernière fois, il y a eu quelques erreurs très techniques qui nous ont obligés à renvoyer le projet de loi, et qu'un an et demi plus tard, nous sommes de retour au même point, pensez-vous que nous devrions adopter le projet de loi dans sa version actuelle et apporter les corrections dans un projet de loi ultérieur?

Mme Robertson : Je reconnais que cela fait un certain temps que je ne suis pas venue ici, mais je me souviens qu'un de vos collègues de ce comité avait émis des réserves concernant les amendements, car on s'inquiétait alors de ce qui se passerait si le projet de loi devait être renvoyé à la Chambre des communes.

Je n'ai pas l'impression que cela occupe une place centrale dans le raisonnement de ce comité. C'est du moins ce que j'en déduis.

Le sénateur Cardozo : Le gouvernement est aujourd'hui plus stable que lors de votre dernière visite, si l'on compare à ce qui se passait dans l'autre chambre à ce qui se passait ici.

Mme Robertson : Malgré cette autre possibilité, j'ai tout de même déclaré lors de mon dernier témoignage — et je le maintiens — qu'il s'agit là d'une stratégie de cybersécurité à long terme. C'est une approche qui pourrait être reproduite au niveau provincial. Lorsqu'on a affaire à un projet aussi novateur, il est essentiel que ses orientations soient bien alignées.

Je le répète : un projet de loi sur les capacités de surveillance est actuellement examiné à la Chambre des communes, et il ne fait aucun doute — du moins je l'espère — que les parlementaires seront attentifs aux mesures de protection importantes qui devraient, en toute logique, accompagner des capacités de ce type.

À l'heure actuelle, comme ce projet de loi n'a pas été présenté comme un texte visant à renforcer les pouvoirs en matière de surveillance, il ne comporte pas les mesures de protection correspondantes.

Ce n'est pas une chose que nous devrions craindre de corriger. Selon la description qu'en donne le gouvernement lui-même, ce texte de loi n'est pas censé être une loi sur la surveillance, et ce comité devrait veiller à ce qu'il n'en soit pas ainsi.

Le sénateur Cardozo : J'ai lu un article que vous avez publié dans *The Walrus*, intitulé « Trump Wants to Tap Your Phone.

with regard to Bill C-22. Some may be interested in reading that article. Will you be testifying on Bill C-22?

Ms. Robertson: I am not sure if I will be testifying. I had understood that the committee will be sitting for at least three hearing dates. If that remains true, then tomorrow will be the last occasion, in which case I will not be testifying because I was not invited.

Senator Cardozo: Thank you for being here today.

The Chair: This brings us to the end of our time with this panel. I would like to thank Ms. Robertson, Mr. Leuprecht and Mr. Malone for being here and taking the time to meet with us today. We appreciate your contributions and work on this bill, as well as the work that you're doing each and every day.

Colleagues, I will be leaving for the second part of this meeting due to another defence-related engagement. Senator Al Zaibak will serve as the chair in my absence.

(Senator Mohammad Al Zaibak, Deputy Chair, in the chair.)

The Deputy Chair: Good afternoon, everyone. I am Senator Al Zaibak, deputy chair of the committee. I will chair the remainder of this meeting.

For our next panel, we are pleased to welcome Jennifer Quaid, Executive Director, Canadian Cyber Threat Exchange; Aaron Shull, Research Director, Centre for International Governance Innovation; and, by video conference, Ali Ghorbani, Professor and Director, Tier 1 Canada Research Chair in Cybersecurity, Canadian Institute for Cybersecurity, University of New Brunswick.

Welcome to you all. Thank you for joining us today.

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

Jennifer Quaid, Executive Director, Canadian Cyber Threat Exchange: Thank you, Mr. Chair. I am here today representing the Canadian Cyber Threat Exchange and its more than 200 member organizations, many of whom are in the sectors that this bill will legislate; others make up their supply chains.

Ottawa Might Let Him », concernant le projet de loi C-22. Certains pourraient être intéressés par la lecture de cet article. Allez-vous témoigner au sujet du projet de loi C-22?

Mme Robertson : Je ne sais pas encore si je vais témoigner. J'avais cru comprendre que le comité tiendrait au moins trois séances. Si c'est toujours le cas, demain sera la dernière séance, et je ne témoignerai pas puisque je n'ai pas été invitée.

Le sénateur Cardozo : Merci d'être ici aujourd'hui.

La présidente : Cela marque la fin de la période de questions avec ce groupe. Je tiens à remercier Mme Robertson, M. Leuprecht et M. Malone d'être ici et d'avoir pris le temps de nous rencontrer aujourd'hui. Nous apprécions vos contributions et le travail que vous avez accompli relativement à ce projet de loi, ainsi que le travail que vous effectuez au quotidien.

Chers collègues, je vais devoir m'absenter pour la deuxième partie de cette séance en raison d'un autre engagement lié à la défense. Le sénateur Al Zaibak assumera la présidence en mon absence.

(Le sénateur Mohammad Al Zaibak, vice-président, occupe le fauteuil.)

Le vice-président : Bonjour à tous. Je suis le sénateur Al Zaibak, vice-président du comité. Je présiderai la suite de cette séance.

Pour notre prochain groupe de témoins, nous avons le plaisir d'accueillir Jennifer Quaid, directrice générale de l'Échange canadien de menaces cybernétiques; Aaron Shull, directeur de recherche au Centre pour l'innovation dans la gouvernance internationale; ainsi que, par vidéoconférence, Ali Ghorbani, professeur et directeur de la Chaire de recherche du Canada de niveau 1 en cybersécurité à l'Institut canadien de la cybersécurité de l'Université du Nouveau-Brunswick.

Bienvenue à tous. Merci d'avoir accepté de témoigner aujourd'hui.

Nous commencerons par vous inviter à prononcer votre déclaration liminaire, qui sera suivie des questions de nos membres. Je vous rappelle que vous disposez chacun de cinq minutes pour votre déclaration.

Jennifer Quaid, directrice générale, Échange canadien de menaces cybernétiques : Merci, monsieur le président. Je suis ici aujourd'hui au nom de l'Échange canadien de menaces cybernétiques et de ses quelque 200 organisations membres, dont bon nombre opèrent dans les secteurs visés par ce projet de loi; d'autres font partie de leurs chaînes d'approvisionnement.

I am here in support of passing Bill C-8, and I want to explain why through the same risk-based lens that security leaders across our country live by because, at its core, this legislation is about managing risk to Canadians.

A risk-based approach asks three simple questions: What is the likelihood of harm? What is the severity if it occurs? What is the cost of prevention versus inaction? Bill C-8 stands up well on all three counts.

First, regarding likelihood, the risks addressed by Bill C-8 are not hypothetical. They are present, persistent, pervasive and growing. Attacks on our systems are real and ongoing. Ignoring them does not make them disappear. It only increases the probability of more costly consequences later.

Second, regarding severity, the consequences of inaction are significant. A cyber breach in one system could trigger broader disruptions beyond the four critical infrastructure sectors addressed here, affecting essential services, markets and public confidence and trust.

Third, regarding cost effectiveness, prevention is surely cheaper and more effective than response. Bill C-8 is a measured investment in resilience. It doesn't try to eliminate all risks; that would be completely impractical. Instead, it targets the most material risks with proportionate tools.

Concurrently, we must ensure that we retain the trust of Canadians. Canadians expect their institutions to anticipate risk, not just react to it.

When governments act early, they reduce both harm and recovery costs. Supporting Bill C-8 signals a commitment to responsible stewardship. This bill acknowledges risk and provides a proportionate strategy — because hope is not a strategy.

Finally, I want to address the concerns about privacy. A risk-based approach doesn't dismiss privacy. It requires us to weigh it carefully. Bill C-8 does not operate in a vacuum.

Canada already has strong legal frameworks, independent oversight and accountability mechanisms that protect personal information and civil liberties. These safeguards are active and effective already today.

Je suis ici pour soutenir l'adoption du projet de loi C-8, et je souhaite vous expliquer pourquoi en adoptant la même approche fondée sur les risques que celle suivie par les responsables de la sécurité partout au pays, car, au fond, cette loi vise à gérer les risques auxquels sont exposés les Canadiens.

Une approche fondée sur les risques pose trois questions simples : quelle est la probabilité qu'un préjudice survienne? Quelle en serait la gravité s'il venait à se produire? Quel est le coût de la prévention par rapport à celui de l'inaction? Le projet de loi C-8 répond favorablement à ces trois questions.

Tout d'abord, en ce qui concerne la probabilité, les risques visés par le projet de loi C-8 ne sont pas hypothétiques. Ils sont bien réels, persistants, omniprésents et en augmentation. Les attaques contre nos systèmes sont bien réelles et se poursuivent. Ne pas en tenir compte ne les fera pas disparaître. Cela ne fera qu'accroître le risque de conséquences plus coûteuses à l'avenir.

Ensuite, en ce qui concerne la gravité, les conséquences d'une inaction sont considérables. Une cyberattaque visant un seul système pourrait entraîner des perturbations plus larges, dépassant le cadre des quatre secteurs d'infrastructures essentielles abordés ici, et affecter les services essentiels, les marchés ainsi que la confiance du public.

Enfin, en ce qui concerne le rapport coût-efficacité, la prévention est assurément moins chère et plus efficace que la réaction. Le projet de loi C-8 constitue un investissement mesuré dans la résilience. Il ne vise pas à éliminer tous les risques; cela serait tout à fait irréalisable. Il cible plutôt les risques les plus importants à l'aide d'outils proportionnés.

Parallèlement, nous devons veiller à conserver la confiance des Canadiennes et des Canadiens. Ceux-ci attendent de leurs institutions qu'elles anticipent les risques, et non qu'elles se contentent d'y réagir.

Lorsque les gouvernements agissent rapidement, ils réduisent à la fois les préjudices et les coûts liés à la reprise. Soutenir le projet de loi C-8 témoigne d'un engagement en faveur d'une intendance responsable. Ce projet de loi reconnaît les risques et propose une stratégie adaptée, car l'espoir n'est pas une stratégie.

Enfin, je tiens à aborder les préoccupations relatives à la vie privée. Une approche fondée sur les risques ne fait pas abstraction de cet aspect. Elle nous oblige à en tenir soigneusement compte. Le projet de loi C-8 ne s'applique pas en vase clos.

Le Canada dispose déjà de cadres juridiques solides, ainsi que de mécanismes indépendants de contrôle et de responsabilité qui protègent les renseignements personnels et les libertés civiles. Ces mesures de protection sont déjà en vigueur aujourd'hui.

The question is not whether privacy will be protected; it already is. The question is whether we can address these risks within the existing framework. The answer is yes.

The bill builds on existing protections, ensuring risk mitigation does not come at the expense of fundamental rights.

Striving for consensus on a bill is admirable, but it is not practical. This bill will deliver real benefits now. It lowers risk. It improves coordination. It strengthens defences in critical systems.

Waiting for perfection doesn't eliminate risk. It is a choice to accept it. The greater cost is in inaction, not imperfection.

We have to act now to reduce the risks facing Canadians while respecting the systems that safeguard their privacy. Bill C-8 strikes that balance.

In closing, Bill C-8 represents responsible governance. It is proactive, proportionate and grounded in evidence. It reduces both the likelihood and severity of future harm. For these reasons, I would urge you to support its passage.

Thank you.

The Deputy Chair: Thank you, Ms. Quaid.

Ali Ghorbani, Professor and Director, Tier 1 Canada Research Chair in Cybersecurity, Canadian Institute for Cybersecurity, University of New Brunswick, as an individual: Good evening. It is a pleasure to be with you today for this discussion on strengthening Canada's legislative and strategic cybersecurity capabilities.

As introduced, my name is Ali Ghorbani. I'm a professor of computer science at the University of New Brunswick, a Tier 1 Canada Research Chair in Cybersecurity and founding director of the Canadian Institute for Cybersecurity, Canada's first dedicated cybersecurity institute. Established 10 years ago, it is now a leading centre for research, training and collaboration.

While much of the importance of securing Canada's critical infrastructure has already been well articulated, I would emphasize a key point: Cybersecurity is no longer solely a technical issue; it is central to our way of life, national security, national power, economic stability, societal values and public trust.

La question n'est pas de savoir si la vie privée sera protégée; elle l'est déjà. La question est de savoir si nous pouvons faire face à ces risques dans le cadre existant. La réponse est oui.

Ce projet de loi s'appuie sur les mesures de protection existantes, garantissant ainsi que l'atténuation des risques ne se fasse pas au détriment des droits fondamentaux.

Chercher à obtenir un consensus sur un projet de loi est louable, mais ce n'est pas réaliste. Ce projet de loi apportera des avantages concrets dès maintenant. Il réduit le risque. Il améliore la coordination. Il renforce la sécurité des systèmes critiques.

Attendre la perfection n'élimine pas le risque. C'est un choix que de l'accepter. C'est l'inaction, et non l'imperfection, qui coûte le plus cher.

Nous devons agir dès maintenant pour réduire les risques auxquels sont exposées les Canadiennes et les Canadiens, tout en respectant les mécanismes qui protègent leur vie privée. Le projet de loi C-8 permet d'atteindre cet équilibre.

Pour conclure, le projet de loi C-8 est le reflet d'une gouvernance responsable. Il renferme des mesures proactives, proportionnées et fondées sur des données probantes. Il permet de réduire à la fois la probabilité et la gravité des préjudices futurs. C'est pourquoi je vous invite instamment à soutenir son adoption.

Merci.

Le vice-président : Merci, madame Quaid.

Ali Ghorbani, professeur et directeur, chaire de recherche du Canada de niveau 1 en cybersécurité, Université du Nouveau-Brunswick, à titre personnel : Bonsoir. Je suis heureux d'être parmi vous aujourd'hui pour cette discussion sur le renforcement des capacités législatives et stratégiques du Canada en matière de cybersécurité.

Comme on vous l'a dit, je m'appelle Ali Ghorbani. Je suis professeur d'informatique à l'Université du Nouveau-Brunswick, titulaire d'une Chaire de recherche du Canada de niveau 1 en cybersécurité et directeur fondateur de l'Institut canadien de cybersécurité, le premier institut canadien consacré à la cybersécurité. Créé il y a 10 ans, il est aujourd'hui un centre de premier plan en matière de recherche, de formation et de collaboration.

Bien que l'importance de la protection des infrastructures essentielles du Canada ait déjà été largement soulignée, je tiens à insister sur un point fondamental : la cybersécurité n'est plus uniquement une question technique; elle est au cœur de notre mode de vie, de notre sécurité nationale, de notre puissance nationale, de notre stabilité économique, de nos valeurs sociétales et de la confiance du public.

Canada's critical infrastructure is increasingly exposed to sophisticated threats from state-sponsored actors, organized cybercriminal groups and rapidly evolving technologies. These risks are compounded by systemic challenges, including outdated regulatory frameworks, inconsistent information sharing, the under-reporting of cyber incidents and deep interdependencies across critical assets and sectors.

In this context, Bill C-8 is an important step forward, albeit a bit too late. It reflects the reality that telecommunications and digital infrastructure are foundational to Canada's security, economy and public services. By strengthening regulatory expectations and enabling more timely intervention, the bill enhances Canada's ability to respond to significant cyber-threats, including those targeting critical infrastructure.

I support the objectives of Bill C-8. The bill introduces consequential updates to Canada's cybersecurity legislative framework and marks an important shift from a largely voluntary best-practices model to a more structured, mandatory, regulatory approach for critical infrastructure providers.

From an operational perspective, I view the bill as a positive development. It enables faster, more coordinated responses to significant cyber-threats and reduces delays in mitigating sophisticated attacks, including state-sponsored campaigns targeting critical infrastructure and telecommunications systems.

At the same time, implementation must be carefully balanced with strong safeguards, including transparency, independent oversight, privacy protections and continued support for encryption, research and innovation. Centralized authorities must be designed to avoid introducing systemic vulnerabilities or undermining public trust.

That reflects a broader tension in the bill: strengthening Canada's physical and digital infrastructure while centralizing command and coordination in response to cyber incidents.

Finally, legislation alone is not sufficient. Long-term cyber resilience depends upon a comprehensive national strategy that combines effective regulation with sustained investments in research, innovation, workforce development, public awareness and strong collaboration across government, industry and academia.

Thank you very much, and I look forward to your questions.

Les infrastructures essentielles du Canada sont de plus en plus exposées à des menaces complexes émanant d'acteurs soutenus par des États, de groupes cybercriminels organisés et de technologies en constante évolution. Ces risques sont aggravés par des défis systémiques, notamment des cadres réglementaires dépassés, un échange de renseignements inégal, une sous-déclaration des incidents cybernétiques et de profondes interdépendances entre les actifs et les secteurs critiques.

Dans ce contexte, le projet de loi C-8 constitue une avancée importante, bien qu'un peu tardive. Il reflète la réalité que les télécommunications et les infrastructures numériques sont essentielles à la sûreté, à l'économie et aux services publics du Canada. En renforçant les exigences réglementaires et en favorisant une intervention plus rapide, le projet de loi améliore la capacité qu'a le Canada de faire face aux cybermenaces majeures, notamment celles qui visent les infrastructures essentielles.

Je soutiens les objectifs du projet de loi C-8. Ce projet de loi apporte des mises à jour importantes au cadre législatif canadien en matière de cybersécurité et marque un tournant décisif, passant d'un modèle fondé en grande partie sur des pratiques exemplaires volontaires à une approche réglementaire plus structurée et obligatoire pour les fournisseurs d'infrastructures essentielles.

D'un point de vue opérationnel, je considère ce projet de loi comme une avancée positive. Il permet d'intervenir plus rapidement et de façon mieux coordonnée aux cybermenaces majeures et de réduire les délais nécessaires pour mettre en œuvre les mesures d'atténuation visant à contrer les attaques complexes, notamment les campagnes soutenues par des États visant les télécommunications et les infrastructures essentielles.

Parallèlement, la mise en œuvre doit être soigneusement équilibrée par des mesures de protection solides, notamment en matière de transparence, de contrôle indépendant, de protection de la vie privée et de soutien continu au chiffrement, à la recherche et à l'innovation. Les autorisations centralisées doivent être conçues de manière à éviter de créer des vulnérabilités systémiques ou de compromettre la confiance du public.

Cela reflète une tension plus générale à l'intérieur du projet de loi : renforcer les infrastructures physiques et numériques du Canada tout en centralisant le commandement et la coordination en cas de cyberincidents.

Enfin, la législation à elle seule ne suffit pas. La cyberrésilience à long terme repose sur une stratégie nationale globale qui allie une réglementation efficace à des investissements soutenus dans la recherche, l'innovation, le perfectionnement de la main-d'œuvre, la sensibilisation du public et une collaboration étroite entre les pouvoirs publics, le secteur privé et le milieu universitaire.

Merci beaucoup, et j'attends vos questions avec impatience.

The Deputy Chair: Thank you, Mr. Ghorbani.

Aaron Shull, Research Director, Centre for International Governance Innovation: Chair and members of the committee, thank you for the opportunity to appear before you on Bill C-8.

For context, I appeared in front of the Public Safety and National Security Committee in the other place last October. They took a lot of my suggested amendments on board. It was quite a technical takedown of the bill, so that makes my job here easy. I am going to urge you to do one thing, which is to pass the bill.

Let me begin with the threat environment because that's why we're all here. It is trite to say that our electrical grids, pipelines, telecommunications, water systems and financial networks are the arteries of modern life, but the point is that they're all increasingly automated and under sustained pressure from sophisticated state-sponsored adversaries who are not simply stealing data any longer; they are pre-positioning to disrupt.

This is not an academic concern. Salt Typhoon told us what happens when telecommunications networks are penetrated at scale. Volt Typhoon told us that pre-positioning in operational technology is no longer a hypothetical, and every operator I work with has stories about the rising tempo of intrusions against industrial control systems.

The problem is that too often, we can't tell if an outage was a fault or a foreign intrusion. The honest answer is that we just don't know. That is a posture this country cannot afford.

In my view, Bill C-8 is the foundation to change that. It establishes a unified framework across federally regulated critical sectors and gives governments the tools to compel the hardening of the systems Canadians depend upon.

Also, the work done by the House Public Safety and National Security Committee has produced a meaningfully better bill. It is tighter on privacy, more procedurally disciplined and now contains a mandatory five-year review. I'll come back to that. Also, as I said, several of the points I raised in October were addressed.

Le vice-président : Merci, monsieur Ghorbani.

Aaron Shull, directeur de recherche, Centre pour l'innovation dans la gouvernance internationale : Monsieur le président et distingués membres du Comité, je vous remercie de me donner l'occasion de m'exprimer devant vous au sujet du projet de loi C-8.

Pour vous donner un peu de contexte, j'ai témoigné devant le Comité permanent de la sécurité publique et nationale de l'autre chambre en octobre dernier. Ils ont retenu bon nombre des amendements que j'avais proposés. Il s'agissait d'une analyse assez technique du projet de loi, et en comparaison, ma tâche ici est plutôt facile. Je vais vous exhorter à faire une seule chose : adopter ce projet de loi.

Je commencerai par évoquer l'environnement des menaces, car c'est bien pour cela que nous sommes tous ici. Il est certes banal de dire que nos réseaux électriques, nos pipelines, nos infrastructures de télécommunications, nos réseaux d'approvisionnement en eau et nos réseaux financiers constituent les artères de la vie moderne, mais le fait est qu'ils sont tous de plus en plus automatisés et soumis à une pression constante de la part d'adversaires avancés soutenus par des États, qui ne se contentent plus de voler des données; ils effectuent un déploiement en vue de provoquer des perturbations.

Il ne s'agit pas là d'une simple préoccupation théorique. L'opération Salt Typhoon nous a montré ce qui se passe lorsque les réseaux de télécommunications sont infiltrés à grande échelle. L'opération Volt Typhoon nous a démontré que le déploiement dans les technologies opérationnelles n'est plus une hypothèse, et tous les exploitants avec lesquels je travaille ont des exemples à citer concernant l'intensification des intrusions visant les systèmes de contrôle industriels.

Le problème, c'est que trop souvent, nous ne pouvons pas déterminer si une panne est due à une défaillance ou à une intrusion étrangère. En toute honnêteté, nous n'en savons tout simplement rien. C'est une situation que ce pays ne peut plus endurer.

À mon avis, le projet de loi C-8 constitue le fondement nécessaire pour changer cet état des choses. Il établit un cadre unifié pour l'ensemble des secteurs essentiels relevant de la compétence fédérale et donne aux gouvernements les outils nécessaires pour imposer le renforcement des systèmes dont dépendent les Canadiennes et Canadiens.

Par ailleurs, les travaux menés par le Comité permanent de la sécurité publique et nationale de la Chambre ont abouti à un projet de loi nettement amélioré. Il est plus strict en matière de protection de la vie privée, plus rigoureux sur le plan procédural et prévoit désormais un réexamen obligatoire tous les cinq ans. J'y reviendrai. De plus, comme je l'ai dit, plusieurs des points que j'avais soulevés en octobre ont été pris en compte.

I want to address what I think is the constitutional elephant in the room. I watched the other witnesses, and I have a good sense of what's going on and am wise to the debate. There is a serious argument, which has been advanced by the Intelligence Commissioner, the Citizen Lab, the Canadian Civil Liberties Association and the Conservative caucus — all groups I have a tremendous amount of respect for — that clause 15.4 should require prior judicial authorization. There are real foundations to that argument. The Supreme Court of Canada's 2024 decision in *Bykovets* brought subscriber and IP data inside section 8 of the Charter, and the doctrinal starting point is *Hunter et al. v. Southam Inc.* That all favours a warrant.

However, on balance, I nevertheless support the passage of this bill as it stands. That is because the *Branch* and *Jarvis* cases recognize that regulatory compulsion of information from regulated entities for regulatory purposes operates under a Charter regime that is more permissive than the criminal-investigation warrant model.

The bill places major orders at the Governor-in-Council level, subjects them to NSIRA and NSICOP review, provides for post hoc judicial review by a designated Federal Court judge and now requires factor-based decision making at the issuing stage. That is serious oversight architecture. The constitutional questions are arguable, but they will be litigated in some form, which is okay. Kate Robertson said she doesn't want the bill to be dragged into the muck of constitutional litigation, but — while I have a tremendous amount of respect for Kate — I don't think that would be a bad thing. I don't think constitutional litigation is "muck" or a quagmire; I think that is another branch of government doing precisely what it is designed to do.

The five-year statutory review, which I mentioned, is the right vehicle for recalibration if the operational record reveals that the harms of the existing scheme are too great.

So, I would urge this committee to do one thing: weigh the cost of delay.

Bill C-26 passed both chambers. It died on the Order Paper. Canada lost more than two years of critical infrastructure protection because the legislative process did not finish. I can tell you for sure that our adversaries did not take those two years off.

Je voudrais aborder ce qui me semble être l'éléphant constitutionnel dans la pièce. J'ai écouté les autres témoins, j'ai une bonne idée de la situation et je connais bien les enjeux du débat. Il existe un argument sérieux, avancé par le commissaire au renseignement, le Citizen Lab, l'Association canadienne des libertés civiles et le caucus conservateur — autant de groupes pour lesquels j'ai un immense respect — selon lequel l'article 15.4 devrait exiger une autorisation judiciaire préalable. Cet argument repose sur des fondements solides. La décision rendue en 2024 par la Cour suprême du Canada dans l'affaire *Bykovets* a fait entrer les données d'abonnés et les données IP dans le champ d'application de l'article 8 de la Charte, et le point de départ doctrinal est l'affaire *Hunter et al. c. Southam Inc.* Tout cela plaide en faveur d'un mandat.

Toutefois, tout bien considéré, je soutiens néanmoins l'adoption de ce projet de loi tel qu'il est présenté. En effet, les arrêts *Branch* et *Jarvis* reconnaissent que l'obligation réglementaire faite aux entités réglementées de fournir des renseignements à des fins réglementaires s'inscrit dans un cadre prévu par la Charte qui est plus souple que le modèle du mandat d'enquête pénale.

Le projet de loi place les ordonnances majeures sous la compétence du gouverneur en conseil, les soumet à l'examen de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, l'OSSNR, et du Comité des parlementaires sur la sécurité nationale et le renseignement, le CPSNR, prévoit un contrôle judiciaire a posteriori par un juge désigné de la Cour fédérale et impose désormais une prise de décision fondée sur des critères objectifs dès la phase d'émission. Il s'agit là d'un mécanisme de contrôle rigoureux. Les questions constitutionnelles sont discutables, mais elles feront l'objet d'un litige sous une forme ou une autre, ce qui n'est pas un problème. Kate Robertson a déclaré qu'elle ne souhaitait pas que le projet de loi soit entraîné dans le bourbier des litiges constitutionnels, mais — bien que j'aie un immense respect pour Mme Robertson — je ne pense pas que ce serait une mauvaise chose. Je ne pense pas que les litiges constitutionnels soient un bourbier ou un marécage; je pense qu'il s'agit d'une autre branche du gouvernement qui fait précisément ce pour quoi elle a été conçue.

L'examen législatif quinquennal, dont j'ai parlé, constitue le moyen approprié pour procéder à un réajustement si l'expérience acquise sur le terrain révèle que les inconvénients du mécanisme en vigueur sont trop importants.

J'invite donc ce comité à faire une chose : bien soupeser le coût d'un report.

Le projet de loi C-26 a été adopté par les deux Chambres pour ensuite mourir au Feuilleton. Le Canada a perdu plus de deux ans en matière de protection des infrastructures essentielles parce que le processus législatif n'a pas abouti. Je peux vous

Operators are now waiting for two things from Parliament. The first is the certainty of an act that is in force. The second is regulations that will tell them what compliance actually means. Every additional week without that certainty is a week during which investment is deferred, hard governance conversations are deferred and adversaries continue their work uncontested.

To be sure, Bill C-8 is not perfect, but the threat surfaces are evolving faster than statutes can anyway. That is precisely why the five-year review matters and why the regulations that will follow the act will matter at least as much as the wording of the act itself.

The work that the House did, in my humble estimation, produced a workable, principled framework that addresses an urgent national security gap. Canada's critical infrastructure operators and the Canadians who rely upon the systems they run are waiting for Parliament to finish what it started.

Thank you, and I would be pleased to answer the committee's questions.

The Deputy Chair: Thank you, Mr. Shull.

We will now proceed to questions. Colleagues, our guests will be with us until 7 p.m.

Senator Cardozo: Welcome to all the witnesses; Mr. Ghorbani, even though you're far away, you're close at hand. Thank you for joining us today.

Ms. Quaid, could you tell us more about the Canadian Cyber Threat Exchange and how you came to the position on this bill that you have?

Ms. Quaid: The Canadian Cyber Threat Exchange is a private-sector, member-based not-for-profit. The reason for our existence is to enable our member companies — there are more than 200 of them — to share cyber information to build resilience in themselves and in each other. Cybersecurity absolutely cannot be a competitive advantage in any sector or organization. It is a team sport, and if we're not sharing information, we are already behind.

affirmer sans hésitation que nos adversaires n'ont pas profité de ces deux années pour se reposer.

Les exploitants attendent désormais deux choses du Parlement. La première est la certitude qu'une loi est en vigueur. La seconde est un règlement qui leur précisera ce que signifie concrètement la conformité. Chaque semaine supplémentaire passée sans cette certitude est une semaine durant laquelle les investissements sont reportés, les discussions difficiles sur la gouvernance sont retardées et les adversaires poursuivent leurs activités sans rencontrer d'opposition.

Certes, le projet de loi C-8 n'est pas parfait, mais les menaces évoluent de toute façon plus vite que les lois. C'est précisément pour cette raison que l'examen quinquennal revêt une importance particulière et que les règlements qui découleront de la loi auront au moins autant d'importance que le libellé de la loi en soi.

À mon humble avis, les travaux menés par la Chambre ont abouti à un cadre applicable et fondé sur des principes qui comble une lacune urgente en matière de sécurité nationale. Les exploitants d'infrastructures essentielles du Canada et les Canadiennes et Canadiens qui dépendent des systèmes qu'ils gèrent attendent que le Parlement mène à bien ce qu'il a commencé.

Merci, et je suis impatient de répondre aux questions du comité.

Le vice-président : Merci, monsieur Shull.

Nous allons maintenant passer aux questions. Chers collègues, nos invités resteront avec nous jusqu'à 19 heures.

Le sénateur Cardozo : Bienvenue à tous les témoins; monsieur Ghorbani, même si vous êtes loin, vous êtes tout près de nous. Merci de vous joindre à nous aujourd'hui.

Madame Quaid, pourriez-vous nous en dire plus sur l'Échange canadien de menaces cybernétiques et nous expliquer comment vous en êtes venue à adopter la position que vous défendez concernant ce projet de loi?

Mme Quaid : L'Échange canadien de menaces cybernétiques est un organisme sans but lucratif du secteur privé, fonctionnant sur la base d'adhésions. Notre raison d'être est de permettre à nos plus de 200 entreprises membres d'échanger des renseignements sur la cybersécurité afin de renforcer leur résilience ainsi que celle de leurs partenaires. La cybersécurité ne doit en aucun cas constituer un avantage concurrentiel pour un secteur ou une organisation. C'est un travail d'équipe, et si nous ne partageons pas nos renseignements, nous sommes déjà en retard.

Regarding the position I have on this bill, I have appeared before various other committees on this bill. At those times, I was, at the instruction of members, requesting certain changes and amendments to the bill. It was early in the process.

At this point, I am hearing from our members that this bill needs to pass. This bill represents basic table stakes in the cybersecurity world now. When it started down its path five or six years ago, the world was not a fabulous place for those in cybersecurity. The criminals were coming at us fast and furious. Let me tell you: It has not slowed down. In fact, it has got much worse.

We now have ransom as a service. Why develop your own code when you can just go online and rent it? Don't buy it. By the way, it comes with a guarantee and a help desk. That is common now.

This bill will set the bar for our critical infrastructure and its supply chain. It's not just the organizations that are being legislated. They are going to force their entire supply chain to elevate their cybersecurity, and that's what we need.

Senator Cardozo: Thank you. If I might, I will ask Professor Ghorbani the same question with regard to the Canadian Institute for Cybersecurity. Tell us a little bit about it and how you came to the position you put forward today.

Mr. Ghorbani: The Canadian Institute for Cybersecurity, or CIC, is within the University of New Brunswick, but it is a self-sustaining institute. We don't receive any money from anyone.

We work with industry, primarily large industry, but we also support medium and small enterprises as well. We work on their problems year-round. The institute has over 100 researchers, and we have members from critical infrastructure like power utilities, financial institutions, banks and companies that build cybersecurity solutions. They are our members. Our team works with them year-round on the types of problems that they have, whether it's defence-related, finance-related or work related to smartgrid. We see how important it is for us to be able to act quickly on threats that are coming toward us and compromises that occur.

To date, as I mentioned, many of the security measures are voluntary-based, whether it's information sharing regarding the compromises or acting toward a compromise. It's not really regulated, and it's not centralized. I think Bill C-8 allows the

En ce qui concerne ma position sur ce projet de loi, j'ai déjà témoigné devant plusieurs autres comités à ce sujet. À ces occasions, j'avais, à la demande des membres, demandé que certaines modifications et certains amendements y soient apportés. C'était au tout début du processus.

À ce stade, nos membres me font savoir que ce projet de loi doit être adopté. Ce projet de loi représente désormais un minimum indispensable dans le domaine de la cybersécurité. Lorsqu'il a commencé son cheminement il y a cinq ou six ans, la situation n'était pas rose pour les professionnels de la cybersécurité. Les cybercriminels nous attaquaient sans relâche. Je peux vous l'assurer : cela ne s'est pas calmé. En réalité, la situation s'est considérablement aggravée.

Il existe désormais des services de rançongiciels à la demande. Pourquoi développer son propre code alors qu'il suffit d'aller sur Internet pour en louer un? Ne l'achetez pas. D'ailleurs, il est assorti d'une garantie et d'un service d'assistance. C'est désormais monnaie courante.

Ce projet de loi fixera la norme pour nos infrastructures essentielles et leurs chaînes d'approvisionnement. Ce ne sont pas seulement les organisations qui seront soumises à cette loi. Elles vont contraindre l'ensemble de leurs chaînes d'approvisionnement à relever leur niveau de cybersécurité, et c'est exactement ce dont nous avons besoin.

Le sénateur Cardozo : Merci. Si vous me le permettez, j'aimerais poser la même question au professeur Ghorbani au sujet de l'Institut canadien de cybersécurité. Pouvez-vous nous en dire un peu plus à ce sujet et nous expliquer comment vous en êtes venu à la position que vous défendez aujourd'hui?

M. Ghorbani : L'Institut canadien de cybersécurité fait partie de l'Université du Nouveau-Brunswick, mais c'est un institut autonome. Nous ne recevons aucun financement de la part de qui que ce soit.

Nous travaillons avec le secteur industriel, principalement les grandes entreprises, mais nous soutenons aussi les entreprises moyennes et petites. Nous travaillons sur leurs problèmes toute l'année. L'institut compte plus de 100 chercheurs, et nous avons parmi nos membres des acteurs d'infrastructures critiques tels que des services publics d'électricité, des institutions financières, des banques et des entreprises qui développent des solutions de cybersécurité. Ce sont nos membres. Notre équipe collabore avec eux toute l'année sur les types de problèmes auxquels ils sont confrontés, qu'ils soient liés à la défense, à la finance ou aux réseaux intelligents. Nous constatons combien il est important d'être capables d'agir rapidement face aux menaces qui se présentent et aux compromissions qui surviennent.

À ce jour, comme je l'ai mentionné, la plupart des mesures de sécurité reposent sur le volontariat, que ce soit le partage d'information concernant les compromissions ou l'action face à une compromission. Ce n'est pas vraiment réglementé ni

country to be responsive and to mitigate problems as quickly as possible in order to reduce damages and costs.

We never talk about the public safety part of the costs or the costs of societal pain that we feel in anything that happens. There are many examples I could give you. Three weeks ago, in Toronto, a fake cell tower affected millions of basic cellphones and brought them down to a point where they were not able to communicate for some time.

It is a societal pain and an economic pain that Bill C-8 will attend to, ensuring that we attend to compromises quickly.

The Deputy Chair: Thank you, Mr. Ghorbani and Mr. Shull.

Senator Yussuff: Thank you, witnesses, for being here. We are talking about cybersecurity. As you know, the federal government's jurisdiction in this country is a certain size. The provincial governments' are a certain size. Then, of course, you have municipal governments to layer on top of that.

Bill C-8 gives the federal government clear responsibility and authority, but the broader challenge we face as a country is in other jurisdictions because we don't have one system in this country to protect Canadians. We recognize that there is a lot of sharing of information and a lot of good practices to do that, but each jurisdiction does its own thing in that regard.

Isn't this a real challenge for the country? Given the seriousness of cybersecurity, do you think we should get to a better place than where we're at given that we're a federation and it is complicated to get other governments to either give up some of their authority or to relinquish some of their oversight in how we can do a better job of protecting this country? We're talking about protecting the country, but the reality is we're not actually talking about protecting the country because the federal government does not have jurisdiction over the other sectors of this country, which is far vaster than the federal government's authority.

I'll leave that to each one of you to respond to and give your own observation on.

Mr. Shull: You're absolutely right. I see your point, and I raise you an exclamation mark. You hit the nail squarely on the head.

Let's deal with it. The actual thing I worry about is municipalities because the federal government touches people in areas that I don't think most Canadians feel on a daily basis. It's super important, but it's, for example, national defence or national security. But if your kid's school goes dark, the hospital

centralisé. Je pense que le projet de loi C-8 permet au pays d'être réactif et d'atténuer les problèmes le plus rapidement possible afin de réduire les dommages et les coûts.

On ne parle jamais de la part des coûts liés à la sécurité publique ni des coûts de la souffrance sociétale que nous ressentons à chaque incident. Je pourrais vous donner de nombreux exemples. Il y a trois semaines, à Toronto, une fausse tour cellulaire a affecté des millions de téléphones cellulaires basiques, les rendant inopérants au point qu'ils n'ont pas pu communiquer pendant un certain temps.

C'est une souffrance sociale et économique que le projet de loi C-8 prendra en compte, en veillant à ce que les compromissions soient traitées rapidement.

Le vice-président : Merci, messieurs Ghorbani et Shull.

Le sénateur Yussuff : Je remercie les témoins d'être ici. Nous parlons de cybersécurité. Comme vous le savez, la compétence du gouvernement fédéral au Canada a une certaine portée. Celle des gouvernements provinciaux en a une autre. Et il y a, bien sûr, les gouvernements municipaux qui viennent s'ajouter à cela.

Le projet de loi C-8 confère au gouvernement fédéral une responsabilité et une autorité claires, mais le défi plus large auquel nous faisons face comme pays se situe dans les autres administrations, car nous n'avons pas un système unique au pays pour protéger les Canadiens. Nous reconnaissons qu'il y a beaucoup de partage d'information et de bonnes pratiques à cet égard, mais chaque administration agit de son côté.

N'est-ce pas là un véritable défi pour le pays? Compte tenu de l'importance cruciale de la cybersécurité, pensez-vous que nous devrions parvenir à une situation plus satisfaisante que celle dans laquelle nous nous trouvons actuellement, sachant que nous sommes une fédération et qu'il est difficile de convaincre les autres gouvernements d'abandonner une partie de leur autorité ou de céder une partie de leur contrôle pour nous permettre de mieux protéger le pays? Nous parlons de protéger le pays, mais en réalité ce n'est pas vraiment de cela que nous parlons, car le gouvernement fédéral n'a pas compétence sur les autres secteurs de ce pays, qui est bien plus vaste que le pouvoir fédéral.

Je laisse à chacun de vous le soin de répondre à cette question et d'apporter son propre point de vue.

M. Shull : Vous avez tout à fait raison. Je comprends votre point, et j'y ajoute un point d'exclamation. Vous avez mis dans le mille.

Allons droit au but. Ce qui m'inquiète vraiment, ce sont les municipalités, car le gouvernement fédéral intervient dans des secteurs qui, selon moi, ne touchent pas la plupart des Canadiens dans leur vie quotidienne. C'est extrêmement important, mais ce sont, par exemple, la défense nationale ou la sécurité nationale.

goes down, the water stops coming out of the tap or your garbage stops getting picked up, those are things that people would tend to notice. Most of those responsibilities are municipal, and that is unequivocally where our greatest threat vector is.

For what it's worth, at the federal level, I'm not really worried about you. You have CSE on your network. You'll be fine, but if you're in Advocate Harbour, Nova Scotia, or Bobcaygeon, Ontario, you have Fred the IT guy who works on Tuesdays and half days on Thursdays. That is absolutely one of the most important gaps. We can't deal with it in this bill, unfortunately, because of section 91 and section 92 of the Constitution Act, but I absolutely agree with you.

Ms. Quaid: I feel your pain on this, and you are quite correct. There are so many disparate, fractured systems, but we have to start somewhere, and this is a good place to start. If the federal government can pass this legislation, it will strengthen those four sectors and their critical supply chains. Those suppliers also supply others, so there will be a trickle-down effect on the overall economy, and perhaps the provinces will follow. I mean, what is it they say? "The best day to have started something was yesterday. The second-best day is today."

Mr. Ghorbani: I would say that's a real question, and it deserves a good answer.

As far as Bill C-8 goes, the areas that it covers — mainly telecommunications, banking, grid construction and others — are mainly also expanded to provinces.

In other words, in some ways, this bill covers the country from a cybersecurity perspective but doesn't cover all — and this needs its own attention, as was mentioned before — health care, for example. It doesn't cover municipalities and so forth. Those are coming into question.

It does cover, through these four major areas that Bill C-8 covers, other third-party providers, either within the country from various provinces or from outside the country.

Generally speaking, Bill C-8 does its work covering the country. However, there are elements of cybersecurity that are definitely left out of this bill and need their own attention. Health care would be one of them.

Senator Yussuff: Maybe I can ask you this, Ms. Quaid, because you represent a large extent of the private sector in your network: Obviously, they see the necessity of the bill and want the bill passed, but given their challenges and recognizing the fragmentation of the country and how we're dealing with

Mais si l'école de votre enfant perd l'électricité, si l'hôpital ferme, si l'eau ne sort plus du robinet ou si vos ordures ne sont plus collectées, ce sont des choses que les gens remarquent. La plupart de ces responsabilités relèvent des municipalités, et c'est sans aucun doute là que réside notre plus grand vecteur de menace.

Pour ce que ça vaut, au niveau fédéral, je ne m'inquiète pas vraiment pour vous. Vous avez le CST sur votre réseau. Vous serez bien protégés, mais si vous êtes à Advocate Harbour, en Nouvelle-Écosse, ou à Bobcaygeon, en Ontario, vous avez Fred, le technicien informatique qui vient travailler le mardi et une demi-journée le jeudi. C'est sans aucun doute une des lacunes majeures. Nous ne pouvons malheureusement pas y remédier dans ce projet de loi à cause des articles 91 et 92 de la Loi constitutionnelle, mais je vous rejoins entièrement.

Mme Quaid : Je ressens votre frustration et vous avez raison. Il y a tant de systèmes disparates et fragmentés, mais il faut bien commencer quelque part, et c'est un bon point de départ. Si le gouvernement fédéral parvient à faire adopter ce projet de loi, cela renforcera ces quatre secteurs et leurs chaînes d'approvisionnement critiques. Ces fournisseurs desservent aussi d'autres acteurs, donc cela aura un effet d'entraînement sur l'économie dans son ensemble, et peut-être que les provinces emboîteront le pas. Comme on dit : « Le meilleur jour pour commencer quelque chose était hier. Le deuxième meilleur jour, c'est aujourd'hui. »

M. Ghorbani : Je dirais que c'est une vraie question et qu'elle mérite une bonne réponse.

En ce qui concerne le projet de loi C-8, les domaines qu'il couvre — principalement les télécommunications, le secteur bancaire, la construction de réseaux électriques et d'autres — relèvent aussi en grande partie de la compétence des provinces.

En d'autres termes, ce projet de loi couvre le pays du point de vue de la cybersécurité, mais ne couvre pas tous les secteurs — ce qui mérite une attention particulière, comme on l'a déjà mentionné —, par exemple la santé. Il ne couvre pas non plus les municipalités. Ces questions font l'objet de discussions.

Il couvre, par le biais de ces quatre grands secteurs que vise le projet de loi C-8, d'autres fournisseurs tiers, qu'ils soient situés au pays, dans diverses provinces, ou à l'étranger.

Dans l'ensemble, le projet de loi C-8 couvre le pays. Cependant, certains aspects de la cybersécurité sont clairement exclus de ce projet de loi et nécessitent une attention distincte. Le secteur de la santé en fait partie.

Le sénateur Yussuff : Permettez-moi de vous poser cette question, madame Quaid, étant donné que vous représentez une grande partie du secteur privé au sein de votre réseau : bien sûr, ses acteurs comprennent la nécessité de ce projet de loi et souhaitent qu'il soit adopté, mais compte tenu des défis auxquels

cybersecurity, is there a clarion call for us to do better with respect to how we can bring all these systems together?

I ask because when Canadians are faced with a crisis, they don't really distinguish between a province, a municipality or the federal government; they want their governments to solve the problem and ensure they never have to face that problem again because they are just people who want to be protected.

How can we do that with the organization that you represent, recognizing we don't currently have a system to do that? How can we move to create a system where such a vision is thought about for the future?

Because this, of course, still leaves that big gap within the system as to how we can work better with each other to ensure we have a better outcome.

Ms. Quaid: I would suggest that it starts with this bill and then trickles down. Large critical infrastructure is going to require their suppliers to be more secure.

Those suppliers are going to require their suppliers to be more secure. There will be a knock-on effect that will start to impact smaller and smaller organizations. Can we do more? Of course we can. There is always more to do. It is cybersecurity. It is a game of Whack-a-Mole.

Perhaps one of the areas we can do more is by providing better, clearer advice, guidance and incentives to small and medium businesses. Small and medium businesses make up 99% of our economy. We are not able to convince them of the need to ensure their own security.

I've run small and medium businesses most of my life. You are concerned with making payroll. As Mr. Shull said, you're lucky if you have a guy that comes in a half day every month to look at your systems.

Give them a real incentive to do more and not just an opportunity for certification. What does that look like? Wiser minds than mine would have to take a look. But there are many things we could be doing — tax or insurance breaks — to get our small businesses to be cyber secure and cyber aware.

But I would also challenge that it starts with education. A million years ago, and I'm now dating myself, we had a program in Canada called ParticipACTION, a fabulous program run by the federal government, which, by the way, doesn't run

ils sont confrontés et compte tenu de la fragmentation du pays ainsi que de la manière dont nous abordons la cybersécurité, y a-t-il un appel pressant à faire pour mieux pour parvenir à harmoniser tous ces systèmes?

Je pose cette question parce que, lorsque les Canadiens sont confrontés à une crise, ils ne font pas vraiment de distinction entre une province, une municipalité ou le gouvernement fédéral; ils veulent que leurs gouvernements règlent le problème et s'assurent qu'ils n'auront plus jamais à y être confrontés, car ils veulent seulement être protégés.

Comment pouvons-nous y parvenir avec l'organisation que vous représentez, sachant que nous ne disposons pas actuellement d'un système pour cela? Comment pouvons-nous créer un système où une telle vision est prise en compte pour l'avenir?

Car cela laisse évidemment un vide important dans le système quant à la manière dont nous pouvons mieux collaborer pour obtenir de meilleurs résultats.

Mme Quaid : Je dirais que cela commencera avec ce projet de loi, puis se répercutera en aval. Les grandes infrastructures critiques auront besoin que leurs fournisseurs soient plus sécurisés.

Ces fournisseurs exigeront de leurs fournisseurs qu'ils renforcent leur sécurité. Il y aura un effet domino qui finira par toucher des organisations de plus en plus petites. Pouvons-nous faire plus? Bien sûr que oui. Il y a toujours plus à faire. C'est la cybersécurité. C'est un jeu de « casse-tête chinois ».

Peut-être qu'un domaine où nous pourrions en faire davantage consiste à fournir de meilleurs conseils, des orientations et des incitatifs clairs aux petites et moyennes entreprises. Les PME représentent 99 % de notre économie. Nous n'arrivons pas à les convaincre de la nécessité d'assurer leur propre sécurité.

J'ai dirigé des petites et moyennes entreprises la majeure partie de ma vie. Vous êtes surtout préoccupé par la paie. Comme l'a dit M. Shull, vous avez de la chance s'il y a quelqu'un qui vient une demi-journée par mois pour vérifier vos systèmes.

Il faut leur offrir une véritable incitation à faire plus, et pas seulement la possibilité d'obtenir une certification. À quoi cela pourrait-il ressembler? Des esprits plus avisés que le mien devraient se pencher sur la question. Mais il y a beaucoup de mesures possibles — des allègements fiscaux ou des avantages en matière d'assurance — pour inciter nos petites entreprises à renforcer leur cybersécurité et leur vigilance.

Mais je dirais aussi que tout commence par l'éducation. Il y a bien longtemps, et cela trahit mon âge, nous avions au Canada un programme appelé ParticipACTION, un programme formidable géré par le gouvernement fédéral qui, soit dit en passant, ne

education. They kind of just did it on a very low budget. It encouraged all Canadians to be fit. We were taught in school at the age-appropriate level about physical fitness. Why are we not doing the same thing with cybersecurity?

The minute you put a device in a child's hand, you have a responsibility to ensure that they understand the device and what it can do.

The Deputy Chair: Thank you.

Senator McNair: Ms. Quaid, thank you for reminding us that the privacy legislation is already in place. Privacy, to some extent, is protected.

Mr. Shull, you talked about amendments to the legislation, which put more guardrails around some of that.

One of the witnesses last week said the biggest threats to Canadians' privacy are the actual cybersecurity incidents that Bill C-8 is meant to prevent — or hopes to prevent. Do you want to comment or expand on that a bit?

Ms. Quaid: That witness was absolutely right. Privacy is critically important; it is the foundation of so much of what Canada is.

However, if we are so focused on protecting the individual's privacy from getting into the hands of our own government that we are losing sight of the fact that what we want to do is protect our privacy from getting into the hands of foreign governments or criminal elements, we've lost sight of the bigger picture.

While we sit here and talk about it and express concern over it, it feels quite a lot like Nero fiddling while Rome is burning around us.

This bill is designed to protect our privacy, plain and simple, from people who shouldn't have access to our information.

Mr. Shull: I'm in the same place as my colleague. I read the Privacy Commissioner's submissions. I've got a tremendous amount of respect for the Privacy Commissioner. I think he's brilliant, for what it's worth. That's on the record now.

However, the issue is warrant or no warrant — go or no go — and getting a warrant is a time-consuming process. There is information to obtain. There are affidavits. There are a lot of things that have to happen in order to get a warrant.

Other witnesses have already testified to this: This type of cybersecurity intrusion happens in seconds or minutes.

s'occupe pas de l'éducation. Il l'a fait avec un budget très modeste. Il encourageait tous les Canadiens à être en forme. À l'école, on nous enseignait le conditionnement physique à un niveau adapté à notre âge. Pourquoi ne faisons-nous pas la même chose avec la cybersécurité?

Dès qu'on remet un appareil à un enfant, on a la responsabilité de s'assurer qu'il comprend cet appareil et ce qu'il peut faire.

Le vice-président : Merci.

Le sénateur McNair : Madame Quaid, merci de nous rappeler que la législation en matière de protection de la vie privée est déjà en place. La vie privée est protégée, dans une certaine mesure.

Monsieur Shull, vous avez parlé des amendements législatifs qui renforcent les garde-fous dans ce domaine.

Un témoin a déclaré la semaine dernière que les plus grandes menaces pour la vie privée des Canadiens sont précisément les incidents de cybersécurité que le projet de loi C-8 vise à prévenir — ou espère prévenir. Voulez-vous nous faire part de votre opinion à ce sujet?

Mme Quaid : Ce témoin avait tout à fait raison. La vie privée est d'une importance cruciale; elle est à la base de ce qu'est le Canada.

Cependant, si nous nous concentrons tellement sur la protection de la vie privée des citoyens contre les intrusions de notre propre gouvernement que nous perdons de vue le fait que ce que nous voulons, c'est protéger notre vie privée contre les gouvernements étrangers ou les éléments criminels, nous perdons de vue la situation dans son ensemble.

Quand je nous vois assis ici en train d'en discuter et d'exprimer nos inquiétudes, cela me fait penser à Néron qui jouait de la lyre pendant que Rome brûlait.

Ce projet de loi est conçu pour protéger notre vie privée, tout simplement, contre ceux qui ne devraient pas avoir accès à nos données personnelles.

M. Shull : Je partage l'avis de ma collègue. J'ai lu les observations du commissaire à la vie privée. J'ai un immense respect pour le commissaire. Je le trouve brillant, pour ce que ça vaut. C'est maintenant consigné au compte rendu.

Cependant, la question est celle du mandat — s'il y a mandat ou non — et l'obtention d'un mandat est un long processus. Il faut collecter des informations, fournir des déclarations sous serment. Beaucoup de démarches sont nécessaires pour obtenir un mandat.

D'autres témoins l'ont déjà dit : ce type d'intrusion dans la cybersécurité se produit en quelques secondes ou minutes.

The orders that we are talking about are designed to protect critical systems, not to exfiltrate Canadians' personal data. As I said previously, there are a bunch of guardrails now currently in the bill.

But there is another issue too, and I want to put a fine point on this. You go to the Federal Court, to a designated judge who is a national security judge, and they are experts in that. But we're talking about cyber-threat intelligence. This is the all-source type of intelligence.

This requires a technical and operational context that the executive holds and judges typically don't. So a preauthorization would require a briefing of classified material to a depth that, in practice, would either be so cursory that it would be meaningless or so in-depth that it would be unworkably slow. That's the issue that we are dealing with here.

My concern is that we're going to push toward this privacy issue when we're talking about personally identifiable information of Canadians, which is not the subject of this bill, into a warrant regime that is going to make us less safe.

Senator McNair: Thank you.

Mr. Ghorbani, is there anything you wish to add?

Mr. Ghorbani: I would not add anything. Everything has been said.

However, from a technical perspective, I want to again emphasize the fact that these cyber-threats or cyberattacks will not wait until we do or do not get a warrant. By that time, millions of peoples' privacy could have been violated and their data could have been exposed, all because we wanted to do it in the way some say we should.

Having said that, it's important to have oversight and do it right at the implementation part. But I don't see waiting for this bill to be changed or amended because of privacy issues.

First, this bill is not violating privacy from what I can see technically. But even if there is some element in the future, which might be the case, then implementation and regulation could close the loop.

[*Translation*]

Senator Youance: My question is about technical standards and infrastructure resilience. Mr. Ghorbani just spoke about the rapid evolution of cyberthreats. Are the requirements proposed in

Les arrêtés dont nous parlons visent à protéger les systèmes critiques, pas à exfiltrer les données personnelles des Canadiens. Comme je l'ai dit, le projet de loi comporte actuellement toute une série de garde-fous.

Mais il y a un autre problème, et je tiens à souligner ce point. Vous vous adressez à la Cour fédérale, à un juge désigné spécialisé en sécurité nationale, et ces juges sont des experts en la matière. Mais nous parlons ici de renseignements sur les cybermenaces. Ce sont des renseignements provenant de toutes les sources.

Cela requiert un contexte technique et opérationnel que l'exécutif maîtrise, mais dont les juges ne disposent généralement pas. Ainsi, une autorisation préalable nécessiterait une présentation de documents classifiés d'une profondeur telle que, dans la pratique, elle serait soit si superficielle qu'elle serait dénuée de sens, soit si approfondie qu'elle serait d'une lenteur ingérable. C'est là le problème auquel nous sommes confrontés ici.

Je crains que nous ne nous orientions vers ce problème de protection de la vie privée lorsque nous parlons des renseignements personnels identifiables des Canadiens, qui ne font pas l'objet de ce projet de loi, en instaurant un régime de mandats qui va nuire à notre sécurité.

Le sénateur McNair : Merci.

Monsieur Ghorbani, souhaitez-vous ajouter quelque chose?

M. Ghorbani : Je n'ajouterais rien. Tout a été dit.

Cependant, d'un point de vue technique, je tiens à souligner une fois de plus que ces cybermenaces ou cyberattaques n'attendent pas que l'on obtienne ou non un mandat. Entretemps, la vie privée de millions de personnes peut avoir été violée et leurs données exposées, tout cela parce que nous avons voulu procéder comme certains le suggèrent.

Cela dit, il est important d'assurer une surveillance et de faire les choses correctement lors de la mise en œuvre. Mais je ne vois pas l'utilité d'attendre que ce projet de loi soit modifié ou amendé pour des raisons liées à la vie privée.

Premièrement, d'un point de vue technique, ce projet de loi ne porte pas atteinte à la vie privée, d'après ce que je peux voir. Mais même s'il y avait un élément qui pouvait poser problème à l'avenir, la mise en œuvre et la réglementation permettraient alors de combler les lacunes.

[*Français*]

La sénatrice Youance : Ma question concerne les normes techniques et la résilience des infrastructures. M. Ghorbani vient justement de parler des changements rapides en matière de

Bill C-8 flexible enough to keep pace with rapidly evolving cyberthreats?

I also have some questions specifically for Mr. Ghorbani.

Does the bill promote innovation in cybersecurity? How do you see the role of universities in applied research or the development of solutions?

[*English*]

Mr. Ghorbani: That is a very good question. In the last part of my opening remarks, I mentioned that I'm hoping, that in implementation and regulation, innovation and research, to strengthen and harden the defensive system are being considered for the future. As a result, I want to see that in the legislation. On the implementation side, the critical infrastructure owners are kind of mandated on the research, innovation, talent development and awareness programs that are needed for this bill to be really successful.

Canada's technical standing is fairly strong in cybersecurity, but this is not an area to be relaxed. With AI coming and AI attacks happening these days, as well as ransomware as a service and things of that nature, we must always stay at the edge of innovation. That's why, again, this bill is a great first step in ensuring we have tools to prevent or mitigate attacks as quickly as possible. However, at the same time, as part of this implementation, I want to see the government mandate more innovation, research and talent development in this area.

Ms. Quaid: To add to what Dr. Ghorbani said, one of the strengths of this bill — you have heard a lot about its weaknesses over the past several days, I'm sure — is that it is technology agnostic. It doesn't speak directly to AI or any other technology because we don't know what's coming. The bill is more based on the principles of collaboration and sharing information in a timely manner.

Mr. Shull: I don't think this is an innovation bill. If anything, it will make it harder for adversarial states to steal our secrets and intellectual property, which has been a big issue for a long time.

If we're talking about the critical cyber systems protection act, up and down, it's simple. It says you have to have a cybersecurity program and you have to tell us what it is. If something bad goes on, you have to tell us what happened, and

cybermenaces. Les exigences proposées dans le projet de loi C-8 sont-elles suffisamment flexibles pour suivre l'évolution rapide des cybermenaces?

De plus, j'aurais des questions plus particulièrement pour M. Ghorbani.

Le projet de loi favorise-t-il l'innovation en cybersécurité? Comment voyez-vous le rôle des universités dans la recherche appliquée ou dans le développement de solutions?

[*Traduction*]

M. Ghorbani : C'est une très bonne question. Dans la dernière partie de ma déclaration préliminaire, j'ai exprimé l'espoir que la mise en œuvre et la réglementation, l'innovation et la recherche chercheront à renforcer et à consolider le système de défense pour l'avenir. C'est pourquoi je souhaite que cela se reflète dans la loi. En ce qui concerne la mise en œuvre, les propriétaires d'infrastructures critiques sont en quelque sorte tenus de mener les programmes de recherche, d'innovation, de développement des compétences et de sensibilisation nécessaires pour que ce projet de loi soit couronné de succès.

Le Canada dispose d'un niveau technique assez solide en matière de cybersécurité, mais ce n'est pas un domaine où l'on peut se permettre de relâcher la vigilance. Avec l'avènement de l'IA et les attaques basées sur l'IA qui se produisent ces derniers temps, sans oublier les rançongiciels comme service et autres menaces de ce type, nous devons toujours rester à la pointe de l'innovation. C'est pourquoi, encore une fois, ce projet de loi constitue une excellente première étape pour nous doter des outils nécessaires afin de prévenir ou d'atténuer les attaques le plus rapidement possible. Néanmoins, parallèlement à cette mise en œuvre, je souhaite que le gouvernement encourage davantage l'innovation, la recherche et le développement des talents dans ce domaine.

Mme Quaid : Pour compléter ce qu'a dit M. Ghorbani, l'un des points forts de ce projet de loi — vous avez certainement beaucoup entendu parler de ses faiblesses ces derniers jours — est qu'il ne se limite pas à une technologie particulière. Il ne fait pas directement référence à l'IA ni à aucune autre technologie, car nous ne savons pas ce que l'avenir nous réserve. Ce projet de loi repose davantage sur les principes de collaboration et d'échange rapide de renseignements.

M. Shull : Je ne pense pas qu'il s'agisse d'un projet de loi en faveur de l'innovation. En fait, il sera plus difficile pour les États hostiles de voler nos secrets et notre propriété intellectuelle, ce qui constitue un problème majeur depuis longtemps.

Si l'on examine la Loi sur la protection des cybersystèmes essentiels sous tous ses aspects, c'est très simple. Elle stipule que vous devez établir un programme de cybersécurité et que vous devez nous dire en quoi il consiste. Si un incident survient, vous

we can tell you to patch your systems or implement solutions to make it harder for bad guys to get in.

I don't see this as an innovation-style bill. I see this as a security measure, which will, de facto, make innovation better, easier and more protected, but I see this as a security bill.

Senator Dasko: Thank you, witnesses. Ms. Quaid, some of your comments about medium and small businesses attracted my attention. I used to work in a medium-sized business in the private sector. What do you think the typical cost of prevention is for a company? I don't know if there is any such thing. You are rolling your eyes, so maybe I've asked a bad question.

Are we talking about significant costs for companies to buy the security that they need? Do you have any sense of what the cost factor is? It is tough for companies to invest in many of these kinds of things.

Ms. Quaid: It is extraordinarily difficult. The cost depends on how secure you want to be. My interest is in going into a small business and ensuring that they can identify what their critical systems are. We're not even talking about costs or technology. It is a matter of whether they can tell me what systems they need to operate their business tomorrow. If they can, can they tell me who has access? Again, we're not talking about cost. We're talking about policies, guidelines and practices.

Senator Dasko: Within the firm, you mean.

Ms. Quaid: Within the firm, and I don't care if it's a business of 1, 10 or 100 people — those same questions hold true. Then we should talk about training your staff. Putting your passwords on a sticky note at the bottom of your keyboard is not security.

Then we can get into the cost of implementing technologies, but with small and medium businesses, we need to start with the basics, the fundamentals, before we start talking about the cost.

Senator Dasko: Do we know about the motivations of perpetrators? We heard from other witnesses that, in some cases, it seems as if it could be random attacks. I don't know if there is any basis for that.

devez nous dire ce qui s'est passé, et nous pouvons vous demander de rectifier vos systèmes ou de mettre en place des solutions visant à compliquer la tâche des pirates.

Je ne considère pas ce projet de loi comme une initiative en faveur de l'innovation. Je le vois plutôt comme une mesure de sûreté qui, dans les faits, rendra l'innovation plus efficace, plus facile et mieux protégée, mais je le considère avant tout comme un projet de loi sur la sûreté.

La sénatrice Dasko : Je remercie les témoins. Madame Quaid, certaines de vos remarques concernant les petites et moyennes entreprises ont retenu mon attention. J'ai moi-même travaillé dans une entreprise de taille moyenne du secteur privé. Selon vous, quel est le coût moyen des mesures de prévention pour une entreprise? Je ne sais pas si un tel chiffre existe. Vous levez les yeux au ciel, alors j'ai peut-être posé une mauvaise question.

S'agit-il de coûts importants pour les entreprises qui souhaitent se doter des mesures de sécurité dont elles ont besoin? Avez-vous une idée de l'ordre de grandeur de ces coûts? Il est difficile pour les entreprises d'investir dans ce genre de choses.

Mme Quaid : C'est extrêmement difficile. Le coût dépend du niveau de sécurité que vous souhaitez atteindre. Ce qui m'intéresse, c'est d'accompagner une petite entreprise et de m'assurer qu'elle soit en mesure d'identifier ses systèmes essentiels. Nous ne parlons même pas de coûts ni de technologie. Il s'agit simplement de savoir si elle est capable de me dire de quels systèmes elle a besoin pour assurer son fonctionnement demain. Si c'est le cas, peut-elle me dire qui y a accès? Encore une fois, nous ne parlons pas de coûts. Nous parlons de politiques, de directives et de pratiques.

La sénatrice Dasko : Au sein de l'entreprise, vous voulez dire.

Mme Quaid : Au sein de l'entreprise, peu importe qu'elle compte 1, 10 ou 100 employés, ces mêmes questions restent d'actualité. Nous devons alors parler de la formation du personnel. Noter ses mots de passe sur un Post-it collé sous son clavier n'a rien de sécuritaire.

Nous pourrons ensuite aborder la question du coût de mise en œuvre des technologies, mais dans le cas des petites et moyennes entreprises, il faut commencer par les bases, les principes fondamentaux, avant d'évoquer le coût.

La sénatrice Dasko : Connaissons-nous les motivations des auteurs de ces actes? D'autres témoins nous ont rapporté que, dans certains cas, il semblerait qu'il s'agisse d'attaques aléatoires. Je ne sais pas si cette hypothèse repose sur des éléments concrets.

You mentioned, Mr. Shull, stealing secrets. Is that a big component of the perpetrators' motivations? Are they trying to steal? Are they trying to extract money from the victims? Do we have a picture of —

Mr. Shull: All of the above. We have to break it down. There is information technology, or IT; and operational technology, or OT. I'll answer your last question and then segue to your primary one.

Security for IT is not that difficult or expensive. I'm just some guy. I don't even work in a company. I use the most sophisticated commercially available malware detection software. I use a biographically and cryptographically locked password manager, and all my passwords are gobbledygook comprised of 17 or 18 characters. I use multifactor hardware authentication for my most sensitive matters, and I use an encrypted multi-hop VPN. All this stuff I listed costs a few hundred dollars a year. That's your IT infrastructure.

Regarding OT, when you're hooking real things up to the internet, they call them supervisory control and data acquisition — or SCADA — systems or industrial control systems, and that's a different order of magnitude.

In answer to your question, if people are going after IT, that is typically for information, fraud, ransomware and all that terrible stuff. The thing that I worry about — that keeps me up at night — and that goes to the core of this bill is hostile state actors going after and pre-positioning on critical infrastructure. That is putting malicious exploits on our electrical grid to use them in the event of a conflict. We don't need to think too long about geostrategy in terms of who we are talking about here.

Senator Dasko: Of course.

Mr. Shull: At the most fundamental level, this bill creates some fairness. If someone swipes in with a military badge or government badge on the other side and goes after civilian infrastructure, they are going to get in.

This is designed to let our government know about that and to balance it out so that we have a bit of a fair fight.

Senator Dasko: We heard about the vulnerability of water — for example, poisoning the water — and sectors like that.

Vous avez évoqué, monsieur Shull, le vol de secrets. Est-ce là un élément majeur des motivations des pirates? Cherchent-ils à voler? Cherchent-ils à soutirer de l'argent aux victimes? Avons-nous une idée de...

M. Shull : Tout ce qui précède. Il faut distinguer les deux. Il y a les technologies de l'information, ou TI, et les technologies opérationnelles, ou TO. Je vais répondre à votre dernière question, puis enchaîner avec la première.

La sécurité de la TI n'est ni si compliquée ni si coûteuse. Je suis un simple profane. Je ne travaille même pas dans une entreprise. J'utilise le logiciel de détection de logiciels malveillants le plus perfectionné disponible sur le marché. J'utilise un gestionnaire de mots de passe verrouillé par des données biométriques et un système cryptographique, et tous mes mots de passe sont des suites de caractères aléatoires composées de 17 ou 18 caractères. J'utilise une authentification matérielle à plusieurs facteurs pour mes données les plus sensibles, et j'utilise un RPV crypté à plusieurs sauts. Tout ce que je viens d'énumérer coûte quelques centaines de dollars par année. Voilà ce qu'est votre infrastructure TI.

En ce qui concerne les TO, lorsqu'on connecte des équipements physiques à Internet, on parle de systèmes de contrôle de supervision et d'acquisition de données — ou SCADA — ou de systèmes de contrôle industriel, et cela représente un tout autre ordre de grandeur.

Pour répondre à votre question, lorsque des gens s'attaquent aux systèmes TI, c'est généralement pour obtenir des informations, commettre des fraudes, lancer des attaques par rançongiciel et toutes ces choses terribles. Ce qui m'inquiète — ce qui m'empêche de dormir la nuit — et qui est au cœur même de ce projet de loi, ce sont les acteurs étatiques hostiles qui s'attaquent aux infrastructures critiques et effectuent leur déploiement à l'avance. Cela consiste à introduire des failles malveillantes dans notre réseau électrique afin de les exploiter en cas de conflit. Nous n'avons pas besoin de réfléchir longuement à la géostratégie pour savoir de qui nous parlons ici.

La sénatrice Dasko : Bien sûr.

M. Shull : Au fond, ce projet de loi rétablit une certaine équité. Si quelqu'un utilise une carte d'accès militaire ou gouvernementale pour s'en prendre à des infrastructures civiles, il parviendra à entrer.

L'objectif est d'en informer notre gouvernement et de rétablir l'équilibre afin que la partie soit un peu plus équitable.

La sénatrice Dasko : Nous avons entendu parler de la vulnérabilité de l'eau — par exemple, l'empoisonnement de l'eau — et de secteurs de ce genre.

Ms. Quaid: That would mostly be nation-state actors. People going after our systems are broken down into nation-state actors and criminal elements. Many of the latter are protected by nation-states and include those straight-up using ransomware to look for cash using what we would call a spray-and-pray approach. They send thousands of phishing emails, and only one has to hit.

Then there are the others, insiders and activists and hacktivists, but those are the two main elements we look at.

Mr. Ghorbani: To add on the last question, you asked about intent. There is an element in cybersecurity called cyber attribution. This is where we identify who attacked us, from where, and with what techniques and tactics. What was the intent of those attacks? This is where the Government of Canada is doing part of their work.

Recently, the government funded us, and we created the Cyber Attribution Data Centre here in Fredericton, where we do these kinds of studies.

Whether it's coming from industry or government, we can study the behaviour and the profile of the attack and attribute them to where they are coming from, what kinds of attack groups they belong to, what kinds of techniques and tactics they use, et cetera.

So, those elements actually help us to identify who is attacking us and what their intentions are.

The Deputy Chair: Thank you, Dr. Ghorbani.

[*Translation*]

Senator Carignan: Mr. Shull, I'm interested in the issue of constitutionality. I like the way you framed it: The goal is to provide a framework and regulate operations. In fact, under that regulatory framework, legitimate expectations are lower, since we're dealing with a regulated sector.

Let me draw a parallel with food. There are government inspectors in slaughterhouses and throughout the entire supply chain to ensure safety, proper labelling and so on. The goal is no longer to catch criminals, but to ensure that food is safe and protected, and that no system exists that could compromise food safety.

The same applies to information, data and computing. You are drawing a parallel by arguing that this is a regulated sector in which the government must have administrative powers to

Mme Quaid : Il s'agit principalement d'acteurs étatiques. Les personnes qui s'attaquent à nos systèmes se répartissent en deux catégories : les acteurs étatiques et les criminels. Bon nombre de ces derniers bénéficient de la protection d'États et comptent notamment ceux qui utilisent purement et simplement des rançongiciels pour soutirer de l'argent, en recourant à ce que l'on pourrait appeler une approche « à l'aveuglette ». Ils envoient des milliers de courriels hameçons, et il suffit qu'un seul atteigne sa cible.

Il y a aussi les autres : les initiés, les militants et les hacktivistes, mais ce sont là les deux principaux groupes sur lesquels nous nous concentrons.

M. Ghorbani : Pour revenir sur la dernière question, vous avez demandé quelle était l'intention des pirates. Il existe en cybersécurité un concept appelé « cyberattribution ». Il s'agit de déterminer qui était l'attaquant, d'où provenaient ces attaques, et quelles techniques et tactiques ont été utilisées. Quelle était l'intention derrière ces attaques? C'est précisément dans ce domaine que le gouvernement du Canada concentre une partie de ses efforts.

Récemment, le gouvernement nous a accordé un financement, et nous avons créé le Centre de données sur la cyberattribution ici à Fredericton, où nous menons ce type d'études.

Qu'elles proviennent du secteur privé ou des États, nous pouvons analyser le comportement et le profil des attaques et déterminer d'où elles proviennent, à quels types de groupes d'attaquants elles appartiennent, quelles techniques et tactiques elles utilisent, etc.

Ces éléments nous aident donc à identifier l'attaquant et quelles sont ses intentions.

Le vice-président : Merci, monsieur Ghorbani.

[*Français*]

Le sénateur Carignan : Monsieur Shull, la question de la constitutionnalité m'intéresse. J'aime la façon dont vous l'avez présentée : l'objectif est d'encadrer et de réglementer une opération. En fait, dans le cadre de cette réglementation, les attentes légitimes sont moins élevées, car nous sommes dans une entreprise réglementée.

Je vais faire un parallèle avec la nourriture. Il y a des inspecteurs du gouvernement dans les abattoirs et dans toute la chaîne d'approvisionnement pour s'assurer de la sécurité, de l'étiquetage, etc. L'objectif n'est plus de trouver un criminel, mais de s'assurer que la nourriture est sécuritaire et protégée, et qu'il n'y a pas de système qui pourrait altérer la sécurité de la nourriture.

C'est la même chose pour l'information, les données et l'informatique. Vous faites un parallèle en affirmant qu'il s'agit d'une entreprise réglementée où il doit y avoir des pouvoirs

intervene in order to ensure that regulation is effective and functional for safety purposes. The objective isn't to identify criminal conduct. In such cases, there would be investigations requiring a search warrant. Did I understand the nuance you're trying to make?

Mr. Shull: Thank you for your question, senator.

[*English*]

That is exactly right.

There is a line of cases that make that clear — regulatory compulsion versus criminal investigation, and they are constitutionally distinct. I think we are in the regulatory compulsion bucket here.

I will also add to that the point I made about cyber-operational tempo. This is very brisk stuff. Warrants take time, and that process would inject into the system a delay that could be problematic.

I already talked about what I said are the layered oversight functions that already exist here. This is not a free-for-all where they can go out and start doing whatever they feel like. There is a pretty good oversight mechanism.

I have also talked about judicial competence in this area. We are talking about the executive holding information that judges don't, and technical and operational contexts and expertise that are difficult to understand. You have to really educate the judges on this.

The orders being made are not penal; they are directed at corporate compliance.

I've also said there is this regulatory review structure. Let's try it. There is a five-year review. If it doesn't work, let's get it right next time. I don't want to let the perfect get in the way of what I think is the "good enough."

Senator McNair: Mr. Shull, I like the way you describe cyber-event tempo, because I think that is the reality of the situation we are in. The other thing you talked about was what was keeping you up at night. A few weeks ago, we had one of the officials, Andre Arbour, indicate that what is keeping him up at night is the lack of authority to take action in this space. He went on to talk about hostile state actors, as you have tonight.

administratifs d'intrusion de l'État pour s'assurer que la réglementation de l'État est effective et fonctionnelle dans un objectif de sécurité. On n'est pas dans un cadre de recherche de criminels — dans ces cas-là, il s'agirait plutôt d'enquêtes pour lesquelles on aurait besoin de mandats de perquisition. Est-ce que j'ai bien saisi la distinction que vous faites?

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

[*Traduction*]

C'est tout à fait exact.

Il existe une jurisprudence bien établie qui établit clairement la distinction entre la contrainte réglementaire et l'enquête criminelle, deux notions distinctes sur le plan constitutionnel. Je pense que nous nous trouvons ici dans le cadre de la contrainte réglementaire.

J'ajouterai également à cela ce que j'ai dit au sujet du rythme des opérations cybernétiques. C'est un domaine où tout va très vite. L'obtention de mandats prend du temps, et ce processus introduirait dans le système un retard qui pourrait poser problème.

J'ai déjà évoqué ce que j'ai qualifié de fonctions de contrôle à plusieurs niveaux qui existent déjà ici. Il ne s'agit pas d'une situation où chacun fait ce qu'il veut. Il existe un mécanisme de contrôle parfaitement efficace.

J'ai également évoqué la question de la compétence judiciaire dans ce domaine. Il s'agit ici d'informations dont dispose le pouvoir exécutif, mais pas les juges, ainsi que de contextes techniques et opérationnels et d'une expertise difficiles à appréhender. Il est indispensable de bien former les juges à ce sujet.

Les décrets édictés ne sont pas de nature pénale; ils visent à garantir la conformité des entreprises.

J'ai également mentionné l'existence du dispositif de révision réglementaire. Voyons ce que cela donnera. Un examen quinquennal est prévu. Si cela ne fonctionne pas, nous ferons mieux la prochaine fois. Je ne veux pas que la perfection m'empêche d'atteindre ce que je considère comme « suffisamment satisfaisant ».

Le sénateur McNair : Monsieur Shull, j'aime la façon dont vous décrivez le rythme des cyber-événements, car je pense que cela reflète bien la réalité de la situation dans laquelle nous nous trouvons. Vous avez également évoqué ce qui vous empêche de dormir. Il y a quelques semaines, l'un des responsables, André Arbour, a indiqué que ce qui l'empêchait de dormir, c'était le manque de pouvoir nécessaire pour agir dans ce domaine. Il a ensuite parlé des acteurs étatiques hostiles, tout comme vous l'avez fait ce soir.

A lot of the devil is in the details and will be worked out in the regulatory process. You have confirmed that again tonight. I would appreciate a comment. I think you're telling us that the judicial review process is just post-order.

Mr. Shull: An example bears it out.

Suppose we are dealing with an interprovincial pipeline in the winter. Suppose, further, there is a hostile state. We'll make up a name and call that state Brussia. Let us say Brussia injects malicious code into the infrastructure and turns the gas off. Suppose, further, that the government knows how to fix it. They need to inject certain code into the infrastructure in order to address it. As it stands right now, there is no legal requirement for that infrastructure provider to take that code. Under this bill, there would be.

That is what we're talking about here: cyber infrastructure and hostile states doing sophisticated things. We're just trying to level the playing field.

Senator McNair: Thank you.

The Deputy Chair: This brings us to the end of our time with this panel. Thank you, Ms. Quaid, Mr. Ghorbani and Mr. Shull, for taking the time to meet with us today and for your service to our country. We greatly appreciate your contributions to our work on this bill.

For our final panel this evening, we are pleased to welcome Mr. Matthew Hatfield, Executive Director, OpenMedia; Ms. Sharon Polsky, President, Privacy and Access Council of Canada; and, by video conference, Mr. Robbie Grant, Associate Lawyer, Privacy and Data Protection, McMillan LLP.

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

Matthew Hatfield, Executive Director, OpenMedia: Good evening.

I'm Matt Hatfield, Executive Director of OpenMedia, a grassroots community of 230,000 people in Canada who work together for an open, accessible and surveillance-free internet. I'm grateful to be with you tonight on the unceded territory of the Algonquin Anishinaabe Nation.

C'est souvent dans les détails que réside le problème, et ceux-ci seront réglés au cours du processus réglementaire. Vous l'avez confirmé une nouvelle fois ce soir. J'aimerais avoir votre avis à ce sujet. Je crois que vous nous dites que le processus de contrôle judiciaire n'intervient qu'après la publication de l'arrêté.

M. Shull : Prenons un exemple concret.

Imaginons qu'il s'agisse d'un pipeline interprovincial en hiver. Imaginons, en outre, qu'il existe un État hostile. Nous allons inventer un nom et appeler cet État « Brussia ». Imaginons que Brussia injecte un code malveillant dans l'infrastructure et coupe l'approvisionnement en gaz. Supposons, en outre, que le gouvernement sache comment y remédier. Il doit injecter un certain code dans l'infrastructure afin de résoudre le problème. À l'heure actuelle, rien n'oblige légalement le fournisseur de cette infrastructure à accepter ce code. En vertu de ce projet de loi, ce serait le cas.

C'est exactement de cela qu'il est question ici : les infrastructures informatiques et les États hostiles qui mènent des actions sophistiquées. Nous essayons simplement de rétablir l'équilibre des forces.

Le sénateur McNair : Merci.

Le vice-président : Cela marque la fin de notre discussion avec ce groupe de témoins. Merci, madame Quaid, monsieur Ghorbani et monsieur Shull, d'avoir pris le temps de vous joindre à nous aujourd'hui et pour votre engagement au service de notre pays. Nous apprécions grandement votre contribution à nos travaux sur ce projet de loi.

Pour notre dernier groupe de témoins de ce soir, nous avons le plaisir d'accueillir M. Matthew Hatfield, directeur exécutif d'OpenMedia; Mme Sharon Polsky, présidente du Conseil du Canada de l'accès et la vie privée; ainsi que, par vidéoconférence, Me Robbie Grant, avocat sociétaire, Protection de la vie privée et des données chez McMillan LLP.

Merci à tous d'être parmi nous aujourd'hui. Nous allons commencer par vous inviter à prononcer votre déclaration préliminaire, qui sera suivie des questions de nos membres. Je vous rappelle que vous disposez chacun de cinq minutes pour votre exposé.

Matthew Hatfield, directeur exécutif, OpenMedia : Bonsoir.

Je m'appelle Matt Hatfield, je suis directeur exécutif d'OpenMedia, une communauté locale de 230 000 personnes au Canada qui œuvrent ensemble pour un Internet ouvert, accessible et exempt de surveillance. Je suis heureux d'être parmi vous ce soir sur le territoire non cédé de la nation algonquine anishinabe.

I want to begin with something I don't often get to say at a committee very often, which is that the other house's amendment work got a lot right on this bill. When civil society and the Privacy Commissioner came to the House with very severe concerns about the previous version of Bill C-8, many were heard, and real improvements were made to the text in front of you.

Every order must now be reasonable in relation to the gravity of the threat. The minister must weigh the impact on Canadians' privacy before acting. The bill states the government cannot order a provider to decode an encrypted private communication and cannot use these powers to intercept private communications, and an individual cannot be cut off from service except against a genuine technical threat.

These are real protections, and the members who fought for them deserve credit. However, the job of fixing Bill C-8 is not entirely done, and I am hoping you will finish it.

Bill C-8 carefully limits why information may be collected and why it may be shared between departments. In each case, the purpose must relate to making or enforcing one of these cybersecurity orders. That is good drafting, but it stops one step short. Once information has been lawfully passed to an agency like the Communications Security Establishment, nothing in this bill limits what that agency may then use it for. The gate into the building is guarded; once inside, the data can be put to other purposes.

During the study of the predecessor bill, a CSE official testified to the agency's interest in using information gathered under these powers beyond its cybersecurity mandate, so this is not a theoretical gap. It is one the government has told Parliament it intends to walk through.

The fix is small and surgical: Say in the statute that information obtained under this act is used only for cybersecurity and information assurance, not repurposed for foreign intelligence or unrelated operations. This is the recommendation the Citizen Lab put to the House. It does not touch the government's cybersecurity powers at all. It simply holds them to their stated purpose.

Je voudrais commencer par une observation que j'ai rarement l'occasion de formuler dans un comité, à savoir que les amendements proposés par l'autre chambre ont apporté de nombreuses améliorations à ce projet de loi. Lorsque la société civile et le commissaire à la vie privée ont fait part à la Chambre de leurs vives préoccupations concernant la version précédente du projet de loi C-8, bon nombre d'entre elles ont été prises en compte, et de réelles améliorations ont été apportées au texte qui vous est présenté.

Toute mesure doit désormais être proportionnée à la gravité de la menace. Le ministre doit évaluer l'impact sur la vie privée des Canadiens avant d'agir. Le projet de loi stipule que le gouvernement ne peut ordonner à un fournisseur de services de décrypter une communication privée cryptée ni utiliser ces pouvoirs pour intercepter des communications privées, et qu'une personne ne peut être privée de service qu'en cas de menace technique réelle.

Il s'agit là de véritables mesures de protection, et les députés qui se sont battus pour les obtenir méritent d'être salués. Cependant, le travail visant à améliorer le projet de loi C-8 n'est pas encore tout à fait terminé, et j'espère que vous le mènerez à bien.

Le projet de loi C-8 définit avec précision les motifs pour lesquels des renseignements peuvent être recueillis et échangés entre les ministères. Dans chaque cas, l'objectif doit être lié à l'adoption ou à l'application de l'un de ces décrets en matière de cybersécurité. Il s'agit là d'une bonne formulation, mais elle ne va pas assez loin. Une fois que les renseignements ont été transmis légalement à un organisme comme le Centre de la sécurité des télécommunications, rien dans ce projet de loi ne limite l'usage que cet organisme peut en faire par la suite. L'entrée du bâtiment est surveillée, mais une fois à l'intérieur, les données peuvent être utilisées à d'autres fins.

Lors de l'examen du projet de loi précédent, un responsable du CST a déclaré que l'agence souhaitait utiliser les informations recueillies en vertu de ces pouvoirs au-delà de son mandat en matière de cybersécurité; il ne s'agit donc pas d'une lacune théorique. C'est une lacune que le gouvernement a déclaré au Parlement avoir l'intention d'exploiter.

La solution est simple et ciblée : il s'agit de préciser dans la loi que les informations obtenues en vertu de celle-ci sont utilisées uniquement à des fins de cybersécurité et de protection des renseignements, et ne sont pas détournées à des fins de renseignement étranger ou d'opérations sans rapport avec ces objectifs. Telle est la recommandation que Citizen Lab a soumise à la Chambre des communes. Elle ne remet nullement en cause les pouvoirs du gouvernement en matière de cybersécurité. Elle vise simplement à ce qu'ils soient utilisés conformément à leur objectif déclaré.

Second, the standard throughout this bill is that an action be reasonable in relation to the gravity of the threat. But the Privacy Commissioner asked this Parliament for something more exacting and more familiar in privacy law: that any collection, use or disclosure of personal information be both necessary to achieve the purpose and proportionate to the benefit. That is the test our privacy framework uses everywhere else, and yet this bill did not adopt it. You can.

Third, an order under this bill can carry a provision forbidding anyone from revealing that it exists, and that secrecy has no end. The bill tells the minister to weigh transparency before imposing silence, which is welcome, but once imposed, there is no sunset and no requirement to return to a court to justify keeping it hidden.

Permanent, unreviewed secrecy is not something Parliament should not grant without limit. I urge you to ensure that the public is eventually informed of the existence of secret orders to service providers, if not their full text, and that representatives in NSIRA and NSICOP can ultimately review and comment on the text of these orders.

Underlying all this is a check that the other house wanted. Its committee adopted independent authorization of non-emergency orders by a judge, a safeguard at the start of the process. That was not voted down. It was removed before third reading on a procedural ruling about the bill's scope. It belongs back in Bill C-8.

I know this committee weighs carefully when to ask democratically elected officials to think again. This is the right time to do so because you would be acting on proposals that the other house considered and even passed or that were directly proposed by Canada's Privacy Commissioner — or both.

There are four narrow amendments, as I outlined, that would help with that purpose. More than 10,000 Canadians have written to ask that this bill become law only once it protects our rights as well as our networks. The other house brought it much of the way to doing that. What remains to do is putting in place basic limits that citizens of a democracy expect: that data taken for one purpose is used for that purpose; that orders are proportional, not just reasonable; that our rights are defended by appointed judges, not a private corporation's decision to fight an order; and that no secret order stays secret forever.

Deuxièmement, le principe qui sous-tend l'ensemble de ce projet de loi est qu'une mesure doit être raisonnable au regard de la gravité de la menace. Or, le commissaire à la vie privée a demandé à ce Parlement d'adopter un critère plus rigoureux et plus courant dans les lois relatives à la protection de la vie privée, à savoir que toute collecte, utilisation ou communication de renseignements personnels, soit à la fois nécessaire, à la réalisation de l'objectif visé, et proportionnée à l'avantage escompté. C'est le critère que notre cadre de protection de la vie privée applique partout ailleurs, et pourtant, ce projet de loi ne l'a pas retenu. Vous pouvez le faire.

Troisièmement, un décret pris en vertu de ce projet de loi peut comporter une disposition interdisant à quiconque de révéler son existence, et ce secret est illimité dans le temps. Le projet de loi impose au ministre de prendre en compte la transparence avant d'imposer le silence, ce qui est une bonne chose; mais une fois cette mesure imposée, elle n'est assortie d'aucune date d'expiration et il n'est pas nécessaire de saisir à nouveau un tribunal pour justifier le maintien de ce secret.

Le Parlement ne devrait pas accorder sans limites un secret permanent et non soumis à un contrôle. Je vous invite instamment à veiller à ce que le public soit finalement informé de l'existence des décrets secrets s'adressant aux fournisseurs de services, à défaut de leur texte intégral, et à ce que les représentants au sein de l'OSSNR et du CPSNR puissent, à terme, examiner et commenter le texte de ces décrets.

À l'origine de tout cela se trouve une disposition que l'autre chambre souhaitait voir figurer dans le texte. Son comité avait adopté une mesure prévoyant l'autorisation indépendante, par un juge, des arrêtés non urgents, une garantie mise en place dès le début du processus. Cette disposition n'a pas été rejetée par un vote. Elle a été supprimée avant la troisième lecture à la suite d'une décision de procédure concernant la portée du projet de loi. Elle doit être réintégrée dans le projet de loi C-8.

Je sais que ce comité réfléchit mûrement avant de demander à des élus de revoir leur position. C'est le moment idéal pour le faire, car vous vous prononceriez sur des propositions qui ont été examinées, voire adoptées, par l'autre chambre, ou qui ont été directement présentées par le commissaire à la protection de la vie privée du Canada — voire les deux.

Comme je l'ai indiqué, quatre amendements ciblés contribueraient à atteindre cet objectif. Plus de 10 000 Canadiens ont écrit pour demander que ce projet de loi ne soit adopté que s'il protège à la fois nos droits et nos réseaux. L'autre chambre a déjà fait un grand pas dans cette direction. Il reste à mettre en place les limites fondamentales auxquelles s'attendent les citoyens d'une démocratie, à savoir que les données recueillies, à une fin précise, soient utilisées à cette fin; que les décrets soient proportionnés, et pas seulement raisonnables; que nos droits soient défendus par des juges nommés, et non par la décision

Completing the job of adopting these safeguards into the law is a job that now only the Senate can do. I hope that you will.

Thank you, and I look forward to your questions.

The Deputy Chair: Thank you, Mr. Hatfield.

Sharon Polsky, President, Privacy and Access Council of Canada: Thank you and good evening. I appreciate the invitation to appear before you this evening.

My name is Sharon Polsky. I am President of the Privacy and Access Council of Canada, an independent, non-profit, non-partisan organization that is not funded by government or industry.

The need to strengthen Canada's cybersecurity, data protection and intellectual property governance framework and protect its infrastructure is not new, nor are the overreaching attempts by too many governments to protect Canadians from themselves or from things that cannot be controlled, with cures that can be worse than the problems they're supposed to fix. So, it is good to see that Bill C-8 now provides for improvement, but it still has a long way to go to earn Canadians' trust and to not be able to be weaponized.

Being able to order telcos to "do anything or refrain from doing anything" is impossibly broad and can now escape all scrutiny.

Even at this late stage, we still don't know who or what will be a designated operator or class of operators, how that will be determined or how narrow or broad it will be. They can be designated by order-in-council, and compliance orders can be issued by order — and presumably secret orders-in-council as well, which is a problem. Who they are should be designated in the law.

It is the Governor-in-Council that gets to gauge the impact of orders it is about to pronounce. And while it's good that directions must be reasonable, when they're secret, it's impossible for anybody to know. But there are even bigger problems. I'll focus on three.

Parts 1 and 2 assure Canadians that ". . . the Minister must not order the decoding of an encrypted *private communication* . . ." Undermining encryption is a feature of Bill C-22 that could be accomplished in secret. Further, with the Secretary of State for

d'une entreprise privée de contester un décret, et qu'aucun ordre secret ne reste secret pour toujours.

C'est désormais au Sénat seul qu'il revient de mener à bien le processus d'intégration de ces mesures de sécurité dans la loi. J'espère que vous le ferez.

Merci, et j'attends vos questions avec impatience.

Le vice-président : Merci, Monsieur Hatfield.

Sharon Polsky, présidente, Conseil du Canada de l'accès et la vie privée : Merci et bonsoir. Je vous remercie de m'avoir invitée à comparaître ce soir.

Je m'appelle Sharon Polsky. Je suis la présidente du Conseil du Canada de l'accès et la vie privée, un organisme indépendant, à but non lucratif et faisant abstraction de tout intérêt partisan.

La nécessité de renforcer le cadre canadien en matière de cybersécurité, de protection des données et de gouvernance de la propriété intellectuelle, ainsi que de protéger ses infrastructures, n'est pas nouvelle, pas plus que ne le sont les tentatives excessives de trop nombreux gouvernements visant à protéger les Canadiens contre eux-mêmes ou contre des éléments incontrôlables, en proposant des solutions qui peuvent s'avérer pires que les problèmes qu'elles sont censées résoudre. Il est donc réjouissant de constater que le projet de loi C-8 prévoit désormais des améliorations, mais il reste encore beaucoup à faire pour qu'il gagne la confiance des Canadiens et pour qu'il ne puisse pas être instrumentalisé.

Le fait de pouvoir ordonner aux fournisseurs de services de télécommunications de « faire ou de s'abstenir de faire toute chose nécessaire » est d'une portée tellement vaste qu'il échappe désormais à tout contrôle.

Même à ce stade avancé, nous ne savons toujours pas qui ou quoi sera désigné comme exploitant ou catégorie d'exploitants, comment cela sera déterminé, ni quelle sera l'étendue de cette désignation. Ces désignations peuvent être faites par décret, et des ordres d'exécution peuvent être donnés par décret — y compris, vraisemblablement, des décrets secrets, ce qui pose problème. L'identité de ces exploitants devrait être précisée dans la loi.

C'est au gouverneur en conseil qu'il revient d'évaluer l'impact des décrets qu'il s'apprête à promulguer. Et s'il est louable que ces directives doivent être raisonnables, lorsqu'elles sont tenues secrètes, il est impossible pour quiconque de s'en juger. Mais il existe des problèmes bien plus graves encore. Je m'attarderai sur trois d'entre eux.

Les parties 1 et 2 garantissent aux Canadiens que « […] le ministre ne peut ordonner le décodage d'une *communication privée* […] qui est chiffrée ». Le contournement du chiffrement est une disposition du projet de loi C-22 qui pourrait être mise en

Combatting Crime having described Bill C-22 as a “first step” — and with the CLOUD Act on top of it — it is fanciful to think Bill C-8 will operate in isolation.

In the meantime, designated operators must report cybersecurity incidents within 72 hours, but within 72 hours of what we don’t know because the bill doesn’t say. That needs clarity.

Bill C-8 also puts our privacy in jeopardy and threatens Canadian industry, contrary to what previous witnesses — several of them this evening — have said. Our personal information is collected and disclosed under strict limits of privacy legislation, but Bill C-8 could compel organizations to disclose it, along with customer lists and system vulnerabilities, to the Government of Canada, to be handed to foreign states and agencies and international organizations, undermining our privacy and security.

The bill does not explicitly restrict data sharing to cybersecurity purposes. It only broadly limits information disclosed to foreign interests from being used for purposes “relevant to” investigating contraventions of laws that wouldn’t have consequences considered penal under Canadian law.

But it does not mandate oversight by our Privacy Commissioner. It does not limit how long information can be retained; and it does not say confidential information disclosed to a law enforcement agency must only be to a Canadian law enforcement agency — and it needs to.

As well, Bill C-8 does say information shared with foreign states and agencies must be disposed of, but it does not say it must be securely destroyed or within specific timelines. Those words make a fundamental difference and are standard in industry.

After-the-fact penalties for non-compliance or for breaching privacy aren’t the answer. If, on the other hand, the law stated that information disclosed to foreign interests was required to remain in Canada, under the custody and control of a Canadian body, it would be possible to monitor, audit and control access and preserve our digital sovereignty. It would be enforceable.

œuvre en secret. De plus, le secrétaire d’État chargé de la lutte contre la criminalité ayant qualifié le projet de loi C-22 de « première étape » — et compte tenu du CLOUD Act qui vient s’y ajouter —, il est illusoire de penser que le projet de loi C8 fonctionnera en isolement.

En attendant, les exploitants désignés sont tenus de signaler les incidents de cybersécurité dans un délai de 72 heures, mais nous ne savons pas à compter de quoi, car le projet de loi ne le précise pas. Il faudrait clarifier ce point.

Le projet de loi C-8 met également en péril notre vie privée et menace l’industrie canadienne, contrairement à ce qu’ont affirmé les témoins précédents — dont plusieurs ce soir. Nos renseignements personnels sont recueillis et communiqués dans le strict respect des limites imposées par la législation en matière de protection de la vie privée, mais le projet de loi C-8 pourrait contraindre les organisations à les divulguer, ainsi que leurs listes de clients et les failles de leurs systèmes, au gouvernement du Canada, afin qu’ils soient transmis à des États et organismes étrangers ainsi qu’à des organisations internationales, ce qui porterait atteinte à notre vie privée et à notre sécurité.

Le projet de loi ne limite pas explicitement l’échange de données à des fins de cybersécurité. Il se contente d’interdire de manière générale que les informations communiquées à des entités étrangères soient utilisées à des fins liées à des enquêtes sur des infractions à des lois qui n’entraîneraient pas de conséquences pénales en vertu du droit canadien.

Mais il n’impose pas un contrôle de la part de notre commissaire à la vie privée. Il ne fixe pas de limite à la durée de conservation des informations ; et il ne précise pas, comme il le devrait, que les informations confidentielles qui sont communiquées à un organisme d’application de la loi doivent l’être exclusivement à un organisme d’application de la loi canadien.

De plus, le projet de loi C-8 stipule, certes, que les informations partagées avec des États et des organismes étrangers doivent être éliminées, mais il ne précise pas qu’elles doivent l’être de manière sécurisée et dans des délais précis. Ces précisions font une différence fondamentale et constituent la norme dans le secteur.

Les sanctions a posteriori en cas de non-conformité ou d’atteinte à la vie privée ne constituent pas la solution. Si, en revanche, la loi stipulait que les informations communiquées à des entités étrangères devaient rester au Canada, sous la garde et le contrôle d’un organisme canadien, il serait alors possible de surveiller, de vérifier et de contrôler l’accès à ces données, et de préserver notre souveraineté numérique. Une telle mesure serait applicable.

Finally, an amendment to the bill, clause 15.01, says interference with a telco includes actions of a technical nature but not the "effect of" lawful expression, persuasion or political debate. That is not as innocuous as it might sound.

For instance, if I praise someone or something, then an unruly mob decides to exhibit their displeasure with my comments by rioting and damaging a cell tower, they would be protected under Bill C-8 if their destructive actions were construed as the effect of my lawful expression.

That insidious provision condones public disorder and unlawful conduct, and it would enable the government to scrutinize, regulate and intervene around the systems, coordination, amplification and operational methods connected to any activity, claiming it is necessary to guard against some imagined future threat.

The wording lets government decide where lawful expression ends and where technical interference begins. They want to referee their own game.

This is all to say that Bill C-8 would benefit from clearer language, clearer mechanisms for independent oversight, accessible recourse for affected parties and stronger safeguards, to ensure cybersecurity measures are genuinely necessary, proportionate and consistent with Canadians' privacy rights, so the power to protect infrastructure can only be used to protect infrastructure.

The Deputy Chair: Thank you, Ms. Polsky.

Robbie Grant, Associate Lawyer, Privacy and Data Protection, McMillan LLP, as an individual: Good evening, Mr. Chair and honourable senators.

My name is Robbie Grant. I am a lawyer at McMillan LLP, where I practise privacy and data protection law. I advise clients on privacy programs, data breaches and cybersecurity matters, including the deployment of AI technologies. I primarily work with private sector organizations, advising on private-sector privacy laws such as PIPEDA.

Enfin, un amendement au projet de loi, l'article 15.01, précise que l'ingérence dans les activités d'un fournisseur de services de télécommunications comprend les actes de nature technique, mais non les « effets » de l'expression licite d'opinions, de la persuasion ou du débat politique. Cela n'est pas aussi anodin que cela pourrait paraître.

Par exemple, si je fais l'éloge de quelqu'un ou de quelque chose, et qu'une foule en colère décide d'exprimer son mécontentement face à mes propos en se livrant à des émeutes et en endommageant une antenne-relais, ces personnes seraient protégées par le projet de loi C-8 si leurs actes de destruction étaient interprétés comme la conséquence de l'expression licite de mon opinion.

Cette disposition insidieuse tolère les troubles à l'ordre public et les comportements illégaux, et elle permettrait au gouvernement de contrôler, de réglementer et d'intervenir sur les systèmes, la coordination, la diffusion et les méthodes opérationnelles liés à toute activité, sous prétexte que l'adoption de cette mesure est nécessaire pour se prémunir contre une menace future imaginaire.

Cette formulation permet au gouvernement de décider où s'arrête la liberté d'expression légitime et où commence l'ingérence technique. Il veut arbitrer son propre jeu.

En résumé, le projet de loi C-8 gagnerait à être formulé de manière plus claire, à prévoir des mécanismes plus précis de contrôle indépendant, à offrir des voies de recours accessibles aux parties concernées et à mettre en place des mesures de sécurité plus solides, afin de s'assurer que les mesures de cybersécurité sont véritablement nécessaires, proportionnées et respectueuses des droits à la vie privée des Canadiens, de sorte que le pouvoir de protéger les infrastructures ne puisse être utilisé qu'à cette fin.

Le vice-président : Merci, Madame Polsky.

Me Robbie Grant, avocat sociétaire, Protection de la vie privée et des données, McMillan LLP, à titre personnel : Bonsoir, monsieur le président et honorables sénateurs.

Je m'appelle Robbie Grant. Je suis avocat chez McMillan LLP, où j'exerce dans le domaine des lois relatives à la protection des renseignements personnels et à la protection des données. Je conseille mes clients sur les programmes de protection des renseignements personnels, les atteintes à la protection des données et les questions de cybersécurité, y compris le déploiement des technologies d'IA. Je travaille principalement avec des organisations du secteur privé, que je conseille sur la législation applicable à ce secteur en matière de protection des renseignements personnels, telle que la LPRPDE.

I am not representing a client today, nor am I speaking on behalf of my firm as a whole. I appear in my personal capacity only.

I have followed the evolution of this legislation closely. I wrote about Bill C-26 when it was first introduced. I continued to write about it as it progressed through Parliament. More recently, I had the privilege of moderating a panel on Bill C-8 at the International Institute of Communications annual conference in September.

I am grateful for the opportunity to share a few observations with this committee, beginning with the threat environment that makes this legislation necessary.

The numbers speak for themselves. According to IBM's *Cost of a Data Breach Report 2025*, while the global average cost of a data breach has declined, the same cannot be said for Canada: The average cost of a data breach here rose to US$4.82 million.

That figure does not account for downstream harms, including increased costs to consumers or impacts on small businesses that rely on critical infrastructure or providers.

The Canadian Centre for Cyber Security's *National Cyber Threat Assessment 2025-2026* warns that Canada has entered ". . . a new era of cyber vulnerability . . . ." in which state-sponsored actors are becoming bolder and more aggressive; cybercriminals are leveraging new business models, such as Cybercrime-as-a-Service, to scale their operations; and artificial intelligence is amplifying the quality, scale and precision of attacks.

Against that backdrop, I want to emphasize that the organizations most directly affected by this bill — Canada's banks, telecom providers, energy companies and transportation operators — are not starting from zero. Many have invested heavily in cybersecurity for years, not merely as a matter of legal compliance but because protecting their systems is fundamental to their business and to maintaining the trust of their customers.

This is worth acknowledging because the framing of cybersecurity legislation sometimes implies a gap in awareness or commitment that, in my experience advising clients in these sectors, does not always reflect reality.

That commitment is reinforced by the regulatory environment in which these organizations already operate. Many are subject to detailed cybersecurity guidance from their sectoral regulators,

Je ne représente aucun client aujourd'hui, et je ne m'exprime pas non plus au nom de mon cabinet dans son ensemble. Je m'exprime uniquement à titre personnel.

J'ai suivi de près l'évolution de ce projet de loi. J'ai écrit un article sur le projet de loi C-26 dès son dépôt. J'ai continué à écrire à ce sujet tout au long de son parcours au Parlement. Plus récemment, j'ai eu le privilège d'animer une table ronde sur le projet de loi C-8 lors de la conférence annuelle de l'Institut international des communications, en septembre.

Je vous suis reconnaissant de me donner l'occasion de partager quelques observations avec ce comité, en commençant par l'environnement de menaces qui rend ce projet de loi nécessaire.

Les chiffres parlent d'eux-mêmes. Selon le *Rapport 2025 sur le coût d'une violation de données* d'IBM , si le coût moyen mondial d'une atteinte à la protection des données a diminué, il n'en va pas de même au Canada : le coût moyen d'une atteinte à la protection des données y a atteint 4,82 millions de dollars américains.

Ce chiffre ne tient pas compte des répercussions en aval, notamment l'augmentation des coûts pour les consommateurs ou les conséquences pour les petites entreprises qui dépendent d'infrastructures ou de fournisseurs essentiels.

L'Évaluation nationale des menaces cybernétiques 2025-2026, du Centre canadien pour la cybersécurité, met en garde contre le fait que le Canada se retrouve dans « […] une nouvelle ère de cybervulnérabilité […] », au cours de laquelle les acteurs parrainés par des États se montrent de plus en plus audacieux et agressifs, les cybercriminels exploitent de nouveaux modèles d'entreprise, tels que la « cybercriminalité comme service », pour étendre leurs activités, et l'intelligence artificielle renforce la qualité, l'ampleur et la précision des attaques.

Dans ce contexte, je tiens à souligner que les organisations les plus directement concernées par ce projet de loi — les banques, les fournisseurs de services de télécommunications, les entreprises du secteur de l'énergie et les exploitants de services de transport canadiens — ne partent pas de zéro. Bon nombre d'entre elles investissent massivement dans la cybersécurité depuis des années, non seulement pour se conformer à la législation, mais aussi parce que la protection de leurs systèmes est essentielle à leur activité et au maintien de la confiance de leurs clients.

Il convient de le souligner, car la manière dont la législation en matière de cybersécurité est présentée laisse parfois entendre un manque de vigilance ou d'engagement qui, d'après mon expérience en tant que conseiller auprès de clients de ces secteurs, ne correspond pas toujours à la réalité.

Cet engagement est renforcé par le cadre réglementaire dans lequel ces organisations évoluent déjà. Bon nombre d'entre elles sont soumises à des directives détaillées en matière de

the Office of the Superintendent of Financial Institutions's Guideline B-13: Technology and Cyber Risk Management being one example.

None of this is to suggest that Bill C-8 is unnecessary, but the bill's implementation, and particularly its regulations, should be designed with this existing landscape in mind, avoiding unnecessary duplication.

That's why I applaud the recently revised subclause 135(2) of the CCSPA, which would provide that the Governor-in-Council must, to the extent possible, ensure consistency with existing regulatory and standards regimes in making its regulations.

I am also supportive of two directions the bill takes, which I believe reflect important improvements from the original version.

First, when Bill C-26 was first introduced, it attracted criticism for the breadth of discretion it would give to government. As the bill progressed, various conditions were added to ensure these new powers are exercised in a more proportionate and accountable manner.

Second, I am pleased to see more protections for the privacy of Canadians incorporated into the bill's framework. Cybersecurity and privacy are complementary, not competing objectives. The admirable goal of improving national security should not be used as a pretense for widespread surveillance.

To conclude, the threat environment facing Canada's critical infrastructure is real and serious, and this legislation represents an important step in addressing it. My submission today is simply that its implementation should treat designated operators as the sophisticated, security-conscious actors many of them already are and should minimize duplication with existing regulatory frameworks.

Thank you, honourable senators. I look forward to our discussion.

The Deputy Chair: Thank you, Mr. Grant.

We will now proceed to questions, colleagues. This final panel will be with us until 8 p.m. As always, four minutes will be allotted for each question, including the answer.

Senator Cardozo: Thank you, witnesses, for being here. I appreciate your time and the considered submissions that you make today.

cybersécurité émanant de leurs autorités de régulation sectorielles, comme en témoigne notamment la directive B-13 du Bureau du surintendant des institutions financières intitulée « Gestion du risque lié aux technologies et du cyberrisque ».

Cela ne signifie pas pour autant que le projet de loi C-8 soit inutile, mais sa mise en œuvre, et en particulier ses règlements d'application devraient être conçus en tenant compte du contexte actuel, afin d'éviter tout double emploi inutile.

C'est pourquoi je me réjouis de la récente révision du paragraphe 135(2) de la Loi sur la protection des cybersystèmes essentiels, la LPCE, selon laquelle à l'heure de prendre des décrets, le gouverneur en conseil doit veiller dans la mesure du possible à ce qu'ils soient compatibles avec la réglementation et les normes en vigueur.

J'appuie également la double orientation du projet de loi qui, à mon avis, représente des améliorations importantes par rapport à la version originale.

Premièrement, lorsque le projet de loi C-26 a été présenté pour la première fois, il a suscité des critiques quant à l'étendue du pouvoir discrétionnaire qu'il accorderait au gouvernement. À mesure que le projet de loi progressait, diverses conditions ont été ajoutées pour que ces nouveaux pouvoirs soient exercés d'une manière plus proportionnée et responsable.

Deuxièmement, je constate avec joie que le cadre du projet de loi prévoit davantage de mesures de protection des renseignements personnels des Canadiens. La cybersécurité et la protection de la vie privée sont des objectifs complémentaires et non concurrents. L'objectif admirable d'améliorer la sécurité nationale ne devrait pas servir de prétexte à une surveillance généralisée.

En conclusion, la menace qui pèse sur les infrastructures essentielles du Canada est aussi réelle que grave, et ce projet de loi représente une étape importante pour y faire face. Je me contenterai de dire quant à moi qu'il devrait traiter les exploitants désignés comme les acteurs avertis et soucieux de la sécurité que bon nombre d'entre eux sont déjà, tout en évitant autant que possible le double emploi avec les cadres réglementaires en vigueur.

Merci, honorables sénateurs. J'ai hâte de discuter avec vous.

Le vice-président : Merci, maître Grant.

Nous allons maintenant passer aux questions, chers collègues. Ce dernier groupe sera avec nous jusqu'à 20 heures. Comme toujours, quatre minutes seront allouées pour chaque question, réponse comprise.

Le sénateur Cardozo : Je remercie les témoins de leur présence. Je vous remercie de votre temps et des mémoires réfléchis que vous avez présentés aujourd'hui.

I'd like to start with Mr. Hatfield and Ms. Polsky and pursue the issue of data sharing you have raised.

Could you point us to the sections in the bill where — I think, Mr. Hatfield, you mentioned there isn't a limitation on how the data is shared within government but that it remains within government agencies. Is that —

Mr. Hatfield: The concern here is that once the CSE acquires the data, then the data leaves the purview of protection. It should only enter CSE's hands for cybersecurity purposes, but once it's in their hands, they can make use of it for other purposes and hand it on to foreign intelligence agencies. That's the concern: that this data could wind up finding quite different purposes.

Senator Cardozo: Within Canada, it could go to other agencies. Do you think it's okay if it's going to another agency for the purpose of looking at foreign interference — if it went to the RCMP, for example?

Mr. Hatfield: That's an interesting question. I think you could get that for a cybersecurity purpose rather than needing to define it as "foreign interference." Foreign interference generally involves a cybersecurity threat. If it were foreign interference through non-cybersecurity means, then, no, I would not want to see these powers used for that. If it were just regular investigations outside of the context of cybersecurity, I don't think it would be necessary to use these powers.

Senator Cardozo: Some people might say foreign interference is a threat to us. Shouldn't we be able to have that information available to people who are dealing with foreign interference?

Mr. Hatfield: There are many legitimate purposes of government that are not cybersecurity. What we're asking is for a cybersecurity bill, one that may involve extraordinary access in some cases, to keep it to cybersecurity.

Senator Cardozo: You talked about sharing with other governments. Ms. Polsky, I think you probably talked about that a little more. Could you expand on that?

Mr. Hatfield: Yes. The concern is that currently once data collected for cybersecurity purposes under this bill enters the hands of our security intelligence agencies, it's often passed on in an intelligence exchange with other foreign governments. Of course, once the data leaves Canada, we have no binding ability to control what is done with that data at all. I think many

J'aimerais commencer par m'adresser à M. Hatfield et à Mme Polsky et revenir sur la question de l'échange de données que vous avez soulevée.

Pourriez-vous nous indiquer les articles du projet de loi où — je crois, monsieur Hatfield, que vous avez mentionné qu'il n'y a pas de limite à la façon dont les données sont échangées au sein du gouvernement, mais elles demeurent sous le contrôle des organismes gouvernementaux. Est-ce que...

M. Hatfield : Le problème, c'est que les données ne sont plus protégées une fois qu'elles sont acquises par le Centre de la sécurité des télécommunications, le CST. Elles ne devraient passer au CST qu'à des fins de cybersécurité, mais une fois là, elles peuvent servir à d'autres fins et être transmises à des organismes de renseignement étrangers. C'est ce qui nous inquiète : ces données pourraient finir par trouver des fins tout à fait différentes.

Le sénateur Cardozo : Au Canada, elles pourraient aboutir à d'autres organismes. Pensez-vous qu'il soit acceptable que ces données soient confiées à un autre organisme dans le but de découvrir une ingérence étrangère — disons par exemple à la GRC?

M. Hatfield : C'est une question intéressante. Je pense qu'on pourrait évoquer des fins de cybersécurité plutôt que d'avoir à le définir comme une « ingérence étrangère ». Or, qui dit ingérence étrangère, dit généralement une menace à la cybersécurité. S'il s'agissait d'une ingérence étrangère par des moyens non liés à la cybersécurité, alors je ne voudrais pas que ces pouvoirs soient utilisés à cette fin. S'il ne s'agit que d'enquêtes régulières en dehors du contexte de la cybersécurité, je ne pense pas qu'il soit nécessaire d'utiliser ces pouvoirs.

Le sénateur Cardozo : Certains diront que l'ingérence étrangère constitue une menace pour nous. Ne devrions-nous pas être en mesure de mettre cette information à la disposition des gens qui s'occupent des ingérences étrangères?

M. Hatfield : Le gouvernement a de nombreux objectifs légitimes en marge de la cybersécurité. Ce que nous demandons, c'est un projet de loi sur la cybersécurité, qui pourrait prévoir un accès extraordinaire dans certains cas, toujours selon les besoins en la matière.

Le sénateur Cardozo : Vous avez parlé d'échange avec d'autres gouvernements. Madame Polsky, je crois que vous en avez parlé plus spécialement. Pourriez-vous nous en dire davantage à ce sujet?

M. Hatfield : Oui. Ce qui est préoccupant, c'est qu'à l'heure actuelle, une fois que les données recueillies aux fins de cybersécurité en vertu du projet de loi sont confiées à nos organismes de renseignement de sécurité, elles sont souvent transmises dans le cadre d'un échange de renseignements avec d'autres gouvernements étrangers. Bien entendu, une fois que les

Canadians are increasingly concerned that not all our allies can be trusted with all Canadian data, so the sense is that, even if our intent were always to use it for cybersecurity purposes, it could easily find very different applications in other hands.

Senator Cardozo: Do you have anything more to add, Ms. Polsky?

Ms. Polsky: I have to concur with what Mr. Hatfield said. There is significant concern, and this bill does not restrict the sharing of data. It specifies that it can be shared with foreign governments and institutions and international organizations. Once it's outside of Canada, we have no control over where it gets to be shared, whom it's being shared with and — if it's a matter of national concern — I have my doubts that any access-to-information request would actually be responded to other than to say, "It's a matter of national security. Thank you for the request but you're getting nothing." It would be a blank page.

How can Canadians have trust? We're told to trust. I'd rather have reason to trust, and this bill doesn't quite give enough assurances to provide a reason to trust. It's still too broad, non-specific and open to interpretation. I do appreciate — and our members appreciate — what a difficult task it is to craft legislation that is flexible and broad enough yet specific enough to go both ways to make it work. However, I think the consensus in our organization and with our members is that it's not good enough to pass a piece of legislation that has so many flaws that so many people recognize while still saying, "Just pass it. It's better than nothing. It's better than what we have."

You have the ability and the power to make recommendations that I hope would not cause significant delay and make something that actually protects information that, in some cases, does legitimately have to be shared with law enforcement, our American counterparts and our allies. Please make sure that it is done in a way where the information can only be used for cybersecurity.

The Deputy Chair: Thank you. Would you like to add anything, Mr. Grant?

Mr. Grant: No. I think they covered it.

Senator Yussuff: Thank you all for being here and sharing your thoughts. Mr. Hatfield and Ms. Polsky, I understand your concerns. I don't think you're here to raise the alarm bells for no

données quittent le Canada, nous n'avons aucun pouvoir contraignant d'en contrôler la destinée. Je pense que de nombreux Canadiens sont de plus en plus préoccupés par le fait qu'il y a des données canadiennes qui ne peuvent pas nécessairement être confiées à tous nos alliés. Ainsi, même si nous avions l'intention d'utiliser ces données à des fins de cybersécurité au départ, elles pourraient facilement servir à des applications très différentes si elles aboutissent dans d'autres mains.

Le sénateur Cardozo : Avez-vous quelque chose à ajouter, madame Polsky?

Mme Polsky : Je suis d'accord avec M. Hatfield. Il y a une préoccupation importante, et ce projet de loi ne restreint pas l'échange des données. Il précise qu'elles peuvent être échangées avec des institutions et des gouvernements étrangers ainsi qu'avec des organisations internationales. Une fois qu'ils se trouvent à l'extérieur du Canada, nous n'avons aucun contrôle sur l'endroit où les renseignements peuvent être communiqués, avec qui ils le sont et — s'il s'agit d'une question d'intérêt national — je doute que toute demande d'accès à l'information soit traitée autrement que pour dire : « C'est une question de sécurité nationale. Je vous remercie de la demande, mais vous n'obtenez rien. » Ce serait une page blanche.

Comment les Canadiens peuvent-ils avoir confiance? On nous dit de faire confiance. Je préférerais avoir des raisons de me fier, et ce projet de loi ne donne pas tout à fait suffisamment d'assurances pour cela. C'est encore trop large, imprécis et sujet à interprétation. Je comprends — et nos membres comprennent — à quel point il est difficile de rédiger une loi qui soit suffisamment souple, mais assez précise pour fonctionner dans les deux sens. Cependant, je pense que notre organisation et nos membres conviennent qu'on ne saurait se contenter d'adopter un projet de loi qui comporte des lacunes aussi évidentes, même si on se dit qu'il faut l'adopter, que c'est mieux que rien, mieux que ce que l'on a.

Vous avez la capacité et le pouvoir de formuler des recommandations qui, je l'espère, n'entraîneront pas de retard important, et de faire quelque chose qui protège réellement les renseignements qui, dans certains cas, doivent légitimement être communiqués aux organismes d'application de la loi, à nos homologues américains et à nos alliés. Veuillez donc vous assurer que cela se fait d'une façon où l'information ne peut être utilisée qu'à des fins de cybersécurité.

Le vice-président : Merci. Voulez-vous ajouter quelque chose, maître Grant?

Me Grant : Non. Je pense qu'ils ont tout dit.

Le sénateur Yussuff : Merci à tous d'être ici et de nous avoir fait part de vos réflexions. Monsieur Hatfield et madame Polsky, je comprends vos préoccupations. Je ne pense pas que vous

good reason. You're here for good purposes and to help us improve legislation.

However, as you know, Parliament went to great lengths to include many things that the original bill did not encompass, so this legislation has clearly been improved compared to the past version.

To acknowledge your point, there were proposed amendments that were ruled out of scope. All the legal minds involved in the process as we do this here — we don't do this by ourselves, and I'm only saying this so that we don't waste our time doing something that will be rejected by the House — have deemed this out of the scope of the legislation, and it's just the way the legislation has been drafted.

Given that reality — and I'm speaking for myself and not for my colleagues who will deal with this when we get to clause by clause — we're not likely to put in amendments that have already been rejected by the House of Commons because they're out of scope. Still, I'd like to acknowledge you're raising some important issues for us to consider.

I'll come back to a point my colleague just touched on — and maybe you can comment on it — which is the sharing of information with other governments, mostly the Five Eyes nations. We provide security based on what other countries sometimes share with us, and we're then able to better protect the Canadian public from harm. Some of it is necessary — and by the way, it prevents our country from experiencing harm. We know from experience.

Clearly, you don't see this is nefarious. You see this as legitimate in the context of protecting Canadians and defending our sovereignty and our country at the same time. I'll let you comment on that. I'm trying to provide a stage because I think improvements to the bill are welcome in this committee. Actually, almost every witness who has come here has acknowledged that this is a better bill than when it was first drafted.

Mr. Hatfield: I have a couple of quick comments on that. It's true that it is much better than how it was first drafted, and that's partly because these concerns were raised and answered. I think there could be a little bit more work done to continue that.

We're within the context of Bill C-22, which, as you know, is likely coming here soon, and I think it's hard not to interpret concerns in this bill in light of that bill, which really takes a wrecking ball to some of these issues.

soyez ici pour sonner l'alarme sans raison valable. Vous êtes ici à de bonnes fins et pour nous aider à améliorer la loi.

Cependant, comme vous le savez, le Parlement s'est donné beaucoup de mal pour inclure bien des aspects que le projet de loi initial n'englobait pas. Il est donc clair que cette mesure législative a été améliorée par rapport à la version précédente.

Pour répondre à votre question, certains amendements proposés ont été jugés irrecevables. Tous les juristes qui participent au processus — nous ne le faisons pas seuls, et je dis cela simplement pour que nous ne perdions pas notre temps à faire quelque chose qui sera rejeté par la Chambre — ont jugé que cela dépassait la portée du projet de loi, et c'est simplement à cause de la façon dont le projet de loi a été rédigé.

Compte tenu de cette réalité — et je parle en mon nom et non en celui de mes collègues qui traiteront de cette question lorsque nous procéderons à l'étude article par article —, il est peu probable que nous proposions des amendements qui ont déjà été rejetés par la Chambre des communes parce qu'ils dépassent la portée du projet de loi. J'aimerais tout de même reconnaître que vous soulevez des questions qui méritent notre attention.

Je vais revenir sur un point que mon collègue vient d'aborder — et peut-être pourriez-vous le commenter —, soit l'échange de renseignements avec d'autres gouvernements, surtout avec les pays du Groupe des cinq. Nous veillons à la sécurité en fonction des renseignements échangés à l'occasion avec d'autres pays, ce qui nous permet de mieux protéger le public canadien. C'est nécessaire, du moins en partie — et, soit dit en passant, cela empêche notre pays de subir des préjudices. Nous le savons d'expérience.

De toute évidence, vous ne voyez rien de répréhensible là-dedans. Vous estimez que c'est légitime pour protéger les Canadiens et défendre notre souveraineté et notre pays en même temps. Je vais vous laisser commenter. J'essaie d'alimenter le débat, car je pense que ce comité est prêt à apporter des améliorations au projet de loi. En fait, presque tous les témoins qui sont passés par ici ont reconnu qu'il s'agit d'un meilleur projet de loi que lorsqu'il a été rédigé au départ.

M. Hatfield : J'ai quelques brèves observations à faire à ce sujet. Il est vrai que cette version est bien meilleure que la première, et c'est en partie parce que ces préoccupations ont été soulevées et qu'on y a répondu. Je pense qu'on pourrait faire un peu plus pour poursuivre dans cette voie.

Nous sommes dans le contexte du projet de loi C-22 qui, comme vous le savez, sera probablement présenté bientôt, et je pense qu'il est difficile de ne pas interpréter les préoccupations soulevées à la lumière de cet autre projet de loi, qui démolit vraiment certaines de ces questions.

In terms of your point about the legitimacy of intelligence sharing, certainly, there are times it's important to share intelligence with our Five Eyes allies. This bill also proposes to expand the potential scope of data collection in Canada and the amount of data that we're collecting domestically on both Canadian firms and Canadians. We're also in a world where many Canadians have more concerns around the misuse of data, and some of our allies seem like less reliable partners around intelligence than they have been in the past.

The concern is that we're potentially gathering much more data. We have greater fears about the misuse of that data in the hands of other governments than previously. Should we not strengthen the oversight there and ensure that data is handed over very judiciously and only when strictly necessary for cybersecurity purposes, not for broader intelligence sharing of "you do this favour, I'll do that favour," potentially leading to quite a bit of Canadian data being misused for other purposes outside Canada?

Senator Yussuff: As you know, we don't know what the regulation will look like, but it will obviously be based on the scope of the bill. Do you not believe that some of the concerns that you're raising can be addressed in the regulatory oversight of this bill?

Mr. Hatfield: I suppose they could be, but from a rights perspective, it's better to have them defended in law. I'm not a lawyer, but it's my understanding that the House's concern regarding scope was specific to the House committee process, not necessarily to your process. Eventually, you could have something done here.

Senator Yussuff: Thank you so much.

The Deputy Chair: I have some questions of my own.

Apparently, similarly aligned democracies are also grappling with similar tensions between security and civil liberties. To your knowledge, are there international best practices that Canada should consider adopting to strengthen trust and accountability and to resolve this kind of tension?

The question is open to all of you.

Ms. Polsky: One of the leading Five Eyes partners that other countries look to is the Information Commissioner's Office of the U.K., as well as to Australia. They have both set out very clear guidelines. The way they go about passing legislation, to my understanding, includes a much more robust engagement of their populations.

Pour ce qui est de la légitimité de l'échange des renseignements, il est certain qu'il est parfois important de le faire avec nos alliés du Groupe des cinq. Le projet de loi propose également d'élargir la portée potentielle de la collecte de données au Canada et la quantité de données que nous recueillons à l'échelle nationale auprès des entreprises et des particuliers. Nous vivons également dans un monde où de nombreux Canadiens sont plus préoccupés par l'utilisation des données à mauvais escient, et certains de nos alliés semblent être des partenaires du renseignement moins fiables que par le passé.

Ce qui est préoccupant, c'est que nous recueillons de plus en plus de données, multipliant par là nos craintes de les voir tomber dans les mains d'autres gouvernements qui les utiliseraient à mauvais escient. Ne devrions-nous pas renforcer la surveillance à cet égard et veiller à ce que les données soient transmises de façon très judicieuse et uniquement lorsqu'elles sont strictement nécessaires aux fins de cybersécurité, et non dans le cadre d'un échange plus large de renseignements sous prétexte de se rendre service mutuellement? N'oublions pas qu'énormément de données canadiennes risquent d'être utilisées à mauvais escient à l'étranger.

Le sénateur Yussuff : Comme vous le savez, nous ignorons à quoi ressemblera le règlement, mais il sera évidemment fondé sur la portée du projet de loi. Ne croyez-vous pas que certaines des inquiétudes que vous soulevez pourront se dissiper à la lumière des règlements qui seront pris en application de ce projet de loi?

M. Hatfield : Je suppose qu'elles pourraient l'être, mais du point de vue des droits, il vaut mieux les défendre dans la loi elle-même. Je ne suis pas avocat, mais je crois comprendre que la préoccupation au sujet de la portée était propre au processus des comités de la Chambre, et pas nécessairement du vôtre. Vous pourriez éventuellement obtenir quelque chose ici.

Le sénateur Yussuff : Merci beaucoup.

Le vice-président : J'ai moi-même des questions à poser.

Il semble que les démocraties aux vues similaires sont également aux prises avec des tensions semblables entre la sécurité et les libertés civiles. À votre connaissance, y a-t-il des pratiques exemplaires internationales que le Canada devrait envisager pour renforcer la confiance et la reddition de comptes et résoudre ce genre de tension?

La question s'adresse à vous tous.

Mme Polsky : L'un des principaux partenaires du Groupe des cinq que les autres pays consultent est le commissariat à l'information du Royaume-Uni, ainsi que celui de l'Australie. Ils ont tous deux établi des lignes directrices très claires. D'après ce que je comprends, la façon dont ils procèdent pour adopter des lois comprend une participation beaucoup plus forte de leur population.

As an example, there was a piece of legislation here that received 49 submissions. In England, I think the equivalent was 45,000. It was comparable legislation. Yes, their population is slightly more than twice ours but the amount of engagement was much greater.

So many Canadians have no idea what this process is all about. I have been doing consulting in privacy for decades. This was new to me until relatively recently. People in Canada don't even know that they can submit a comment. They pound their keyboards online on social media like Facebook and think that will make a difference. It doesn't.

We need to look to other countries that do this much better in terms of having the public's input so that the lawmakers, legislators and bureaucrats have a real sense of what the people do and don't want.

Mr. Hatfield: Your instinct to look for international best practices is right. Although I don't have a major concern at this stage of this bill around that, I do think you should always be asking the relevant ministries why we have deviated in major ways from the practices of our comparable allies, which will be highly relevant when Bill C-22 reaches the Senate.

Mr. Grant: I sympathize with my fellow panellists' emphasis on consulting the public and checking in with other standards around the world. However, this bill has now gone through almost two complete rounds of the legislative process, and I think that process has been effective at rallying feedback. I would caution that, in trying to strike a balance between government powers to protect our critical infrastructure and privacy vis-à-vis the government, in trying to perfect that, we might be missing an opportunity to pass this legislation, which would protect us all from threat actors and foreign-state adversaries.

In a perfect world, we could consult forever, perfect things and still pass things on time, but we are past the deadline for when this legislation should have been passed.

The Deputy Chair: My follow-up on your answers is that the answers you have just provided relate to the process of borrowing best practices, but are there any specific provisions or amendments made in other countries that we can borrow that would be relevant to our deliberations at this point?

Mr. Hatfield: "Necessary and proportionate" is a very commonly well-recognized best-practice standard that we are lacking here. "Reasonableness" is a much more contestable standard, so adopting "necessary and proportionate" would be helpful.

À titre d'exemple, chez nous, un projet de loi a reçu 49 mémoires. En Angleterre, je crois que l'équivalent était de 45 000. C'était une loi comparable. Certes, leur population est un peu plus du double de la nôtre, mais le taux de participation était sensiblement plus élevé.

Un trop grand nombre de Canadiens n'ont aucune idée de la nature du processus. Je fais de la consultation en matière de protection des renseignements personnels depuis des décennies, mais ça, c'était nouveau pour moi jusqu'à tout récemment. Les gens au Canada ne savent même pas qu'ils peuvent soumettre un commentaire. Ils brandissent leur clavier en ligne sur les médias sociaux comme Facebook et pensent que cela fera une différence. Il n'en est rien.

Nous devons regarder ce qui se fait dans d'autres pays où la participation du public est bien meilleure, afin que les législateurs et les bureaucrates aient une idée réelle de ce que les gens veulent et de ce qu'ils ne veulent pas.

M. Hatfield : Votre instinct de rechercher des pratiques exemplaires internationales est bon. Même si je n'ai pas d'inquiétude majeure à ce chapitre à ce stade-ci du projet de loi, je pense que vous devriez toujours demander aux ministères responsables pourquoi nous avons tellement dévié des pratiques de nos alliés comparables, ce qui sera très pertinent lorsque le projet de loi C-22 arrivera au Sénat.

Me Grant : Je sympathise avec les autres témoins qui insistent sur la nécessité de consulter le public et de s'intéresser aux normes suivies dans d'autres pays. Or, ce projet de loi a pratiquement franchi deux séries complètes du processus législatif, et je pense que la rétroaction a été bonne. Je tiens toutefois à souligner qu'à force de vouloir perfectionner le projet de loi pour établir un équilibre entre les pouvoirs du gouvernement de protéger nos infrastructures essentielles ainsi que nos renseignements personnels, nous risquons de rater une occasion d'adopter un instrument qui nous protégerait tous contre les auteurs de menaces et les adversaires d'États étrangers.

Dans un monde idéal, on pourrait consulter les gens et perfectionner le libellé à tout jamais, voire tout faire à temps, mais voilà que nous avons dépassé la date limite pour l'adoption de ce projet de loi.

Le vice-président : Pour faire suite à vos réponses, celles que vous venez de donner portent sur le processus consistant à imiter des pratiques exemplaires, mais y a-t-il des dispositions ou des modifications précises apportées dans d'autres pays qui seraient pertinentes pour nos délibérations en ce moment?

M. Hatfield : « Nécessaire et proportionné » est une norme de pratique exemplaire très répandue qui fait défaut ici. Le « caractère raisonnable » est une norme beaucoup plus contestable, de sorte qu'il serait utile d'adopter l'expression « nécessaire et proportionné ».

The Deputy Chair: Thank you so much.

[*Translation*]

Senator Youance: Thank you to the witnesses.

My question is for Ms. Polsky and concerns the practical implementation of Bill C-8.

You've talked about grey areas several times. Beyond the principles, in the practical implementation of Bill C-8, when are privacy risks the greatest?

I'm trying to determine which risks are most concerning in the short term. You also mentioned data destruction. In the practical application of this bill, when are the risks the greatest?

[*English*]

Ms. Polsky: Most acute.

Part of the problem — and please understand that I have been inside organizations, from Fortune 50s to mom-and-pop shops, and advised and consulted governments across Canada — is that much of what Bill C-8 asks organizations to do involves things they ought to have been doing all along; it is nothing new to them. Yes, it is expensive, particularly for small- and medium-size businesses. They should have been doing this a long time ago. Without proper enforcement of those laws, of this one, the more things change, the more they stay the same.

Secure destruction is important because once the information gets into a department's hands or a foreign government's hands, when should it be destroyed. When? Destruction policies are internal to any organization, including government. It's not publicly known, and they can change on a whim. It is an internal document. There is no control or accountability. It can stay there forever. It can be stored insecurely.

We have seen that countless times. The former Canada Student Loans Program stored every applicant's information without encryption. A drive went missing — whoops. Alberta Health Services — every Albertan's health record was on a tape. It went missing — whoops. So they changed the process so that there would be continuity; someone would have to sign for it when the courier picked it up.

That's not adequate.

Secure destruction, secure storage, proper enforcement — and there are more than just those. It is a cascading effect. The Privacy Commissioner of Canada needs to have order-making

Le vice-président : Merci beaucoup.

[*Français*]

La sénatrice Youance : Je remercie les témoins.

Ma question s'adresse à Mme Polsky et porte sur la mise en œuvre concrète du projet de loi C-8.

Vous avez parlé des zones d'ombre à plusieurs reprises. Au-delà des principes, dans l'application concrète du projet de loi C-8, à quel moment les risques pour la vie privée deviennent-ils les plus élevés?

J'essaie de voir quels risques sont les plus préoccupants à court terme. Vous avez également parlé de la destruction des données. Dans la vie concrète de ce projet de loi, à quel moment les risques sont-ils les plus élevés?

[*Traduction*]

Mme Polsky : C'est très incisif.

Une partie du problème — et je vous prie de comprendre que j'ai l'expérience de diverses organisations, des sociétés Fortune 50 jusqu'aux petites entreprises familiales, et que j'ai conseillé et consulté les gouvernements partout au Canada —, c'est que le projet de loi C-8 demande aux organisations de faire ce qu'elles auraient dû faire dès le départ; ça n'a rien de nouveau pour elles. Oui, c'est coûteux, surtout pour les petites et moyennes entreprises. Elles auraient dû s'y prendre il y a longtemps. Sans une bonne application de ces lois, de celle-ci, plus ça change, plus c'est la même chose.

La destruction sécuritaire est importante, car une fois que l'information se retrouve entre les mains d'un ministère ou d'un gouvernement étranger, il s'agirait de savoir à quel moment elle devrait être détruite. Or, les politiques de destruction sont internes à toute organisation, y compris le gouvernement. Ce n'est pas connu du public, et il suffit de changer d'avis pour les modifier. C'est un document interne. Il n'y a pas de contrôle ni de reddition de comptes. Il peut rester tel quel pour toujours. Il peut être stocké de façon non sécurisée.

Nous l'avons vu à maintes reprises. L'ancien Programme canadien de prêts aux étudiants stockait les renseignements de chaque demandeur sans cryptage. Une clé USB a disparu, aïe aïe! Les services de santé de l'Alberta ont perdu une cassette — mauvaise nouvelle pour tous les dossiers médicaux qui y étaient enregistrés. Elle a disparu — aïe aïe! On a dès lors modifié le protocole pour qu'il y ait une continuité; quelqu'un devait signer lorsque le messager ramassait le colis.

Ce n'est pas suffisant.

La destruction sécuritaire, l'entreposage sûr, l'application adéquate de la loi — et il n'y a pas que cela. C'est un effet en cascade. Le commissaire à la protection de la vie privée du

power. We do not need an order-making power that ends up being overseen by another body to evaluate whether the commissioner's decision is adequate or proper. Give the Privacy Commissioner the power to do his job and be involved in this so he can actually protect Canadians' privacy. We already have his office, the framework is there and the laws are there — though inadequate and in need of updating, but in this particular instance, it could work.

Those are major concerns.

Mr. Hatfield: Surveillance routines are a fungus. They spread and go crazy in darkness, and they are kept limited in strong light. That is the concern around the potential for permanent secret orders that never become very clear to the public. The text of the order should be reviewable by the appropriate vetted authorities, and the public should be aware of the scope and extent.

Mr. Grant: I have two quick points.

On confidentiality, I understand that the annual reporting requirement does apply to confidentiality orders and that the reporting requirement to NSICOP and NSIRA within 90 days would also still apply to the confidential orders made under Part 1 of the act. I think this provides some response on whether these confidentiality orders are confidential forever. They would show up in an annual report.

On the point of government having free rein over data collected once it is in the government's clutches, I would note that in the other place, amendments were added to say that, for greater certainty, nothing in the act affects the provisions of the Privacy Act, and the Privacy Act does have purpose limitations. They only apply to personal information, so there might be other data, but I think the primary concern is about personal information in this context.

I just wanted to put that on the record here, too.

[*Translation*]

Senator Youance: You've raised several concerns. You spoke about public trust. Does the bill, as proposed and amended by the House of Commons, maintain public trust in the handling of personal data?

Canada doit avoir le pouvoir de rendre des ordonnances. Nous n'avons que faire d'un pouvoir qui finit par être supervisé par un autre organisme pour évaluer si la décision du commissaire est adéquate ou appropriée. Donnez au commissaire à la protection de la vie privée le pouvoir de faire son travail et d'intervenir de sorte qu'il puisse réellement protéger la vie privée des Canadiens. Nous avons déjà son bureau, le cadre est en place et les lois sont là — bien qu'elles soient inadéquates et doivent être actualisées, mais dans ce cas particulier, cela pourrait fonctionner.

Ce sont des préoccupations majeures.

M. Hatfield : Les surveillances de routine sont comme des champignons. Elles se propagent comme folles dans la pénombre, et il faut une lumière assez puissante pour les ralentir. Ce qu'on craint, c'est la possibilité que des ordonnances secrètes permanentes ne deviennent jamais assez claires pour le public. Le texte de l'ordonnance devrait pouvoir être examiné par les autorités compétentes, et le public devrait en connaître la portée.

Me Grant : J'ai deux brèves observations à faire.

En ce qui concerne la confidentialité, je crois comprendre que l'exigence de rapport annuel s'applique aux ordonnances de confidentialité et que l'obligation de faire rapport au Comité des parlementaires sur la sécurité nationale et le renseignement, le CPSNR, et à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, l'OSSNR, dans un délai de 90 jours s'appliquerait également aux ordonnances confidentielles prises en vertu de la partie 1 de la loi. Je pense que cela nous permet de savoir si ces ordonnances de confidentialité demeurent confidentielles pour toujours. Il en serait question dans un rapport annuel.

Quant au fait que le gouvernement puisse avoir toute liberté sur les données recueillies une fois qu'elles sont entre ses mains, je signale qu'à l'autre endroit, des amendements ont été ajoutés pour préciser qu'il est entendu que rien dans la loi n'a d'incidence sur les dispositions de la Loi sur la protection des renseignements personnels, et cette loi comporte des limites quant à la finalité. Cela ne s'applique qu'aux renseignements personnels, alors il pourrait y avoir d'autres données, mais je pense que la principale préoccupation concerne les renseignements personnels dans ce contexte.

Je tenais à ce que cela figure également au compte rendu.

[*Français*]

La sénatrice Youance : Vous avez soulevé plusieurs préoccupations. Vous avez parlé de la confiance du public. Est-ce que le projet de loi, tel qu'il est proposé et modifié par la Chambre des communes, permet de maintenir la confiance des membres du public dans la gestion de leurs renseignements personnels?

[*English*]

Mr. Hatfield: It has a dual effect, of course. Insofar as it improves our cybersecurity, then yes, it does contribute to Canadian trust and security. But if and when it leads to Canadian data being in the wrong hands at some point, or if it leads to a sort of future Snowden moment where it turns out there's been quite a bit going on that Canadians were not aware of that's suddenly unveiled, then, of course, it can be very damaging and destructive to trust.

Ms. Polsky: The other part is that if there are secret orders, things going on behind closed doors, in the dark, without that sunshine of visibility, Canadians will wonder. It's the same as Americans wonder what happened under a FISA order. It's secret. Nobody knows. Nobody is allowed to talk about it. There are rumours. It is hard to defeat rumours when they get started. So, no, that way it will undermine trust.

Reporting to Parliament is wonderful. It's after the fact. It may be statistical. There are no details. Rationale? It was necessary. For why? National security. It's vague.

Give us something that people can look to and say, "There was a threat from a nation-state in this continent or this hemisphere." That is something and not just, "Trust us." That hasn't worked.

Senator Yussuff: Mr. Grant, I thought you made a point earlier about security and privacy not being treated as competing objectives. That's always a challenge in an important piece of legislation. However, in plain terms, how would Parliament think about the risk of not doing enough to prevent a serious cyberattack versus the risk of government going too far?

Mr. Grant: Well, plainly, those risks need to be balanced as much as possible. This legislation, while not perfect, strikes a good balance in that regard.

As I said, these critical infrastructure providers that are being regulated here, many of them are extremely sophisticated. Many of them already know that they are under a constant barrage of cyberattacks, and they are doing what they can. Where the legislation helps is it creates a kind of collaborative process. By reporting all breaches and being able to share information among regulators, and with the proactive auditing mechanisms, we are

[*Traduction*]

M. Hatfield : Cela a un double effet, bien sûr. Dans la mesure où cela améliore notre cybersécurité, alors oui, ça contribue à la confiance et à la sécurité des Canadiens. Mais si et quand les données canadiennes se retrouvent entre de mauvaises mains à un moment donné, ou si cela mène en quelque sorte à un futur moment Snowden où il s'avère qu'il y a eu pas mal de choses dont les Canadiens n'étaient pas au courant et qui sont soudainement dévoilées, alors, bien sûr, il peut être très dommageable et destructeur de s'y fier.

Mme Polsky : L'autre aspect, c'est que s'il y a des ordres secrets, des choses qui se passent derrière des portes closes, dans le noir, sans la visibilité de ce qui se passe au grand soleil, les Canadiens vont se poser des questions. C'est comme si les Américains se demandaient ce qui s'était passé en vertu d'une ordonnance de la Foreign Intelligence Surveillance Act, la loi américaine sur la surveillance et le renseignement étranger, la FISA. C'est secret. Personne ne sait. Personne n'a le droit d'en parler. Il y a des rumeurs. Il est difficile d'étouffer les rumeurs une fois qu'elles commencent à circuler. Donc, non, de cette façon, cela ne fera que miner la confiance.

C'est merveilleux de faire rapport au Parlement. C'est après coup. C'est peut-être statistique. Il n'y a pas de détails. La justification? C'était nécessaire. Pour quelle raison? Sécurité nationale. C'est vague.

Donnez aux gens une information concrète dans le genre : « Il y avait une menace de la part d'un État-nation sur ce continent ou dans cet hémisphère. » C'est au moins quelque chose, et pas seulement « faites-nous confiance » tout court. Cela n'a pas fonctionné.

Le sénateur Yussuff : Maître Grant, je pensais que vous aviez dit tout à l'heure que la sécurité et la protection de la vie privée n'étaient pas traitées comme des objectifs concurrents. C'est toujours un défi dans le cadre d'une mesure législative importante. Cependant, pour parler simplement, comment le Parlement envisagerait-il le risque de ne pas en faire assez pour prévenir une cyberattaque grave par rapport au risque d'aller trop loin?

Me Grant : Eh bien, clairement, ces risques doivent être équilibrés autant que possible. Ce projet de loi, même s'il n'est pas parfait, établit un bon équilibre à cet égard.

Comme je l'ai dit, bon nombre des fournisseurs d'infrastructures essentielles qui sont réglementés ici sont extrêmement avancés. Ils savent déjà qu'ils sont constamment la cible de cyberattaques, et ils font ce qu'ils peuvent. Là où le projet de loi est utile, c'est qu'il crée une sorte de processus collaboratif. En signalant toutes les atteintes et en permettant l'échange d'information entre les organismes de réglementation,

raising the tide and hopefully lifting all boats in that regard, which will really help.

Similarly, the supply chain requirements in the CCSPA would also contribute to promoting privacy in a much broader space than just this critical infrastructure and government. I sympathize with the submissions made by my fellow panellists and others at the Citizen Lab, but fighting to get this absolutely perfect may be impossible, and we are due for this legislation.

Senator Yussuff: Listening to the debate around this bill, do you think there is sometimes the risk that we frame every cybersecurity power as government overreach without weighing the real consequences to Canadians on critical infrastructure that might be breached, with foreign actors taking advantage of the challenges that we face?

Mr. Grant: We have heard submissions on both sides of that point. Listening to others today, you have had really strong proponents of the bill and passing it in its current form with urgency, as well as other pretty reasonable submissions on potential government overreach. Right now, I think that overreach is more theoretical than anything else. While there could be improvements made and it is not perfect in its current form, again, I say pass it now.

The Deputy Chair: We still have time for more questions or closing remarks, if you wish.

Ms. Polsky: Let me challenge my fellow panellist, Mr. Grant. We certainly don't look for perfection, and it is too easy to say making tweaks and minor amendments that will have a major and fundamental positive impact is striving for perfection. It is striving for better. "Good enough" isn't a good enough reason to pass the legislation as it is. It really could benefit from some minor tweaks that would make a huge difference and improve Canadians' trust. Give them a reason to trust.

Mr. Hatfield: Laws sometimes last a very long time. Small imperfections passed in a law today can turn out to be very impactful and could kick around for many years. We heard from some of the earlier witnesses, including ones who care a lot about this bill and believe it should pass, that the biggest obstacles to cybersecurity in Canada today are not whether we do or don't have this legislation. It's basic things like education, investment and other things that we can rush forward without rushing forward this bill.

ainsi qu'au moyen de mécanismes de vérification proactifs, nous faisons monter la marée pour que tous les bateaux puissent flotter au même niveau, ce qui sera vraiment utile.

De même, les exigences relatives à la chaîne d'approvisionnement prévues dans la Loi sur la protection des cybersystèmes essentiels, la LPCC, contribueraient également à promouvoir la protection des renseignements personnels dans un espace beaucoup plus vaste que cette infrastructure essentielle et le gouvernement. Je comprends les arguments présentés par mes collègues et d'autres témoins au Citizen Lab, mais il est peut-être impossible de se battre pour que ce projet de loi soit absolument parfait, et il est grand temps de l'adopter.

Le sénateur Yussuff : En écoutant le débat entourant ce projet de loi, pensez-vous qu'il y a parfois le risque que nous considérions chaque pouvoir en matière de cybersécurité comme une intervention excessive du gouvernement sans tenir compte des conséquences réelles pour les Canadiens sur les infrastructures essentielles qui pourraient être endommagées par des acteurs étrangers qui tirent parti des défis auxquels nous sommes confrontés?

Me Grant : Nous avons entendu des arguments des deux côtés. D'après ce que j'ai entendu aujourd'hui, vous avez eu de très solides partisans du projet de loi et de son adoption urgente dans sa forme actuelle, ainsi que d'autres mémoires assez raisonnables sur la possibilité que le gouvernement aille trop loin. À ce stade-ci, je pense que cette exagération est plus théorique qu'autre chose. Même si le projet de loi n'est pas parfait dans sa forme actuelle et qu'il y aurait lieu de l'améliorer, j'insiste pour dire qu'il faut l'adopter sans plus tarder.

Le vice-président : Il nous reste du temps pour d'autres questions ou observations finales, si vous le souhaitez.

Mme Polsky : Permettez-moi de lancer un défi à mon collègue, Me Grant. Nous ne visons certainement pas la perfection, et il est trop facile de dire qu'apporter des ajustements et des modifications mineures qui auront un impact positif majeur et fondamental, c'est viser la perfection. C'est chercher à mieux faire. « Assez bien » n'est pas une cote suffisante pour adopter le projet de loi dans sa forme actuelle. Il pourrait vraiment bénéficier de quelques ajustements mineurs qui feraient une énorme différence et renforceraient la confiance des Canadiens. Donnez-leur une raison de faire confiance.

M. Hatfield : Les lois durent parfois très longtemps. Les petites imperfections adoptées dans une loi aujourd'hui peuvent se révéler très percutantes et traîner pendant de nombreuses années. Nous avons entendu certains témoins précédents, y compris ceux qui se soucient énormément de ce projet de loi et qui croient qu'il devrait être adopté, que les plus grands obstacles à la cybersécurité au Canada aujourd'hui ne sont pas le fait que nous ayons ou non cette loi. Il y a des aspects fondamentaux comme l'éducation, les investissements et autres

So, yes, pass a version of this bill eventually, but there is no reason to get this done so urgently that you can't take a few more weeks to make necessary improvements.

Senator Yussuff: I would only make the point that we have heard from a lot of Canadians who have written to us and communicated with us, and they don't distrust their government. They want their government to do the right thing and to protect them from foreign actors taking advantage of their security.

Ms. Polsky: That is a good thing — that Canadians are voicing their concerns. I certainly don't have access to the submissions made by Canadians, but I would wonder, given the lack of education about all computer issues — desktop computers have been around since the 1980s. There is still not any effective, comprehensive education. There is coding. There's being cyber-safe. There's being polite online. But how to defend and protect yourself from scams, which are basics now — human nature is the biggest risk, and that is what is in every organization in both the public and private sectors. Without that basic, fundamental understanding of what they are dealing with, the people are the risk.

For the people who have submitted comments — and I applaud them and am glad they did — what is their actual level of understanding of the technology and of the risks, more than just to say, "Government, do something"? Because that absolves them of doing for themselves.

Senator Yussuff: My only point is we shouldn't make assumptions we don't know the answers to.

Ms. Polsky: That's right. We don't.

The Deputy Chair: Thank you. This has been a very rich session with a great diversity of thought and views. We really appreciate all of those views. This brings us to the end of our time with this panel.

Thank you, Ms. Polsky, Mr. Hatfield and Mr. Grant for taking the time to meet with us today. We greatly appreciate your testimony as we consider this bill.

This concludes the agenda items for today's meeting. Our next meeting will take place on Monday, June 1, at our usual time, 4 p.m., when we intend to begin clause-by-clause consideration of Bill C-8.

que nous pouvons cultiver à toute vapeur sans précipiter l'adoption de ce projet de loi.

Donc, oui, adoptez une version du projet de loi à un moment donné, mais il n'y a aucune raison d'agir si rapidement sans prendre quelques semaines de plus pour y apporter les améliorations nécessaires.

Le sénateur Yussuff : Je me contenterai de dire que nous avons entendu beaucoup de Canadiens qui nous ont écrit et communiqué avec nous, et ils ne se méfient pas de leur gouvernement. Ils veulent que leur gouvernement fasse ce qu'il faut et les protège contre des acteurs étrangers qui profitent de leur sécurité.

Mme Polsky : C'est une bonne chose que les Canadiens expriment leurs préoccupations. Je n'ai certainement pas accès aux mémoires présentés par les Canadiens, mais je me pose des questions sur le manque de sensibilisation à toutes les questions informatiques. Les ordinateurs de bureau existent pourtant depuis les années 1980, mais il n'y a toujours pas d'éducation efficace et complète à ce chapitre. Il y a la codification. Il y a la cybersécurité. Il y a l'exigence d'être poli en ligne. Mais nul ne sait comment se défendre et se protéger contre les escroqueries, ce qui est devenu fondamental — la nature humaine est le plus grand risque, que ce soit dans le secteur public ou privé. Sans cette compréhension fondamentale de ce à quoi ils ont affaire, ce sont les gens eux-mêmes qui incarnent le risque.

Pour les personnes qui ont présenté des commentaires — et je les en félicite —, quel est leur niveau réel de compréhension de la technologie et des risques, au-delà de s'attendre à ce que le gouvernement fasse quelque chose, les exonérant ainsi d'agir pour eux-mêmes.

Le sénateur Yussuff : Tout ce que je veux dire, c'est que nous ne devrions pas faire de suppositions dont nous ignorons les réponses.

Mme Polsky : En effet, nous ne le devrions pas.

Le vice-président : Merci. Cette séance a été très enrichissante et a suscité une grande diversité de réflexions et de points de vue. Nous apprécions vraiment toutes ces opinions. C'est ce qui met fin à notre séance avec ce groupe de témoins.

Merci, madame Polsky, monsieur Hatfield et maître Grant, d'avoir pris le temps de nous rencontrer aujourd'hui. Nous vous sommes très reconnaissants de votre témoignage dans le cadre de notre étude du projet de loi.

Cela met fin aux points à l'ordre du jour de la réunion d'aujourd'hui. Notre prochaine réunion aura lieu le lundi 1er juin, à l'heure habituelle, 16 heures, où nous avons l'intention de commencer l'étude article par article du projet de loi C-8.

Members are encouraged to contact the Office of the Law Clerk and Parliamentary Counsel should they wish to bring forward amendments and to share the amendments with the clerk as soon as possible.

If you would like your amendments bundled and distributed in advance of the meeting, please share them with the clerk by Friday morning at the latest. Otherwise, please bring sufficient copies of your amendments in English and French to the meeting.

With that, I wish everyone a good evening.

(The committee adjourned.)

Les membres du comité sont invités à communiquer avec le Bureau du légiste et conseiller parlementaire s'ils souhaitent proposer des amendements et à en faire part à la greffière dès que possible.

Si vous souhaitez que vos amendements soient regroupés et distribués avant la réunion, veuillez les transmettre à la greffière au plus tard vendredi matin. Sinon, veuillez apporter suffisamment de copies de vos amendements en anglais et en français à la réunion.

Sur ce, je vous souhaite à tous une bonne soirée.

(La séance est levée.)