EVIDENCE

OTTAWA, Monday, March 27, 2023

The Standing Senate Committee on National Security, Defence and Veterans Affairs met with videoconference this day at 4 p.m. [ET] to examine and report on issues relating to national security and defence generally; and, in camera, for the consideration of a draft agenda (future business).

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

[*English*]

The Chair: Welcome to this meeting of the Standing Senate Committee on National Security, Defence and Veterans Affairs. I am Tony Dean, senator from Ontario, the chair of the committee. I now invite my colleagues to introduce themselves.

[*Translation*]

Senator Dagenais: Jean-Guy Dagenais, Quebec.

Senator Boisvenu: Senator Boisvenu, Quebec.

[*English*]

Senator M. Deacon: Good afternoon. Marty Deacon, Ontario.

Senator Richards: David Richards, New Brunswick.

Senator R. Patterson: Rebecca Patterson, Ontario.

Senator Yussuff: Hassan Yussuff, Ontario.

Senator Dasko: Donna Dasko, senator from Ontario.

[*Translation*]

Senator Gignac: Clément Gignac, senator from Quebec.

[*English*]

Senator Boehm: Peter Boehm, Ontario.

The Chair: For those watching live across Canada, we are once again focusing our attention on cyber-threats to Canada's defence infrastructure. We are pleased to welcome to today's session, from the National Security and Intelligence Committee of Parliamentarians, the Honourable David McGuinty, Member of Parliament for Ottawa South and chair of the committee, The Honourable Senator Frances Lankin, a member of the committee, Lisa-Marie Inman, Executive Director and Nabil Bhatia, Review Analyst. Thank you for joining us today.

TÉMOIGNAGES

OTTAWA, le lundi 27 mars 2023

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, pour en faire rapport, les questions concernant la sécurité nationale et la défense en général; et à huis clos, pour étudier un projet d'ordre du jour (travaux futurs).

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

[*Traduction*]

Le président : Bonjour et bienvenue à cette réunion du Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants. Je suis Tony Dean, sénateur de l'Ontario et président du comité. J'invite mes collègues à se présenter à leur tour.

[*Français*]

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

Le sénateur Boisvenu : Sénateur Boisvenu, du Québec.

[*Traduction*]

La sénatrice M. Deacon : Bon après-midi. Marty Deacon, de l'Ontario.

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

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

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

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

[*Français*]

Le sénateur Gignac : Clément Gignac, sénateur du Québec.

[*Traduction*]

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

Le président : Pour ceux qui nous regardent en direct de partout au Canada, je rappelle que nous nous concentrons aujourd'hui sur les cybermenaces à l'endroit de l'infrastructure de défense du Canada. Nous avons le plaisir d'accueillir à la séance d'aujourd'hui, l'honorable David McGuinty, député d'Ottawa-Sud et président du Comité des parlementaires sur la sécurité nationale et le renseignement, l'honorable sénatrice Frances Lankin, membre du même comité, Lisa-Marie Inman, directrice générale, et Nabil Bhatia, analyste de révision. Je vous remercie de vous être joints à nous aujourd'hui.

You have been invited to speak to your report from February 14, 2022, entitled *Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack*. We will begin by inviting you to provide your opening remarks to be followed by questions from our members. Mr. McGuinty, you may begin whenever you're ready. Welcome.

Hon. David McGuinty, P.C., M.P., Chair, National Security and Intelligence Committee of Parliamentarians: Thank you very much, Mr. Chair, and thank you very much honourable members of the committee for your invitation to appear today as you explore the topic of cyber-threats to Canada's defence infrastructure. As the chair has just announced, I am joined by Senator Frances Lankin, who has been a member of the National Security and Intelligence Committee of Parliamentarians, or NSICOP, since its inception. I am also joined by the executive director of the secretariat, Lisa-Marie Inman to my right, and Nabil Bhatia, a review analyst with our secretariat.

It is our pleasure to discuss the *Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack.* It is a 127-page foundational report on the cyberdefence of government networks. Its time frame was between the years 2001 and 2021 — 20 years chosen deliberately by the committee to help indicate the evolution of our cyber systems and networks.

The National Security and Intelligence Committee of Parliamentarians submitted this report to the Prime Minister on August 11, 2021. It was tabled in Parliament on February 14, 2022.

[*Translation*]

The review examined how the government defends its systems and networks from cyber-attack. We conducted the review because of the importance of federal systems and networks, which form part of Canada's critical infrastructure.

These networks store large amounts of personal information, and are used to deliver essentially every government service. They also store information on Canada's military operations, defence technology and equipment, as well as information about military strategies, intelligence, and procurement plans.

The theft of information about military operations could reveal strategies, targets, and capabilities. This could jeopardize military operations, intelligence gathering, and the safety of Canadian Armed Forces personnel around the world. Government and military networks are under relentless cyber-

Vous avez été invités pour vous exprimer sur votre *Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques* qui a été publié le 14 février 2022. Nous allons commencer par vous inviter à présenter vos remarques préliminaires, qui seront suivies de questions de la part de nos membres. Monsieur McGuinty, vous pouvez commencer quand vous êtes prêt. Je vous souhaite la bienvenue.

L'honorable David McGuinty, c.p., député, président du Comité des parlementaires sur la sécurité nationale et le renseignement : Merci beaucoup, monsieur le président, et merci beaucoup, chers membres du comité, de m'avoir invité à comparaître aujourd'hui pour aborder le sujet des cybermenaces à l'endroit de l'infrastructure de défense du Canada. Comme le président vient de l'annoncer, je suis accompagné de la sénatrice Frances Lankin, qui est membre du Comité des parlementaires sur la sécurité nationale et le renseignement depuis sa création. Je suis également accompagné de la directrice générale du secrétariat, Lisa-Marie Inman, à ma droite, et de Nabil Bhatia, analyste de révision au sein de notre secrétariat.

Nous sommes heureux de discuter du *Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques.* Il s'agit d'un rapport fondamental de 127 pages sur la cyberdéfense des réseaux du gouvernement. Il porte sur une période de 20 ans — entre 2001 et 2021 — choisie délibérément par le comité pour mieux illustrer l'évolution de nos cybersystèmes et de nos cyberréseaux.

Le Comité des parlementaires sur la sécurité nationale et le renseignement a présenté le rapport au premier ministre le 11 août 2021. Le rapport a été déposé devant le Parlement le 14 février 2022.

[*Français*]

L'examen a permis d'étudier la façon dont le gouvernement protège ses systèmes et réseaux contre les cyberattaques. Le comité a réalisé cet examen en raison de l'importance des systèmes et des réseaux fédéraux qui font partie de l'infrastructure essentielle du Canada.

Des tonnes de renseignements personnels sont stockées dans ces réseaux, lesquels sont utilisés pour offrir pratiquement tous les services gouvernementaux. De plus, ils contiennent des renseignements sur les opérations militaires, les technologies et le matériel de défense du Canada ainsi que des stratégies, données de renseignement et plans d'approvisionnement militaires.

Le vol de renseignements concernant les opérations militaires pourrait révéler des stratégies, des cibles et notre capacité, et ainsi compromettre les opérations militaires, la collecte de renseignement et la sécurité du personnel des Forces armées canadiennes partout dans le monde. Les réseaux

attack by a number of states, most notably China and Russia, and may be vulnerable to malware and other forms of cybercrime.

Today, the federal government is a world leader in defending its networks. But this was not always the case. In the 2000s and early 2010s, China and Russia conducted successful cyber-intrusions against the Department of National Defence, for example. Also in the early 2010s, China carried out damaging cyber-attacks against 31 federal departments. This was a wake-up call in terms of the scale of the government's cyber vulnerability and its poor defences.

Since then, the government has incrementally developed a strong cyber defence system, both in terms of governance and technical capability.

[*English*]

This brings me to our findings and recommendations. I'll begin with two findings.

First, our report noted that over time, the government's approach to cyberdefence evolved toward one that considers all government systems as a single enterprise. This horizontal approach has considerably improved cyberdefence, although we found it is challenged by the vertical nature of accountability in the government. Deputy heads have a lot of leeway to reject government-wide, horizontal cybersecurity policies and protections.

Second, our report noted that not all federal organizations receive the same cybersecurity protection. There are two related reasons for this.

First, the Treasury Board's cybersecurity policies do not apply to the entire government. When they do apply, they do not always apply evenly.

Second, departments are not obligated to adopt the cyberdefence services offered by Shared Services Canada, or SSC, and the Communications Security Establishment, also known as CSE. They are not obligated to do so. This means that many federal organizations are entirely outside the government's cyberdefence perimeter while others pick and choose services and do not subscribe to the full suite of government security services.

gouvernementaux et militaires font continuellement l'objet de cyberattaques par plusieurs États, plus particulièrement la Chine et la Russie. Les réseaux pourraient être vulnérables aux logiciels malveillants et à d'autres formes de cybercrimes.

Aujourd'hui, le gouvernement fédéral est un chef de file mondial en ce qui concerne la protection de ses réseaux. Toutefois, cela n'a pas toujours été le cas. Dans les années 2000 et au début des années 2010, la Chine et la Russie ont réussi à s'introduire dans les réseaux du ministère de la Défense nationale, par exemple. Toujours au début des années 2010, la Chine a lancé des cyberattaques préjudiciables contre 31 ministères fédéraux. Ces événements ont tiré la sonnette d'alarme quant à l'étendue de la vulnérabilité informatique du gouvernement et ses mécanismes de défense inadéquats.

Depuis, le gouvernement a graduellement élaboré un solide système de cyberdéfense, tant sur le plan de la gouvernance que sur le plan des capacités techniques.

[*Traduction*]

Cela m'amène à discuter de nos conclusions et de nos recommandations. Je commencerai par deux conclusions.

Premièrement, le rapport du comité révèle qu'au fil du temps, l'approche du gouvernement à l'égard de la cyberdéfense est devenue plus globale en considérant l'ensemble des systèmes gouvernementaux comme un tout. Cette approche horizontale a considérablement amélioré les capacités du gouvernement en matière de cyberdéfense. Nous avons toutefois constaté que ces capacités sont compromises par la nature verticale de la structure de reddition de comptes au sein du gouvernement. Les administrateurs généraux ont beaucoup de latitude lorsque vient le temps d'adopter ou non les politiques et systèmes horizontaux et pangouvernementaux en matière de cybersécurité.

Deuxièmement, le rapport révèle que ce ne sont pas tous les organismes fédéraux qui bénéficient de la même protection en matière de sécurité. Deux raisons expliquent cela.

Pour commencer, les politiques en matière de cybersécurité du Conseil du Trésor ne s'appliquent pas à tout le gouvernement. Et si elles s'appliquent, elles ne s'appliquent pas toujours de façon uniforme.

Ensuite, les ministères n'ont pas l'obligation d'adopter les services de cyberdéfense offerts par Services partagés Canada et le Centre de la sécurité des télécommunications. Autrement dit, de nombreux organismes fédéraux évoluent entièrement à l'extérieur du périmètre de cyberdéfense du gouvernement, alors que d'autres choisissent seulement certains services offerts par ces organismes.

These gaps and inconsistencies, we concluded, undermine the strength of the government's overall enterprise approach to cyberdefence. The interconnectedness of government systems means that the government's cyberdefence perimeter is only as strong as its weakest link. For example, our report noted that the Department of National Defence, or DND, is responsible for monitoring its own networks. While the committee did not examine DND or any other departments' cybersecurity specifically, we are confident that departments that receive cybersecurity services from Shared Services Canada and the Communications Security Establishment are far better protected than those that do not.

As we say in the report, CSE's dynamic defence tools are world-class, and they are constantly evolving to keep pace with the threat. Because we did not look into DND in depth, we are very encouraged to hear that your committee is considering a study of DND's cybersecurity.

Bringing more and more departments into the cyberdefence perimeter that has been created by Shared Services Canada and CSE creates a virtuous cycle, and this is how. As more departments subscribe to the government's cyberdefence services, CSE obtains and analyzes more data, which allows it to better protect all the departments within the perimeter. Even though the protection offered by Shared Services Canada and CSE will never block all threats, their combined cyberdefence services offer the greatest likelihood of protecting government data and systems.

With all this in mind, the committee made two recommendations.

First, the committee recommended that the government continue to strengthen this enterprise approach to cyberdefence while keeping up with evolution in technology and the threat environment.

Second, we recommended that the government bring all federal organizations into the cyberdefence perimeter and provide them with a full range of cyberdefence tools and that the cybersecurity policy suite should apply to all federal organizations — which isn't the case today.

The government agreed with both recommendations.

Ces incohérences et disparités affaiblissent l'approche intégrée du gouvernement à l'égard de la cyberdéfense. L'interdépendance des systèmes gouvernementaux signifie que le périmètre de cyberdéfense du gouvernement est aussi solide que son maillon le plus faible. Par exemple, le rapport du comité révèle que le ministère de la Défense nationale est responsable de surveiller ses propres réseaux. Bien que le comité n'ait pas examiné la cybersécurité du ministère de la Défense nationale ou d'autres ministères en particulier, il est persuadé que les ministères qui bénéficient des services de cybersécurité de Services partagés Canada et du Centre de la sécurité des télécommunications sont beaucoup mieux protégés que ceux qui n'en bénéficient pas.

Comme le comité l'explique dans son rapport, les outils de défense dynamiques du Centre de la sécurité des télécommunications sont de renommée mondiale, et sont mis à jour constamment pour qu'ils demeurent adaptés aux menaces. Puisque le comité n'a pas examiné le cas du ministère de la Défense nationale en profondeur, il est heureux d'entendre que votre comité envisage d'examiner le système de cybersécurité de ce ministère.

Le fait d'étendre le périmètre de cyberdéfense créé par Services partagés Canada et le Centre de la sécurité des télécommunications à de plus en plus de ministères crée un cercle vertueux. À mesure que d'autres ministères adoptent les services de cyberdéfense du gouvernement, le Centre de la sécurité des télécommunications recueille et analyse d'autres données, ce qui lui permet de mieux protéger les ministères qui font partie du périmètre. Même si la protection offerte par Services partagés Canada et le Centre de la sécurité des télécommunications n'arrivera jamais à contrer toutes les menaces, les services qu'ils offrent, ensemble, constituent la meilleure chance de protéger les données et les systèmes du gouvernement.

Avec toutes ces considérations à l'esprit, le comité a formulé deux recommandations.

Tout d'abord, le comité a recommandé au gouvernement de continuer de renforcer son approche intégrée de la cyberdéfense, tout en restant au fait des évolutions technologiques et du contexte dans lequel les menaces se manifestent.

Deuxièmement, le comité a recommandé au gouvernement d'intégrer tous les organismes fédéraux dans le périmètre de cyberdéfense, de leur fournir une gamme complète d'outils de cyberdéfense et de veiller à ce que l'ensemble des politiques de cybersécurité s'applique à tous les organismes fédéraux, ce qui n'est pas le cas aujourd'hui.

Le gouvernement est d'accord avec les deux recommandations.

[*Translation*]

Indeed, we are pleased that, for the first time, the government provided an official response to our recommendations. And that it did so again when our special report on Global Affairs Canada was tabled in November 2022. The government's responses strengthen accountability and transparency.

Having said that, the government has still not provided any updates with respect to the 23 recommendations contained in our other seven reports — all of which are listed in our 2021 annual report. This is not the only challenge that we have faced, however. As a committee, we also face three challenges in obtaining the information we are entitled to under the law and that we need to fulfil our mandate.

[*English*]

As a committee, we also face three challenges in obtaining the information we are entitled to under the law and that we need to fulfill our mandate.

First, several departments have cited reasons for not providing information that is outside the statutory exceptions found in the NSICOP Act, such as inappropriately refusing to provide relevant emails or a departmental study.

Second, several departments selectively refused to provide information even though the information fell within a request for information from the committee.

Third, the committee is concerned that departments are applying an overly broad interpretation of what constitutes a cabinet confidence. If departments were required to inform the committee of how many and which relevant documents are being withheld and on what basis, it would help resolve these challenges. Indeed, this year we expect Parliament to begin a comprehensive review of the NSICOP Act, which creates this committee.

While we look forward to making specific recommendations about potential reforms of the act to the designated committee at the appropriate time — drawing on seven years of practice — today I'd like to mention that the act could be amended to improve the committee's access to government information.

In closing, I wish to say that all of our reports are the result of the incredibly dedicated work of my colleagues on the committee. The cyberdefence report is yet another example of a unanimous, non-partisan review of a crucial government activity

[*Français*]

À vrai dire, le comité se réjouit du fait que, pour la première fois, le gouvernement a fourni une réponse officielle à ses recommandations. Il l'a fait une seconde fois lorsque le rapport spécial du Comité sur Affaires mondiales Canada a été déposé en novembre 2022. Ces réponses permettent d'accroître la responsabilisation et la transparence du gouvernement.

Cela dit, le gouvernement n'a toujours pas répondu aux sept autres rapports du comité, lesquels contiennent 23 recommandations, qui sont toutes énumérées dans le rapport annuel de l'année 2021 du comité. Il ne s'agit toutefois pas du seul défi auquel le comité fait face. Il se heurte également à trois défis relatifs à l'obtention des renseignements auxquels il a droit en vertu de la loi et dont il a besoin pour remplir son mandat.

[*Traduction*]

Il ne s'agit toutefois pas du seul défi auquel le comité fait face. Il se heurte également à trois défis relatifs à l'obtention des renseignements auxquels il a droit en vertu de la loi et dont il a besoin pour remplir son mandat.

D'abord, plusieurs ministères ont invoqué des raisons ne s'inscrivant pas dans les exceptions législatives de la Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement pour justifier leur refus de fournir des renseignements. Ils ont notamment refusé à tort de fournir des courriels pertinents et une étude ministérielle.

Ensuite, plusieurs ministères ont, de manière sélective, refusé de fournir des renseignements, même si ces renseignements s'inscrivaient dans une demande d'informations présentée par le comité.

Enfin, le comité craint que les ministères aient une interprétation trop large de ce que signifie « renseignements privilégiés ». Si les ministères avaient l'obligation de divulguer au comité la nature et le nombre de documents pertinents qui sont tenus confidentiels, ainsi que la raison pour laquelle ils le sont, il serait plus facile de résoudre ces problèmes. En effet, cette année, le Parlement doit entreprendre un « examen approfondi » de la Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement.

Bien que le comité se réjouisse à la perspective de soumettre d'éventuelles recommandations au comité désigné le moment venu, afin de réformer la Loi — en s'appuyant sur ses sept années d'expérience —, j'aimerais mentionner dès aujourd'hui que la loi pourrait être modifiée dans le but d'améliorer l'accès du comité aux renseignements du gouvernement.

En conclusion, j'aimerais souligner que tous nos rapports témoignent du travail acharné de mes collègues du comité. Le rapport sur la cyberdéfense n'est qu'un autre exemple d'un examen unanime et impartial d'une activité gouvernementale

by a committee of security-cleared senators and members of Parliament from all major parties and a number of Senate groups.

Thank you very much for your attention.

The Chair: Thank you very much, Mr. McGuinty. That's a telling final comment. Thank you. I'm sure your presentation will provoke a lot of questions.

Before proceeding to those questions, I would remind participants in the room to please refrain from leaning in too close to the microphone or remove your earpiece when doing so. This will avoid any sound feedback that could negatively impact committee staff in the room.

Mr. McGuinty, Senator Lankin, Ms. Inman and Mr. Bhatia are with us today for one hour. To ensure that each member has time to participate, I'm going to limit each question, including the answer, to four minutes. Please keep your questions succinct and identify the person you're addressing the question to.

I offer the first question, as in the normal course, to our deputy chair, Senator Dagenais.

[*Translation*]

Senator Dagenais: It's good to see you again, Mr. McGuinty. There is no doubt that your reports are very important, although people still need to adopt them.

I'd like to briefly discuss the procedures involved when a report is produced, such as the 2019 report, which was already addressing foreign interference. I think security briefings are among the most important aspects of governing a country.

How is the Prime Minister informed of such a report? Is he briefed personally or through an intermediary? When he is informed of instances of interference, among other things, who else is in the room?

Mr. McGuinty: First of all, the committee does not make decisions lightly regarding the choice of topic. There are certain criteria used to arrive at a final choice. It involves deliberations among all members of the committee. After these deliberations, we proceed with the work. We obviously have an extremely qualified team within the secretariat; we work with departments, we work with the information.

In the case of the foreign interference report, I can't recall the quantity of material, but I can tell you that we obtained over 2,500 documents and 37,000 pages of documentation. So we study the report, develop a plan for the review, and finalize the work. Once the work is finalized, the unredacted report is sent to the Prime Minister and the appropriate department. At this point,

primordiale, lequel a été réalisé par un comité composé de sénateurs et de députés dotés d'une habilitation de sécurité adéquate et issus de tous les parties et groupes majeurs.

Je vous remercie pour votre attention.

Le président : Merci beaucoup, monsieur McGuinty. Votre dernier commentaire est très révélateur. Je vous remercie. Je suis sûr que votre présentation va susciter beaucoup de questions.

Avant de passer aux questions, je voudrais demander aux participants présents dans la salle de ne pas se pencher trop près du microphone et de ne pas retirer leur oreillette. Cela permettra d'éviter une rétroaction sonore qui pourrait avoir un impact négatif sur le personnel du comité qui se trouve dans la salle.

M. McGuinty, la sénatrice Lankin, Mme Inman et M. Bhatia sont avec nous aujourd'hui pour une heure. Pour que chaque membre ait le temps de participer, je limiterai les questions et les réponses à quatre minutes. Je vous demande d'être bref et de préciser le nom de la personne à qui vous adressez votre question.

Je cède la parole à notre vice-président, le sénateur Dagenais, qui posera la première question, comme d'habitude.

[*Français*]

Le sénateur Dagenais : Je suis heureux de vous revoir, monsieur McGuinty. Il est certain que vos rapports sont très importants, encore faut-il que les gens les adoptent.

J'aimerais que l'on parle brièvement des procédures de travail lorsque vous produisez un rapport, comme celui, entre autres, de 2019, où il était déjà question d'ingérence étrangère. Je crois que le breffage sur la sécurité est un des éléments les plus importants de la gouvernance d'un pays.

Comment le premier ministre est-il informé d'un tel rapport? Est-il informé personnellement ou par personne interposée? Lorsqu'il est informé de cas d'ingérence, entre autres, quelles personnes sont présentes à ce moment-là?

M. McGuinty : Premièrement, le comité ne prend pas les décisions à la légère concernant le choix du sujet. Il y a des critères que l'on utilise pour arriver à un choix final. C'est une question de délibérations entre tous les membres du comité. C'est après ces délibérations que l'on procède au travail. On a évidemment une équipe extrêmement qualifiée au sein du secrétariat; on travaille avec les ministères, on travaille avec l'information.

Dans le cas du rapport d'ingérence étrangère, j'oublie la quantité de matériel, mais je peux vous dire que nous avons obtenu plus de 2 500 documents et 37 000 pages de documentation. Donc on étudie le rapport, on élabore un plan pour la revue, et on finalise le travail. C'est après avoir finalisé le travail que le rapport est envoyé au premier ministre et au

negotiations begin between the committee and the government. The issue is knowing where the government should remove certain information, but these tests are well established in law.

[*English*]

The government cannot redact our reviews on a willy-nilly basis. Upon receipt of an unredacted version, the Prime Minister does not sit with a black marker and black out passages. This is an iterative process among the committee, the secretariat and members of the government. They are bound, of course, to redact on four core grounds, which are stated in the act.

Once the review is finalized, it is presented to the Prime Minister. Once the Prime Minister has a copy of the unredacted version, I sit down with him and brief him for a period of time to walk through the details. The Prime Minister then takes the brief, will ask questions, might push back and might ask for more information.

You should know — and I think the committee and Canadians should know — that, wherever possible, the committee has always tended to be more transparent than less, pushing out for Canadians' benefit.

That's how the process works over time. Of course, once it is redacted, within a fixed period of time it has to be tabled on the floor of the House and the Senate.

Senator Richards: Thank you for being here today, Mr. McGuinty. These are two very quick questions. They might have been answered somewhat in your preliminary remarks.

How fast are these malware attacks evolving? How are we able to keep ahead of these attacks, or are we able to?

You mentioned cabinet confidence being interpreted, "too broadly." I'm wondering how this might hamper security activities.

Mr. McGuinty: One of the things the committee was struck with when it came face to face with this challenge of cyberprotection by the federal government was the speed, multiplicity and different categories of actors — state, non-state, domestic, international and sometimes foreign state actors acting through criminal elements. It turns out it's quite a sophisticated puzzle.

One of the things we came face to face with is that I think it's fair to say that the speed of change, the speed of the challenge and the complexity are all accelerating.

ministère approprié en version non caviardée. C'est à ce moment que les négociations débutent entre le comité et le gouvernement. La question est de savoir où le gouvernement veut enlever des éléments d'information, mais ce sont des tests bien établis dans la loi.

[*Traduction*]

Le gouvernement ne peut pas caviarder nos rapports comme bon lui semble. Lorsqu'il reçoit une version non caviardée, le premier ministre ne s'assoit pas avec un marqueur noir pour en biffer des passages. Il s'agit d'un processus itératif entre le comité, le secrétariat et les membres du gouvernement. Ils sont tenus, bien sûr, de caviarder pour quatre raisons essentielles, qui sont énoncées dans la loi.

Une fois la révision finalisée, elle est présentée au premier ministre. Une fois que le premier ministre a reçu une copie de la version non caviardée, je le rencontre et je prends le temps de l'informer des détails de la situation. Le premier ministre prend alors connaissance du dossier, pose des questions, peut faire des objections et demander des informations supplémentaires.

Vous devriez savoir — ainsi que le comité et les Canadiens — que, dans la mesure du possible, notre comité a toujours eu tendance à privilégier la transparence plutôt que le manque de transparence, et ce, dans l'intérêt des Canadiens.

C'est ainsi que le processus fonctionne au fur et à mesure. Bien entendu, une fois que le rapport est caviardé, il doit être déposé dans un délai déterminé à la Chambre et au Sénat.

Le sénateur Richards : Merci d'être présent aujourd'hui, monsieur McGuinty. J'ai deux questions très rapides à poser. Il se peut que vous y ayez déjà répondu dans vos remarques préliminaires.

À quelle allure ces attaques de logiciels malveillants évoluent-elles? Comment pouvons-nous devancer ces attaques, si nous en sommes capables?

Vous avez parlé d'une interprétation « trop large » de l'expression « secret du cabinet ». Je me demande comment cela pourrait entraver les activités de sécurité.

M. McGuinty : L'une des choses qui a frappé le comité lorsqu'il a relevé le défi de la cyberprotection pour le gouvernement fédéral, c'est la rapidité, la multiplicité et les diverses catégories d'acteurs — étatiques, non étatiques, nationaux, internationaux et parfois des acteurs étatiques étrangers agissant par l'intermédiaire d'éléments criminels. En réalité, il s'agit d'un casse-tête assez sophistiqué.

Je pense qu'il est juste de dire que la fréquence des changements, ainsi que la rapidité et la complexité du problème s'accentuent.

With respect to cabinet confidence, the committee respects the need for cabinet confidence and understands cabinet confidence. There is a role for cabinet confidence. But there were a couple of instances where the committee came face to face with information where we had been informed that it was a matter of cabinet confidence but then we found the information through other sources. We have gently but persuasively worked with the Privy Council Office and the Prime Minister's team to say, "No, sorry, you have to start working with us more openly and on behalf of Canadians; they need to know as much as we can inform them."

Of course, we're bound by the reality of dealing with highly classified information, where sources, methods and international relationships have to be protected, as well as the men and women who work in security and intelligence. I think we all accept that. I think Canadians accept that. But the cabinet confidence issue is one that is an organic, continuing dialogue.

Senator Richards: Thank you. As far as keeping up with the attacks by, say, Russia or China, we're on par with that, or do you think we have work to do, sir?

Mr. McGuinty: I would say this on behalf of the committee: We were unanimous in concluding that Canada is a leader in and through its three main actors — the Communications Security Establishment, Shared Services Canada, and the Treasury Board Secretariat — we are very fortunate to have evolved. One of the things we did with the six case studies in this review is to illustrate the evolution and the iterative nature of where we've arrived at.

The committee is not in a position to say that we can deal with every and all and every sophisticated overture, but we have in front of us a very robust system, one which, for example, even the United Kingdom is now relying on from time to time. So Canada's work through CSE is actually quite groundbreaking and I think internationally recognized.

Senator Richards: Thank you.

Mr. McGuinty: Thank you, sir.

Senator M. Deacon: Thank you, all four of you, for being here today. I welcome the question I ask to be answered across the table. That's fine.

Again, I can still remember where I was when the report of 2019 came out, and the work of the committee with a high, as you said, degree of intelligence and competence is greatly appreciated.

En ce qui concerne le secret du cabinet, le comité respecte la nécessité de ce secret et le comprend. Le secret du cabinet a une raison d'être. Toutefois, dans certains cas, le comité a découvert des informations dont on lui avait dit qu'elles relevaient du secret du cabinet dans des documents obtenus par d'autres sources. Nous avons travaillé avec le Bureau du Conseil privé et l'équipe du premier ministre de manière délicate, mais persuasive pour les convaincre de commencer à travailler avec nous de manière plus ouverte au nom des Canadiens; car ces derniers ont besoin de savoir tout ce que nous pouvons leur dire.

Bien sûr, nous sommes contraints par la réalité du traitement de renseignements hautement confidentiels, dans le cadre duquel les sources, les méthodes et les relations internationales doivent être protégées, de même que les hommes et les femmes qui travaillent dans le domaine de la sécurité et du renseignement. Je pense que nous l'acceptons tous. Je pense que les Canadiens l'acceptent. Mais la question du secret du cabinet est une question qui fait l'objet d'un débat organique et permanent.

Le sénateur Richards : Je vous remercie. Pour ce qui est de lutter contre les attaques de la Russie ou de la Chine, par exemple, nous sommes à la hauteur, ou pensez-vous que nous ayons encore du travail à faire, monsieur?

M. McGuinty : Je dirais ceci au nom du comité : nous avons conclu à l'unanimité que le Canada est un chef de file dans le domaine de la sécurité des communications et que, grâce à ses trois principaux acteurs — le Centre de la sécurité des télécommunications, Services partagés Canada et le Secrétariat du Conseil du Trésor — nous avons la chance d'avoir progressé. L'une des choses que nous avons faites avec les six études de cas de ce rapport est d'illustrer l'évolution et la nature itérative de la situation à laquelle nous sommes parvenus.

Le comité n'est pas en mesure de dire que nous pouvons répondre à tous les problèmes sophistiqués, mais nous avons devant nous un système très robuste, sur lequel, par exemple, même le Royaume-Uni s'appuie maintenant de temps en temps. Le travail du Canada par l'intermédiaire du Centre de la sécurité des télécommunications est donc tout à fait novateur et je pense qu'il est reconnu au niveau international.

Le sénateur Richards : Merci.

M. McGuinty : Merci, monsieur.

La sénatrice M. Deacon : Je vous remercie tous les quatre d'être présents aujourd'hui. Je serais heureuse que la question que je pose reçoive une réponse de la part des autres membres autour de la table. Cela ne pose aucun problème.

Je me souviens encore de l'endroit où je me trouvais lorsque le rapport de 2019 a été publié, et des travaux du comité qui, comme vous l'avez dit, présentent un degré élevé d'intelligence et de compétence, et qui sont grandement appréciés.

You mentioned, Mr. McGuinty, when you were speaking, that the recommendations from the Treasury Board, the policies and the services be extended to all federal organizations, including Crown corporations. Last week, I asked the witnesses who were here from CSE about this and was told essentially that the work is ongoing, but the sense I got was it was almost voluntary. That's the sense I got. It has been some time since these committee recommendations were made to the Prime Minister.

I'm wondering if you can give us a sense of why you think it's taking so long to get Crown corporations under the TBS cybersecurity umbrella. You described a number of factors today — the responsibility that some may not recognize the urgency of protecting their cyber systems.

Mr. McGuinty: I'll go first. Maybe Senator Lankin might want to chime in.

With respect to why the government has not moved more quickly on these recommendations, that's a question you'd have to put to the government directly, and I encourage you to do so. Whether it's through DND or anyone else you would like to call, whether it's the Treasury Board Secretariat, for example, who have a lot to say about this.

What we have identified is that being in the perimeter is better than not being in the perimeter. Being entirely in the perimeter is better than being halfway in the perimeter. Being outside the perimeter is a risk not just to your own organization, Crown corporation or otherwise, but to the entire federal family of organizations. We have listed how many are in, how many are out and how many are partly in or out.

We're of the view that Canada ought to up its game as a federal government. There's a lot of material here at risk, a lot of Canadians' personal data, military information, plans. This is national security writ large, so we are trying to illustrate through the study and through access to this information that we can really make improvements here. In many ways, that's why we only made 2 recommendations, not 20.

We're hopeful the government will move, and I would encourage you to call the Treasury Board Secretariat to ask them that question. Senator?

Monsieur McGuinty, vous avez mentionné lors de votre intervention que les recommandations du Conseil du Trésor, ainsi que les politiques et les services, devraient être étendus à toutes les organisations fédérales, y compris les sociétés d'État. La semaine dernière, j'ai interrogé les témoins du Centre de la sécurité des télécommunications qui étaient présents à ce sujet et on m'a répondu essentiellement que le travail était en cours, mais j'ai eu l'impression qu'il s'agissait presque d'une démarche facultative, sur la base du volontariat. C'est l'impression que j'ai eue. Cela fait un certain temps que les recommandations du comité ont été présentées au premier ministre.

Je me demande si vous pouvez nous expliquer pourquoi, selon vous, il faut tant de temps pour que les sociétés d'État puissent bénéficier de la protection du Secrétariat du Conseil du Trésor en matière de cybersécurité. Vous avez aussi évoqué aujourd'hui un certain nombre de facteurs, comme le fait que certains ne reconnaissent peut-être pas l'urgence de protéger leurs cybersystèmes.

M. McGuinty : Je commencerai par répondre à la question, mais la sénatrice Lankin voudra peut-être intervenir.

Quant à savoir pourquoi le gouvernement n'a pas donné suite plus rapidement à ces recommandations, c'est une question qu'il faut poser directement au gouvernement, et je vous encourage à le faire. Vous pouvez vous adresser au ministère de la Défense nationale ou à toute autre personne que vous souhaitez convoquer, par exemple au Secrétariat du Conseil du Trésor, qui a beaucoup de choses à dire à ce sujet.

Ce que nous savons, c'est qu'il est préférable d'être dans le périmètre que de ne pas y être. Il vaut mieux être entièrement dans le périmètre qu'à mi-chemin. Sortir du périmètre représente un risque non seulement pour l'organisation, la société d'État ou autre, mais aussi pour l'ensemble des organisations fédérales. Nous avons dressé la liste de ceux qui sont dans le périmètre, de ceux qui sont en dehors et de ceux qui sont à la limite du périmètre.

Nous sommes d'avis que le Canada devrait se montrer à la hauteur en tant que gouvernement fédéral. Il y a beaucoup de documents, de données personnelles de Canadiens, de renseignements militaires, de plans, qui sont exposés à des risques. Il s'agit de la sécurité nationale au sens large, et nous essayons donc de montrer, par le biais du rapport et de l'accès à ces informations, que nous pouvons réellement apporter des améliorations dans ce domaine. À bien des égards, c'est la raison pour laquelle nous n'avons formulé que 2 recommandations, et non 20.

Nous espérons que le gouvernement passera à l'action, et je vous encourage à appeler le Secrétariat du Conseil du Trésor pour poser cette question. Madame la sénatrice?

Hon. Senator Frances Lankin, P.C., Member, National Security and Intelligence Committee of Parliamentarians: Thank you. I think it's relevant to remember within the structure — and I'm talking about small "p" political — within relationships between departments and central agencies, there are a lot of issues that fall into this basket in terms of compliance, non-compliance, willingness to be brought in if it's not a compulsory direction. I think that's why the recommendation is so important that it become compulsory.

The reality in our structures and many departments and Crown corporations, the authorities rest with the deputy and related to the minister as well. But the fiscal decisions that are taken, the allocation of resources that are taken, which is part of what we do in our framework reviews as well. We have looked at what's the talk and what's the walk, and how does it match up? In this report, we saw very clearly that there are gaps and those gaps are dangerous for Canadians and dangerous for our national security, personal data, as the chair said.

I think that there is a willingness to move, but there's great reluctance and inertia at times within large departmental structures and the interdepartmental relations. So your voices on this will be important. I agree with the chair; calling Treasury Board is a very good idea.

The Chair: Thank you, both.

[*Translation*]

Senator Gignac: You delivered an amended report to the Canadian Prime Minister on February 8, 2022. The world has changed since February 2022. When we were in Brussels along with other parliamentarians, we were told that in the weeks leading up to the invasion of Ukraine, Russia had been very active in cyberattacks. One year later, in light of what you know about Russia's tactics, are there things in your report that you perhaps should have expanded upon, or things that you should have focused on more, given that the world has changed in the past year?

Mr. McGuinty: That is an excellent question, senator. It's not an issue that's been discussed by the committee since the report was presented to the House. Certainly, it has been determined that foreign interference is ongoing. It shows no signs of slowing down; on the contrary, it shows signs of increasing, of accelerating, but with respect to Russia, I am sorry, we are not in a position to tell you more. Everything about Russia is already in the report. Obviously, Russia and China were extensively discussed in our foreign interference report.

L'honorable sénatrice Frances Lankin, c.p., membre, Comité des parlementaires sur la sécurité nationale et le renseignement : Je vous remercie. Je pense qu'il est important de se rappeler qu'au sein de la structure — et je parle du petit « p » de la politique — dans les relations entre les ministères et les administrations centrales, il y a beaucoup de questions qui tombent de la nacelle pour ce qui est de la conformité, de la non-conformité, ou encore de la volonté de participer s'il ne s'agit pas d'une directive obligatoire. Je pense que c'est la raison pour laquelle il est si important que la recommandation devienne obligatoire.

En réalité, dans nos structures et dans de nombreux ministères et sociétés d'État, les pouvoirs appartiennent à l'adjoint et au ministre. Mais les décisions fiscales qui sont prises, l'allocation des ressources qui est faite, font également partie de ce que nous étudions dans nos examens du cadre. Nous avons observé ce qui était dit et ce qui était fait, et nous avons cherché à savoir si cela concordait. Dans ce rapport, nous constatons très clairement qu'il y a des lacunes et que ces lacunes sont dangereuses pour les Canadiens et pour notre sécurité nationale, en ce qui concerne les données personnelles, comme l'a dit le président.

Je pense qu'il y a une volonté d'agir, mais qu'il y a aussi parfois une forte réticence et une grande inertie au sein des grandes structures ministérielles et dans les relations interministérielles. À ce chapitre, il serait donc important que vous fassiez entendre votre voix. Je suis d'accord avec le président, vous devriez convoquer le Conseil du Trésor, c'est une très bonne idée.

Le président : Merci à tous les deux.

[*Français*]

Le sénateur Gignac : Vous avez remis un rapport modifié le 8 février 2022 au premier ministre canadien. Le monde a changé depuis février 2022. Lorsqu'on était à Bruxelles, en compagnie de certains parlementaires, on nous disait que dans les semaines qui avaient précédé l'invasion de l'Ukraine, la Russie avait été très active en matière de cyberattaques. Un an plus tard, à la lumière ce que vous savez concernant les tactiques de la Russie, y a-t-il des choses dans votre rapport que vous auriez peut-être dû approfondir davantage ou des éléments sur lesquels vous auriez dû vous pencher davantage, puisque le monde a changé depuis un an?

M. McGuinty : C'est une excellente question, monsieur le sénateur. Ce n'est pas une question sur laquelle le comité s'est penché depuis la présentation du rapport à la Chambre. C'est sûr et certain, on a bien déterminé que l'ingérence étrangère continue. Il n'y a aucun signe de ralentissement; au contraire, on voit des signes d'augmentation, d'accélération, mais en ce qui a trait à la Russie, je suis désolé, nous ne sommes pas en mesure de vous en dire plus. Tout ce qui touche la Russie est déjà dans le rapport. Évidemment, on a beaucoup parlé de la Russie et de la Chine dans notre rapport sur l'ingérence étrangère.

Senator Gignac: Let's move on to another part of the report, namely the government's activities in defending the system, the network, from cyberattacks. In your experience — it's not just the federal government, but also the private sector and private infrastructure — are there countries we could look to for inspiration in terms of having better coordination? There's the federal government, the private sector, universities; it can come in many shapes and sizes. Does Canada have a forum where information is exchanged between the various stakeholders?

Mr. McGuinty: Not that we know of. I don't think there is such a forum in Canada. The Communications Security Establishment works very closely with our universities; intellectual property and research are two issues. There is significantly more dialogue now with the provinces. The Communications Security Establishment (CSE) is also capable of detecting a problem. In the case studies presented in the report, several times it was the Communications Security Establishment that actually found a problem and notified the agency or Crown corporation to let them know they had a problem, before they even knew it. That's exactly what happened with the Canadian Armed Forces.

So that's why there's such a strong push for all departments, all agencies and all federal organizations to be within that protective perimeter. It would go a long way towards standardizing an all-encompassing protection system. I know that CSE is working extensively with the private sector right now. One of the case studies involves a Crown corporation, and another involves a private company that, for the first time, used CSE's resources, because it fell within a critical infrastructure sector; it was the first Canadian case study published in our report.

Senator Gignac: Thank you.

[*English*]

Senator Lankin: The chair just raised it with respect to the private sector and their own critical infrastructure in this country.

It is, to me, a critical issue that the communications are improved. CSE is doing an amazing job of reaching out. I would say CSIS does now too in a much broader way, but they're hampered in what they can say. They can share resources and skills, but in terms of what they can share in terms of their knowledge, the national security restrictions apply to them, and most people, the head of critical infrastructure organizations in the private sector doesn't have security clearance. That's true of our police forces too.

Le sénateur Gignac : Passons à un autre volet du rapport, soit les activités du gouvernement en matière de défense du système, du réseau contre les cyberattaques. Selon votre expérience — ce n'est pas juste le gouvernement fédéral, mais c'est également le secteur privé et les infrastructures privées — y a-t-il des pays dont on pourrait s'inspirer pour qu'il y ait une meilleure coordination? Il y a le gouvernement fédéral, le secteur privé, les universités, cela peut prendre toutes sortes de formes. Existe-t-il un forum au Canada où il y a un échange d'information entre les différentes parties prenantes?

M. McGuinty : Pas à ce que l'on sache, je ne crois pas qu'il y ait un forum au Canada. Le Centre de la sécurité des télécommunications travaille de très près avec nos universités; il y a la question de la propriété intellectuelle et celle des recherches. Il y a beaucoup plus de dialogue maintenant avec les provinces. Le Centre de la sécurité des télécommunications (CST) est aussi en mesure de détecter s'il y a un problème, et dans les études de cas qu'on a présentées dans le rapport, plusieurs fois, on voit que c'est le Centre de la sécurité des télécommunications qui a effectivement trouvé un problème et qui a avisé, qui est allé voir l'organisme ou la société de la Couronne pour lui expliquer qu'elle avait un problème avant même qu'elle le sache. C'est exactement ce qui s'est passé aux Forces armées canadiennes.

C'est donc pourquoi on insiste tellement pour que tous les ministères, toutes les agences, tous les organismes fédéraux doivent faire partie de ce périmètre de protection. Cela aiderait énormément à l'uniformisation d'un système de protection présent partout. Je sais que le CST collabore beaucoup en ce moment avec le secteur privé. Dans l'une des études de cas, il est question d'une société de la Couronne et dans une autre, il y a une société privée qui, pour la première fois, a utilisé les ressources du CST, parce que c'était dans un secteur d'infrastructures essentielles; c'est la première étude de cas au Canada qu'on a publiée dans notre rapport.

Le sénateur Gignac : Merci.

[*Traduction*]

La sénatrice Lankin : Le président vient de soulever la question du secteur privé et de ses infrastructures essentielles dans ce pays.

J'estime qu'il est essentiel d'améliorer la communication. Le Centre de la sécurité des télécommunications fait un travail remarquable de sensibilisation. Je dirais que le Service canadien du renseignement de sécurité le fait maintenant aussi de manière beaucoup plus large, mais il y a des limites à ce qu'il peut communiquer. Il peut partager ses ressources et ses compétences, mais pas ses connaissances, car il est soumis à des restrictions en matière de sécurité nationale, et que la plupart des responsables du secteur privé chargés des infrastructures essentielles n'ont pas de cote de sécurité. Il en va de même pour le corps policier.

There are issues that we have to come to terms with when we understand how pervasive this problem and the nature of these attacks are, and where they can come from, and where they can hit, which has equal effect on our economy, and our social well-being, as well as the structures of government and its relationship to people.

It's an important question that you've asked.

The Chair: Thank you very much.

Senator Yussuff: Let me thank all of you for being here and the report.

I guess the positive is the recommendation that's been accepted by Treasury Board, so you're not fighting or arguing. That's the good news. But what is more stunning, I guess, is the lack of resistance by the department to cooperate fully while you were conducting your report. I find it quite challenging to get my head around that, given that I thought the department would want to know if there are vulnerabilities and, more importantly, reveal what they might be able to tell you to help improve the system, given you're a non-partisan committee, but given the desire to review the act and how we can bring that in concert, so we have a full review. I guess the timeliness is going to be something I see as a priority for the government. The longer we wait, the vulnerabilities are still there, so through you, chair, maybe some points you can reflect on the need for this to happen, what you see in terms of your thoughts?

Mr. McGuinty: One of the things we wanted to do through the review was to be practical and grab the reader by the eyeball in the sense of we're going to illustrate what can happen. That's why the six case studies — the China case study that targeted 31 departments with 8 suffering severe compromises, the Treasury Board Secretariat, also referred to as TBS, and the Department of Finance Canada were the worst affected; or study Number 2, the private company using CSE's abilities for the first time; or case study 3, the heart bleed attack on the Canada Revenue Agency; or Number 4, the National Research Council attack by China, which cost us $100 million to repair, and we lost 40,000 files; or Number 5, the attack on DND by a state-sponsored actor, where significant amounts were stolen from DND; or case Number 6, perhaps the most worrisome for us, where in 2020 a state compromised a network of a Crown corporation and we believe a government department but other departments as well.

All this so that the government of Canada and those who are on the front lines of making these decisions at Treasury Board, or CIO's of individual departments or Crown corporations, could understand they could be next. They could be next. And that

Nous devons nous attaquer à certaines questions si nous comprenons à quel point ce problème et la nature de ces attaques sont omniprésents, d'où ils peuvent venir et où ils peuvent frapper, ce qui a des répercussions sur notre économie et notre bien-être social, ainsi que sur les structures du gouvernement et son rapport à la population.

C'est une question primordiale que vous posez là.

Le président : Merci beaucoup.

Le sénateur Yussuff : Permettez-moi de vous remercier tous pour votre présence et pour votre rapport.

Je suppose que le point positif est que la recommandation a été acceptée par le Conseil du Trésor, de sorte que vous n'êtes pas en train de vous démener ou de plaider cette cause. C'est une bonne nouvelle. Ce qui est plus étonnant, je suppose, c'est le fait que le ministère se soit montré peu enclin à coopérer pleinement pendant que vous réalisiez votre rapport. J'ai du mal à le comprendre, car il me semble que le ministère a tout intérêt à savoir s'il y a des failles et, surtout, à révéler les informations qui pourraient contribuer à améliorer le système, étant donné que vous êtes un comité non partisan, mais aussi parce qu'il faut réviser la loi et voir comment nous pouvons le faire tous ensemble, afin de procéder à une révision approfondie. Je pense que le respect des délais sera une priorité pour le gouvernement. Plus nous attendons, plus les failles sont importantes. Par votre intermédiaire, monsieur le président, j'aimerais demander au témoin de nous dire ce qu'il pense de la nécessité d'agir.

M. McGuinty : L'une des choses que nous voulions faire dans le cadre de cette étude était de rester pragmatique et d'attirer l'attention du lecteur en lui montrant ce qui peut arriver. C'est l'objectif des six études de cas. L'étude de cas sur la Chine montre que 31 ministères ont été ciblés et 8 ont été gravement compromis; dont le Secrétariat du Conseil du Trésor et le ministère des Finances du Canada qui ont été les plus touchés. Dans l'étude n^{o} 2, on détaille le cas d'une entreprise privée qui n^{o} 3 a utilisé les compétences du Centre de la sécurité des télécommunications pour la première fois. Dans l'étude de cas n^{o} 3, on raconte l'histoire de l'attaque HEARTBLEED contre l'Agence du revenu du Canada. Dans l'étude n^{o} 4, c'est l'attaque du Conseil national de recherches par la Chine, dont la réparation nous a coûté 100 millions de dollars et qui nous a fait perdre 40 000 fichiers. Dans l'étude n^{o} 6, l'attaque d'un acteur parrainé par un État sur le ministère de la Défense nationale, qui a réussi à voler des sommes importantes au ministère en question. Dans l'étude n^{o} 6, peut-être la plus inquiétante, on découvre qu'en 2020, un État a compromis le réseau d'une société d'État et d'un ministère, ou comme nous le supposons, de plusieurs ministères.

Nous avons fait ce rapport pour que le gouvernement du Canada et ceux qui sont en première ligne pour prendre ce genre de décisions au Conseil du Trésor, ou encore les directeurs informatiques des différents ministères ou des sociétés d'État

buying shrinkwrapped technology off the shelf and trying to deal with this unbelievably sophisticated threat may not be your best approach.

That's why we gave lift to these six case studies, to say you might just see yourself in here as a government department or an organization. We hope that would have helped to grab their attention immediately, but as Senator Lankin said earlier, I think the fact that you're looking at this, you have an incredible voice and a role here, an opportunity to bring TBS, the Treasury Board Secretariat in here and shared services and CSE again to say, okay, well, where are we, how fast can you implement this? What is at risk?

Senator Yussuff: Security is not just in the federal domain. Private sector companies are responsible for information, and a lot of data we share. But provinces and municipalities are equally vulnerable, because they manage the infrastructure of this country. So in the absence of knowing what is going on in the country, we have no national legislation that anybody would have to reveal a cyber attack. Canadians know because it's in the media, or your Rogers phone went out of service because the transfer of information or whatever didn't happen.

To seek your opinion, do you think it's desirable for us to have legislation that this information should be shared because if we're not aware of the volatility and the challenges we're faced with, how do we as a country come together to figure out how we're going to better work together?

And the second one, private companies, of course, are private companies, but they have an obligation to the public to tell us things that we should have a database in place, and we should know, because that should reveal, despite their best effort, that they're still vulnerable. Because if some of these companies shut down, it could have major impacts on what we do, and many are integral to the economy, to a large extent. If we don't know that, how do we protect the economy?

Senator Lankin: I think the point you've raised and it follows on Senator Gignac's point is important.

The answer of how we go about it is not something our committee has discussed, and so I won't speak on behalf of the committee in any way with respect to that. But, we do note, not just in this report, but in our general review, framework reviews, and a couple of the activity reviews, we do note ourselves in our

puissent comprendre qu'ils pourraient être les prochains à être touchés. Ils pourraient être les prochains. Nous avons aussi pointé du doigt le fait que l'achat d'outils technologiques standardisés pour faire face à cette menace incroyablement sophistiquée n'est peut-être pas la meilleure solution.

C'est la raison pour laquelle nous avons présenté ces six études de cas, pour montrer que chaque ministère ou organisation pouvait se retrouver dans cette situation. Nous espérons que cela aurait permis de frapper les esprits, mais comme la sénatrice Lankin l'a dit plus tôt, je pense que vous avez une voix et un rôle incroyables à jouer, l'occasion de faire intervenir le Secrétariat du Conseil du Trésor, les Services partagés et le Centre de la sécurité des télécommunications pour leur demander où ils en sont, quand ils pourront mettre cela en œuvre et quels sont les risques.

Le sénateur Yussuff : La sécurité n'est pas l'apanage du gouvernement fédéral. Les entreprises du secteur privé sont responsables des renseignements qu'elles possèdent et d'un grand nombre de données qu'elles échangent. Les provinces et les municipalités sont tout aussi vulnérables, car elles gèrent l'infrastructure du pays. Par conséquent, si nous ne savons pas ce qui se passe dans le pays, nous ne pouvons pas nous appuyer sur une législation nationale pour révéler une cyberattaque. Les Canadiens le savent parce que les médias en parlent, ou que leur téléphone Rogers est tombé en panne parce que le transfert de données ou autre a échoué.

À votre avis, est-il souhaitable que nous disposions d'une législation prévoyant le partage de ces données? Car si nous ne sommes pas conscients de la précarité et des défis auxquels nous sommes confrontés, comment pouvons-nous, en tant que pays, nous rassembler pour réfléchir à la manière dont nous pourrions mieux travailler ensemble?

Deuxièmement, les entreprises privées sont bien entendu des entreprises privées, mais elles ont l'obligation d'informer le public, de nous dire ce qu'il y a dans leur base de données, ce que nous devrions savoir, mais cela devrait montrer que, malgré tous leurs efforts, elles sont toujours vulnérables. Si certaines de ces entreprises venaient à fermer, cela pourrait avoir des conséquences majeures sur nos activités. En effet, nombre d'entre elles font partie intégrante de l'économie, dans une large mesure. Comment pouvons-nous protéger l'économie si nous ne savons pas ce qui se passe?

La sénatrice Lankin : Je pense que le point que vous avez soulevé et qui découle de la remarque du sénateur Gignac est important.

Le comité ne s'est pas penché sur la question de savoir comment s'y prendre, et je ne parlerai donc pas au nom du comité à ce sujet. Toutefois, lors de nos échanges, nous constatons, non seulement dans ce rapport, mais aussi dans notre examen général, dans nos examens du cadre et dans certains

conversations that this is a significant problem in terms of the lack of coordination.

I sat for a while on the board of Hydro One and there I learned about the coordination of a North American grid, the kind of security concerns for critical infrastructure. This committee in 2016 or 2017 or so, did a report, that is almost quaint now, about pulse technology that could wipe out our communications systems. There are much more effective and advanced ways at this point in time, but those things are still real issues, and I think that those are questions that should be explored and to what extent we could do that.

I would just make two comments, through legislative changes, CSE — as I said before — and CSIS were enabled to do community outreach, which they had been beginning to practise, but it was not clear what the legal foundation for this was. A bill then went through the House of Commons and the Senate, was passed and changed that — it provided an enabling process there for them. CSE has been proactive in reaching out, but all of those things are constrained by what I said in terms of the, one, resources, which is always going to be a case, but, two, the nature of some of the information.

I think that the question you raised should be given a thorough airing and debate. I won't comment on my own personal opinions about it, but I am concerned about critical infrastructure. If we can get that one in there again.

Senator Cardozo: Thank you very much for being here. I have a general question, and you can answer to the extent that you can, understanding that you operate with a lot of confidentiality. I think it probably intrigues a lot of Canadians as to how a committee like yours works, given that you come from different partisan backgrounds, the House of Commons, and the Senate. To the extent that you can, can you give us a sense of how you operate when people come to the table with different agendas? Is it somewhat like a committee, a House of Commons committee would work or Senate committee where people put their priorities first and you try and figure out what those priorities are, and then if you have time, if you can just share with us a little more thoughts about why some of these agencies and departments are reluctant to come under the umbrella?

Mr. McGuinty: I think the highest compliment the committee has likely ever received was from officials who had appeared, and their feedback to us was, if you close your eyes and listen to the voice of the speaker, you have no idea from which political persuasion it was coming.

examens des activités, que le manque de coordination constitue un problème important.

J'ai siégé pendant un certain temps au conseil d'administration de Hydro One et j'y ai appris ce qu'était la coordination pour gérer un réseau nord-américain, ainsi que les problèmes de sécurité pour les infrastructures essentielles. En 2016 ou 2017, le comité a publié un rapport, presque désuet aujourd'hui, sur la technologie des impulsions qui pourrait anéantir nos réseaux de communication. Il existe aujourd'hui des moyens beaucoup plus efficaces et avancés, alors ces questions restent d'actualité, et je pense qu'il convient de les étudier et de déterminer dans quelle mesure nous pourrions nous protéger.

Je voudrais juste faire deux observations. Comme je l'ai déjà dit, grâce aux modifications législatives, le Centre de la sécurité des télécommunications et le Service canadien du renseignement de sécurité ont été autorisés à mener des activités de sensibilisation auprès des collectivités. Ils avaient commencé à le faire, mais la base juridique de ces activités n'était pas clairement établie. Un projet de loi a alors été soumis à la Chambre des communes et au Sénat, puis adopté, et cela leur a permis de mener ces activités. Le Centre de la sécurité des télécommunications s'est montré proactif dans ses échanges, mais tous ces efforts sont limités non seulement par le manque de ressources — ce qui sera toujours le cas — mais aussi par la nature de certaines informations.

Je pense que la question que vous avez soulevée devrait faire l'objet d'un examen et d'un débat de fond. Je n'exprimerai pas mon opinion personnelle à ce sujet, mais je suis préoccupée par les infrastructures essentielles, si je puis me permettre de le répéter.

Le sénateur Cardozo : Je vous remercie de votre présence. J'ai une question d'ordre général, et vous pouvez y répondre au mieux, étant donné que vous travaillez dans la plus grande confidentialité. Je pense que beaucoup de Canadiens s'interrogent sur le fonctionnement d'un comité comme le vôtre, compte tenu du fait que vous venez de différents partis, de la Chambre des communes et du Sénat. Dans la mesure du possible, pouvez-vous nous donner une idée de votre mode de fonctionnement lorsque des personnes ont des intérêts différents? Est-ce que vous fonctionnez un peu comme un comité classique de la Chambre des communes ou du Sénat, où chacun met en avant ses priorités et où il faut essayer de les comprendre? Puis, si vous avez le temps de répondre, pourriez-vous nous expliquer pourquoi certains organismes et certains ministères sont réticents à l'idée de se placer dans le périmètre de protection du Centre de la sécurité des télécommunications?

M. McGuinty : Je pense que le plus grand compliment que le comité ait jamais reçu vient de hauts fonctionnaires qui ont comparu et qui nous ont dit : « Si on ferme les yeux et qu'on écoute la voix du président, on n'a aucune idée de son orientation politique. »

I think we've found a way to work together in a non-partisan, consensual way where we treat national security and intelligence the way we believe it ought to be treated. We remove it from the immediate cut and thrust of the arena. Those of us who have been involved in elected life know all about the cut and thrust of the arena. These issues transcend any party or government, and we're certainly seeing that right now with some of the concerns Canadians are expressing around this discussion on foreign interference.

We work in a very consensual way. Our reports are pored over and deliberated at length — sentence by sentence, paragraph by paragraph, finding by finding and recommendation by recommendation. If we can't get agreement, we go back and do it again.

I will say that in six years of practice, we have never once had to vote on anything. It's important for Canadians and senators to know that the government does not have a majority on the committee. It was designed not to have one. It's more a question of, we think, putting the purpose and importance of the issues front and centre in order to try to make recommendations for change to improve the situation.

It's not easy. We're trying something new. It's never been done before in this country. We seem to be making progress. We also generally don't enter into the fray of cut-and-thrust political debate. We communicate when we have something to communicate. Today we think we have something to communicate. When we complete our next review on foreign interference, we'll have something to communicate. We remain disciplined. We're dealing with highly sensitive materials, so we have to remain disciplined.

That's sort of how we work. We choose subjects using different metrics: Has it ever been examined before? Is it of interest to Canadians? How important is it? Is it public? We can take referred matters. The Prime Minister or a minister can refer matters to us. It doesn't mean we're bound by it. We can take it under advisement, we can decline or we can accept.

The committee is very much independent. If it wants more information, it goes back and asks for more information. There's never a shortage of information, by the way. There are 25,000 to 50,000 pages of documentation per review, so it's a heavy load.

There's no delegation. You can't substitute an outstanding senator like Francis Lankin. You couldn't do it anyway, but the point being that Senator Lankin can't turn to somebody else and say, "Can you pinch-hit for me today?" There's a reason why the members are cleared to a very high level, sign an oath and wave away the parliamentary privilege — because of the nature of the

Je pense que nous avons trouvé un moyen de travailler ensemble de manière non partisane et consensuelle, pour traiter la sécurité nationale et le renseignement comme nous estimons qu'ils doivent l'être. Nous mettons de côté les batailles de clocher. Ceux d'entre nous qui ont été impliqués dans la vie politique manient fort bien la joute oratoire. Cependant, ces questions transcendent les partis et les gouvernements, comme en témoignent les inquiétudes exprimées par les Canadiens dans le cadre du débat sur l'ingérence étrangère.

Nous travaillons de manière très consensuelle. Nous examinons et discutons longuement des rapports, phrase par phrase, paragraphe par paragraphe, constatation par constatation et recommandation par recommandation. Si nous ne parvenons pas à nous mettre d'accord, nous recommençons.

Je peux dire qu'en six ans d'existence, nous n'avons jamais eu à procéder à un vote. Il est important que les Canadiens et les sénateurs sachent que le gouvernement n'a pas de majorité au sein du comité. Il a été conçu pour ne pas en avoir. Le but est plutôt, selon nous, de mettre en avant l'objectif et l'importance de ces questions afin d'essayer de formuler des recommandations pour améliorer la situation.

Ce n'est pas facile. Nous expérimentons quelque chose de nouveau. Cela n'a jamais été fait auparavant dans ce pays. Nous avons l'impression de faire des progrès. En général, nous ne nous lançons pas dans des débats politiques à l'emporte-pièce. Nous nous exprimons quand nous avons quelque chose à dire. Aujourd'hui, nous estimons avoir quelque chose à dire. Lorsque nous aurons terminé notre prochain examen de l'ingérence étrangère, nous aurons quelque chose à dire. Nous restons disciplinés. Nous traitons des documents très sensibles, alors il faut rester discipliné.

C'est en quelque sorte notre façon de travailler. Nous choisissons les sujets en fonction de différents critères. La question a-t-elle déjà été étudiée? Présente-t-elle un intérêt pour les Canadiens? Quelle est son importance? Cette question est-elle publique? Nous pouvons aussi traiter des questions qu'on nous soumet. Le premier ministre ou un ministre peut nous soumettre des questions. Cela ne signifie pas que nous sommes tenus de les traiter. Nous pouvons les prendre en considération, les refuser ou les accepter.

Le comité est très indépendant. S'il a besoin de plus d'informations, il les demande à nouveau. Les informations ne manquent jamais, d'ailleurs. Il y a entre 25 000 et 50 000 pages de documents par examen, ce qui représente une énorme charge de travail.

Il est impossible de déléguer le travail. On ne peut pas remplacer une sénatrice exceptionnelle comme Frances Lankin. De toute façon, ce serait impossible, mais le fait est que la sénatrice Lankin ne peut pas demander à quelqu'un de la remplacer. Ce n'est pas pour rien que les membres du comité ont une cote de sécurité très élevée, qu'ils signent un serment et

work that goes on here. It's serious business, and we try to rise up to meet that challenge for Canadians.

Senator Lankin: I think it's important to know that our chair went through some of the criteria. We also take a look at the way in which these issues implicate Charter rights for Canadians. We look at the issues of sovereignty and integrity of our institutions and the economic and societal impacts. We bring forward the departments — sometimes individually and sometimes we've had grand presentations that are across departments. We reach outside of government as well for comment, whether it's academics or people from particular NGOs who have expertise in a subject, on what the impact is on Canadians. That's part of our mandate as well.

Within the legislation, there are two types: a framework review and an activity review. All of that has to relate back to why we're doing this, which is for the Canadian public. In our reports, we try to speak in a way that can communicate to the Canadian public. As the chair said, we try to be as transparent as possible, except for those areas that are actually dictated in the legislation as exceptions and that, therefore, must be redacted.

Senator Dasko: Thank you, witnesses, for being here. I want to pursue the topic of the kind of information that the committee is entitled to receive and the granularity of the information.

You receive information briefings from departments, from the CSE and other sources, but how entitled are you to ask for information that is really granular, that has to do, let's say, with individuals or specific situations that might even go beyond the case studies that you have in your report?

Mr. McGuinty, since you used the term "foreign interference," I'm going to pick up on that.

Mr. McGuinty: I opened the door, did I?

Senator Dasko: You opened the door, just in time for me to ask you to pursue that topic in terms of, again, the granularity of the information.

Can you ask for information about individuals who may have been targets of attacks, or situations, notwithstanding the fact that departments are blocking some of the information you're looking for, as you said earlier? Notwithstanding that, what are you entitled to receive? How far down can you go? How extensive is the information you can request and hope to receive?

qu'ils renoncent au privilège parlementaire — c'est à cause de la nature de notre travail. Il s'agit d'une mission sérieuse, et nous nous efforçons de relever ce défi pour les Canadiens.

La sénatrice Lankin : Je crois qu'il est important de savoir que notre président a passé en revue certains critères. Nous examinons également la manière dont ces questions impliquent les droits des Canadiens garantis par la Charte. Nous examinons les questions de souveraineté et d'intégrité de nos institutions, ainsi que les incidences économiques et sociétales. Nous faisons appel aux ministères, parfois de façon individuelle, parfois pour de grands exposés transministériels. Nous faisons également appel à des intervenants en dehors du gouvernement, que ce soit des universitaires ou des gens œuvrant pour des ONG qui ont une certaine expertise, afin de connaître les incidences d'un enjeu précis sur les Canadiens. Cela fait également partie de notre mandat.

La loi prévoit deux types d'examens: un examen du cadre réglementaire et un examen des activités. Tout cela doit être relié à la raison pour laquelle nous faisons ce travail, c'est-à-dire les Canadiens. Dans nos rapports, nous tentons d'être vernaculaires avec la population. Comme le président l'a dit, nous tentons d'être aussi transparents que possible. Cela dit, nous n'avons bien sûr pas le choix de caviarder certaines informations en raison des exceptions prévues dans la loi.

La sénatrice Dasko : J'aimerais remercier les témoins d'être parmi nous. J'aimerais poursuivre sur le sujet du type d'informations que le comité est en droit de recevoir et de la granularité de ces informations.

Vous assistez à des séances d'information offertes par des ministères, par le CST et d'autres, mais à quel point pouvez-vous demander des détails? Pouvez-vous demander des informations sur des personnes ou des situations précises qui pourraient même aller au-delà des études de cas comprises dans votre rapport?

Monsieur McGuinty, je reprends votre terme d'« ingérence étrangère ».

M. McGuinty : J'ai ouvert la porte, n'est-ce pas?

La sénatrice Dasko : Oui, et juste à temps pour ma question sur la granularité de l'information.

Pouvez-vous demander des informations sur des personnes susceptibles d'avoir été la cible d'attaques ou sur des situations précises, malgré le fait que les ministères vous empêchent d'avoir accès à toute l'information que vous recherchez, comme vous l'avez dit plus tôt? Qu'avez-vous le droit de recevoir malgré tout cela? Jusqu'où pouvez-vous aller? Quelle est l'étendue des informations que vous pouvez demander et espérer recevoir?

Mr. McGuinty: The first thing to remember is that we're a review committee, not an oversight committee, so there are some restrictions with regard to the kinds of information we can request. For example, we can't ask for details on ongoing investigations.

If I can ask Lisa-Marie Inman to answer you with regard to the granularity. She's perhaps best placed because she's often negotiating and following through with the information owners.

Lisa-Marie Inman, Executive Director, Secretariat of the National Security and Intelligence Committee of Parliamentarians: Thank you very much for the question. In terms of granularity, there's no limit to the degree of granularity we can seek in our requests for information. Of course, there is certain information that we're not entitled to — notably, information about an ongoing investigation, law enforcement investigations that may result in prosecution, human source information, Witness Protection Program information and cabinet confidence.

As to the granularity, it can be any information at all that is relevant to our review. We regularly see very granular information.

I will make the point, though, that often we will get information about individuals, but the committee doesn't have an individual complaint mandate. Folks can't come to the committee to complain about their particular situation, so there won't be a lot of occasions where we would look into, say, someone's individual case. There are other mechanisms for that.

We have raised some challenges to getting particular types of information. Cabinet confidence was the one thing that the chair highlighted. Generally speaking, and particularly over the five years that the committee has existed, we have found that departments and agencies have evolved a fair bit. There's now a relationship of trust with the security and intelligence community. I don't want to speak for them, but they are confident that the committee can take appropriate measures to safeguard their information. They're generally forthcoming and cooperative in the information that they provide.

Other than the specific instances that the chair described where we have had issues, getting information is generally a fairly seamless process. As the chair said, we'll often get information, look at it, and realize that something is referred to in this or that document that we don't have before us, so it's an

M. McGuinty : Retenez tout d'abord une chose : nous ne sommes pas un comité de surveillance, mais plutôt un comité d'examen, alors nous devons nous plier à certaines restrictions quant au type d'informations que nous pouvons demander. Par exemple, nous ne pouvons pas demander de détails sur des enquêtes en cours.

Si vous me le permettez, je demanderais à Mme Inman de vous parler de la granularité de l'information. Elle est probablement la mieux placée pour vous en parler, puisqu'elle participe souvent aux négociations et aux suivis avec les détenteurs d'informations.

Lisa-Marie Inman, directrice générale, Secrétariat du Comité des parlementaires sur la sécurité nationale et le renseignement : Je vous remercie de la question. Il n'existe aucune limite quant au degré de granularité que nous pouvons rechercher dans nos demandes d'information. Bien sûr, nous n'avons pas le droit d'obtenir certaines informations. Par exemple, nous ne pouvons pas obtenir des informations sur des enquêtes en cours ou sur des enquêtes policières en cours susceptibles de mener à des poursuites, des informations provenant de sources humaines, des informations relatives au programme de protection des témoins ou encore de l'information confidentielle du Cabinet.

En ce qui concerne la granularité, nous pouvons demander toute information que nous estimons pertinente pour notre examen. Nous recevons régulièrement des informations très détaillées.

Je tiens cependant à préciser une chose. Certes, nous recevons souvent des informations sur des personnes précises, mais notre comité n'a pas de mandat en matière de plainte individuelle. Les gens ne peuvent pas venir à notre comité pour se plaindre d'une situation personnelle, alors nous nous attardons rarement à des cas individuels. Il existe d'autres mécanismes pour ce genre de cas.

Nous avons relevé certaines difficultés dans le processus d'obtention d'informations. Le président a parlé des informations confidentielles du Cabinet. De façon générale, nous avons constaté une belle évolution au sein des ministères et des agences, et particulièrement au cours des cinq dernières années, soit depuis que notre comité existe. Il existe désormais une relation de confiance avec la communauté de la sécurité et du renseignement. Je ne veux pas parler pour eux, mais je dirais qu'ils nous font confiance. Ils savent que nous prendrons les mesures appropriées pour protéger leurs informations. Ils font habituellement preuve d'ouverture et de coopération lorsqu'ils nous transmettent des informations.

Le président a relevé des défis précis, mais nous n'avons habituellement pas de difficulté à obtenir des informations. Comme l'a dit le président, souvent, nous recevons des informations, nous les examinons, et nous réalisons que tel ou tel document fait référence à d'autres informations que nous

iterative process of asking for information. We'll often get information and then ask for more information several times up until the end of a review.

Senator Dasko: At the same time, you're getting blocked in some of the requests you're getting. That is what I understood from the remarks that the departments are resisting or refusing information.

Mr. McGuinty: Senator, only in certain cases. We don't want to overstate that case. It's generally very good. We've cultivated a strong relationship.

In some cases — for example, after performing the DND/Canadian Armed Forces review of their security and intelligence activities — it actually helped lead to the creation of a review office inside the department to be able to start sharing information with us in a forthcoming way in the future, or with NSIRA, the National Security and Intelligence Review Agency, or some other group.

We don't want to overstate the case. There have been a couple of instances where we've been very firm about information, and we're working our way through that. We don't expect to face many of those; to be honest, I don't think we expect to face that very often in the future.

Senator Boehm: I'd like to thank the witnesses for being here. It's great to have Senator Lankin back with us, even in a witness capacity.

I have a number of questions. I think I'll just put them all out, recognizing we have only a few minutes and that I don't think we're going to have much of a round two.

Mr. McGuinty, you mentioned the cyberdefence perimeter a number of times. I think that when most people think about a perimeter, they think of a fence. I know you're referring to something that is much more elastic.

Canada has over 150 offices abroad whether embassies, consulates or offices at embassies and the like. The provinces also have some offices abroad as well. When you speak about the cyberdefence perimeter and, perhaps, its weakest link, it's conceivable that the weakest link could be far away from our shores, and we would have to have the electronic cyber protection to ensure that. That's one question, I would like your thoughts on that.

The other is this: I know yours is a review committee. Other parliaments among the Five Eyes have similar sorts of committees. Is there any back and forth or discussion on best

n'avons pas. Nous devons donc continuellement demander des informations. Bien souvent, nous recevons et demandons des informations à multiples reprises jusqu'à la fin de notre examen.

La sénatrice Dasko : Cela dit, vous essuyez parfois des refus. C'est ce que j'ai compris en vous écoutant. Les ministères résistent ou refusent de vous envoyer des informations.

M. McGuinty : Seulement dans certains cas, sénatrice. Nous ne voulons pas exagérer la chose. Tout se passe généralement très bien. Nous avons bâti une bonne relation.

Dans certains cas — après l'examen des activités de sécurité et de renseignement du ministère de la Défense nationale et des Forces armées canadiennes, par exemple — cela a mené à la création d'un bureau d'examen au sein du ministère afin qu'il puisse commencer à partager des informations ouvertement avec nous à l'avenir, ou avec l'Office de surveillance des activités en matière de sécurité nationale et de renseignement — l'OSSNR — ou un autre groupe.

Nous ne voulons pas exagérer la chose. Il y a eu quelques cas où nous tenions mordicus à certaines informations, et nous y travaillons. Nous ne nous attendons pas à faire face à de tels obstacles fréquemment à l'avenir, pour être franc.

Le sénateur Boehm : J'aimerais remercier les témoins d'être ici. Je suis heureux de vous revoir parmi nous, sénatrice Lankin, même si c'est à titre de témoin.

J'ai quelques questions à vous poser. Je crois que je vais toutes les poser d'un coup, étant donné qu'il ne nous reste que quelques minutes. Je ne crois pas que nous aurons vraiment un deuxième tour de questions.

Monsieur McGuinty, vous avez parlé du périmètre de cyberdéfense à quelques reprises. Je pense que la plupart du temps, quand on pense à un périmètre, on s'imagine une clôture. Or, je sais que vous faites référence à quelque chose de nettement plus élastique.

Le Canada dispose de 150 bureaux à l'étranger, que ce soit des ambassades, des consulats, des bureaux dans des ambassades, ou autre. Les provinces disposent également de bureaux à l'étranger. Lorsque vous parlez du périmètre de cyberdéfense, et peut-être, de son maillon le plus faible, il est concevable que le maillon le plus faible puisse se situer loin de nos côtes, et qu'il nous faille donc disposer de la cyberprotection électronique nécessaire pour le protéger. Voilà ma première question. J'aimerais vous entendre à ce sujet.

J'ai une autre question. Je sais que votre comité est un comité d'examen. Ce genre de comité existe dans d'autres parlements du Groupe des cinq. Discutez-vous entre vous des pratiques

practices, since the NSICOP has been operating for some time? Are the reports shared? Do you get inputs — that sort of thing?

My last question is really to you. As a parliamentarian, you know well how many meeting requests we receive from embassies and from lobbyists. As chair of this particular review committee, do you feel you're getting attention yourself, and if so, how would you handle it?

Mr. McGuinty: I'm not sure what kind of attention you mean.

Senator Boehm: Popularity. Sponsor [Technical difficulties].

Mr. McGuinty: I'll start with the last question first.

Maybe. I think that all members have found we've had to govern ourselves a bit differently now that we sit on this committee in terms of meetings and attending diplomatic settings. As a general rule, I don't anymore. I tend to be very careful. Or if I'm travelling, I'm very careful and so on and so forth. I think most of us have been briefed and briefed yet again about those risks.

On the question of how we share information, how we conduct our practice and whether there are other groups: Yes, we have liaised with the intelligence and security committee in the U.K. Ms. Inman led a delegation there just last January and had a week of meetings. We have had the Intelligence and Security Committee of Parliament, or ISC, members from Britain here to Canada previously. We're hoping to get to Britain at some point. They have a longer tradition in that practice and approach. We've learned a lot from them. We've met with the New Zealanders, Australia and some U.S. counterparts. We've also had many overtures from other countries in the world, asking how we're doing this — Romania, Israel, South Africa. They ask us to share our know-how in terms of what we're doing here because they're looking for models that might be appropriate for them. So we're finding our way forward.

On your first question, I'm going to ask Nabil Bhatia to talk about the details of the technical side of this.

Nabil Bhatia, Review Analyst, Secretariat of the National Security and Intelligence Committee of Parliamentarians: Thank you very much for your question, Senator Boehm.

When we're speaking about the cyberdefence perimeter, we're speaking about three tools operated by the CSE, and we outline these tools from paragraphs 188 to 202 in our report. I understand that not long ago, you spoke to Mr. Khoury and

exemplaires, étant donné que le CPSNR existe depuis un certain nombre d'années? Vous envoyez-vous vos rapports? Vous font-ils part de leurs réflexions, par exemple?

Ma dernière question s'adresse précisément à vous. À titre de parlementaire, vous savez très bien à quel point nous recevons des demandes de réunion des ambassades et de lobbyistes. À titre de président de ce comité d'examen, sentez-vous qu'on vous interpelle personnellement? Si oui, comment réagissez-vous à cela?

M. McGuinty : Je ne suis pas certain de saisir ce que vous voulez dire par là.

Le sénateur Boehm : Je parle de popularité, de parrainage. [Difficultés techniques]

M. McGuinty : Je vais commencer par la dernière question.

Oui, peut-être. Je crois que nous avons tous dû modifier un peu notre comportement dans les réunions et lors d'événements diplomatiques depuis que nous siégeons au sein de ce comité. Je n'ai plus à le faire, de façon générale. Je tends à être très prudent. Je fais preuve d'une grande prudence lorsque je voyage, par exemple. Je crois que la plupart d'entre nous ont été informés des risques à maintes reprises.

En ce qui concerne la transmission d'informations, nos pratiques et les autres groupes, oui, nous communiquons avec le comité de sécurité et de renseignement du Royaume-Uni. Mme Inman était à la tête d'une délégation là-bas en janvier dernier et a participé à une semaine de réunions. Les membres de ce comité sont déjà venus au Canada. Nous espérons aller en Grande-Bretagne un de ces jours. Les Britanniques ont plus d'expérience avec ce type de pratique et d'approche. Ils nous ont beaucoup appris. Nous avons également rencontré nos homologues néo-zélandais, australiens et certains de nos homologues américains. De plus, nombre d'autres nations sont entrées en contact avec nous pour nous demander de leur expliquer notre méthode de travail, dont la Roumanie, Israël et l'Afrique du Sud. Ces pays nous ont demandé de leur faire part de notre savoir et de notre travail, parce qu'ils sont à la recherche de modèles qui pourraient leur convenir. Nous sommes donc en train de trouver notre voie.

Pour en revenir à votre première question, je demanderai à M. Bhatia de vous parler des détails techniques.

Nabil Bhatia, analyste de révision, Secrétariat du Comité des parlementaires sur la sécurité nationale et le renseignement : Je vous remercie de la question, sénateur Boehm.

Lorsque nous parlons du périmètre de cyberdéfense, nous faisons référence aux trois outils du CST, que nous présentons dans les paragraphes 188 à 202 dans notre rapport. J'ai cru comprendre que vous avez récemment parlé à M. Khoury et

Mr. Couillard from the Canadian Centre for Cyber Security, so they can speak to this with much authority.

The three types of sensors employed by CSE are network-based sensors, host-based sensors and cloud-based sensors. These three sensors work together at the network level, at the host level — which is on actual end-point devices — and at the cloud level to complement commercially available measures such as firewalls and anti-viruses. They serve two purposes. On the one hand, they identify malicious cyber activity, and on the other hand, they proactively defend networks against cyberattack. Sensors constantly monitor for anomalous cyber activity and analyze that activity to identify new, malicious cyber behaviour. CSE then uses this information to mitigate threats in the present and plan for threats in the future.

Senator Boehm: Thank you very much.

[*Translation*]

Senator Boisvenu: Welcome, Senator Lankin, Mr. McGuinty and Ms. Inman. It's a pleasure to see you again.

You know we're doing a study on Arctic security. I discovered — I can't speak for my colleagues — that if it weren't for the U.S. presence through North American Aerospace Defence Command (NORAD), Canada would be poorly positioned in terms of its national security, particularly with respect to that neighbour to the north, Russia. The Americans are safeguarding a substantial portion of Canada's security.

Preliminary findings also indicated that military equipment and personnel are in a sorry state. We're really lagging in terms of modernization and value for money in the Canadian Armed Forces.

In your 2022 report, you talked about government cyber defence. Theft of information in military operations could lead to the unveiling of strategies, and so on. That's an important aspect of our study.

In terms of providing input to the government on improving this situation, how do you address the lack of equipment in the military and the management of an issue as important as cyberattacks? There seems to be a contradiction between the lack of resources and equipment and the need to counter these cyberattacks. Resources and equipment are needed.

M. Couillard du Centre canadien pour la cybersécurité. Ils pourraient vous en parler en toute connaissance de cause.

Le CST utilise trois types de capteurs : des capteurs réseau, des capteurs sur l'hôte et des capteurs infonuagiques. Ces trois capteurs travaillent ensemble au niveau du réseau, au niveau de l'hôte — soit sur des systèmes d'accès terminaux — et au niveau infonuagique et constituent un complément aux mécanismes commerciaux disponibles comme les logiciels antivirus ou les pare-feu. Ils ont deux rôles. Ils servent à la fois à relever les cyberactivités malveillantes et à défendre de façon proactive les réseaux contre les cyberattaques. Les capteurs surveillent constamment les cyberactivités anormales et les analysent afin de relever de nouveaux comportements cybernétiques malveillants. Le CST utilise ensuite ces informations pour atténuer les menaces actuelles et préparer les plans d'intervention pour les menaces futures.

Le sénateur Boehm : Merci beaucoup.

[*Français*]

Le sénateur Boisvenu : Bienvenue, sénatrice Lankin, monsieur McGuinty et madame Inman. Cela me fait plaisir de vous revoir.

Vous savez que nous menons une étude sur la sécurité en Arctique et ce que j'ai découvert — je ne peux pas parler au nom de mes collègues — est que si ce n'était de la présence américaine au moyen du Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD), le Canada serait en mauvaise posture en matière de sécurité nationale, notamment en ce qui a trait à ce voisin du Nord, la Russie. Les Américains assurent une grande part de la sécurité du Canada.

On a également fait des constats préliminaires, à savoir que les équipements et le personnel des forces armées sont dans un piteux état. On est vraiment en retard quant à la modernisation et l'optimisation des ressources dans les Forces armées canadiennes.

Dans votre rapport de 2022, vous avez parlé de la cyberdéfense du gouvernement. Le vol d'informations dans les opérations militaires pourrait mener au dévoilement de stratégies, et ainsi de suite. C'est un volet important de notre étude.

En ce qui a trait à l'apport au gouvernement pour améliorer cette situation, comment faites-vous pour pallier le manque d'équipement dans les forces armées et la gestion d'un dossier aussi important que les cyberattaques? Il semble y avoir une contradiction entre le manque de ressources et d'équipement et le fait d'avoir à contrer ces cyberattaques. Il faut des ressources et des équipements.

What position do you take with the government regarding the huge disconnect between the current state of the military and the global monitoring of cyberattacks?

[*English*]

Senator Lankin: First of all, I think I'm correct in the words I'm using. DND monitors their own cybersecurity. It's a different organization and a different culture, and the imperatives are different. Their use of cybersecurity and monitoring has implications in the field on the front lines, so it's quite different.

About the issue of resources: I understand that this is something your committee may be looking at deeply. We didn't do a stand-alone review of DND with respect to cybersecurity, and we would include them in the general recommendation that all should be inside the same perimeter and that the resources of CSE should be more widely utilized. But the question you raised with respect to the resources available would entail us doing a framework review to look at the administrative, legislative, regulatory and financial administration pieces of this, which we have not done at this point in time.

Again, these are good questions. One of the things I was saying in addition to what the chair said earlier — about how we have criteria for what we review, how we make our decisions and how the committee works to come to those decisions — is that every time we do a review, by the end of it, we have thoughts about what we need to go back on in an appropriate manner of time, making sure it's review and not oversight. It's been seven years of learning. It's been seven years of learning for the government and departments who have never had this kind of interaction with parliamentarians before. While it took a while, I concur with the comments that we generally have excellent relationship — a trust-based relationship — and there has been a good exchange of information.

The question of DND and how that may be done warrants a review, whether it's by this committee or by the National Security and Intelligence Committee of Parliamentarians some time in the future. That would be helpful because those questions are important, in particular, I would say, with respect to the foreign interference file and the Arctic at this point in time.

[*Translation*]

Senator Boisvenu: Mr. McGuinty, you spoke at length about exchanges with other countries, including Australia and the United Kingdom. Did your findings about our partners point to any worthwhile approaches that Canada could build on to improve its performance on cyberattacks?

Quelle position défendez-vous auprès du gouvernement en ce qui a trait au décalage énorme entre la situation actuelle des forces armées et la surveillance du monde en matière de cyberattaques?

[*Traduction*]

La sénatrice Lankin : Tout d'abord, je crois utiliser les bons termes. Le ministère de la Défense nationale surveille sa propre cybersécurité. Il s'agit d'une organisation et d'une culture différentes, avec des obligations divergentes. Leur utilisation de la cybersécurité et de la surveillance se ressent sur le terrain en première ligne, alors la situation est très différente.

En ce qui concerne les ressources, j'ai cru comprendre que votre comité se penche sérieusement sur la question. Nous n'avons pas mené d'examen portant uniquement sur la cybersécurité au sein du ministère de la Défense nationale, et nous l'inclurions dans la recommandation générale, qui propose d'avoir un seul périmètre pour tous et d'utiliser davantage les ressources du CST. Cela dit, vous vouliez connaître les ressources disponibles. Pour vous répondre, il nous faudrait mener un examen du cadre afin d'étudier les aspects administratifs, législatifs, réglementaires et financiers de la question, ce que nous n'avons pas encore fait.

À nouveau, ce sont de bonnes questions. L'une des choses que j'ai dites plus tôt en complément de ce qu'a dit le président — sur nos critères d'examen et notre processus décisionnel — c'est que chaque fois que nous menons un examen, nous réfléchissons à ce sur quoi nous devrions revenir dans un délai approprié, en nous assurant de nous en tenir à un processus d'examen et non pas de surveillance. Nous avons appris des choses au cours des sept dernières années, tout comme le gouvernement et les ministères qui n'avaient jamais eu ce genre d'interactions avec des parlementaires avant. Je crois aussi que nous avons généralement une excellente relation avec eux basée sur la confiance. Certes, il a fallu un peu de temps pour la bâtir, mais le processus de transmission d'informations fonctionne bien.

Cela vaudrait la peine de réfléchir à la façon de mener un examen des activités du ministère de la Défense nationale un de ces jours, que ce soit au sein de votre comité ou du nôtre. Ce serait utile, parce qu'il s'agit de questions importantes. C'est particulièrement vrai pour l'ingérence étrangère et l'Arctique. Cela vaudrait la peine de s'y pencher à l'avenir.

[*Français*]

Le sénateur Boisvenu : Monsieur McGuinty, vous avez beaucoup parlé d'échanges avec les autres pays, notamment l'Australie et le Royaume-Uni. Vos constats au sujet de nos partenaires vous ont-ils indiqué des pistes intéressantes sur lesquelles le Canada pourrait s'appuyer pour améliorer sa performance en matière de cyberattaques?

Mr. McGuinty: We regularly obtain material, for instance, from the United Kingdom. Its committee has been active for decades. We share where we can, when we can. Obviously, we are unable to share confidential information. We learn from each other. There is a partnership, but we are different. Australia's committee structure is not the same as ours; it's not the same at all. In New Zealand, committees meet perhaps two or three times a year and the Prime Minister serves as chair.

It all depends on which country we're talking about. I think people are becoming more aware of the whole issue of cybersecurity risk and cyberattacks. I know that internationally, the United Nations is negotiating at least one and possibly two conventions that would address this issue.

[*English*]

The Chair: If you will indulge me for one more minute, I have a quick question to ask you, to add to those you have received.

You mentioned, chair, CSE engaging in "proactive defensive operations," I think is the term you used. Does that extend to measures that would degrade a known assailant's ability to attack our critical infrastructure?

Mr. McGuinty: Mr. Chair, I'm not sure if you're deliberately trying to be difficult or what here. I'd have to try to answer that question —

The Chair: I understand.

Mr. McGuinty: I'd have to go through this review a bit more carefully to answer it carefully for you.

The Chair: That's fine. That's great. Thank you.

This brings us to the end of the panel. I'd like to extend our thanks to you, Mr. McGuinty, to Senator Lankin, who we are delighted to see here with us, to Ms. Inman and Mr. Bhatia. We greatly appreciate the contributions and the time you've taken to share your experience with us. We thank you for your work on NSICOP. We know that is taken on in addition to your day jobs, to the other weighty responsibilities that you have. We're grateful for the work you all do, and I thank you on behalf of the committee, of the Senate of Canada and on behalf of Canadians. We wish you well in the important work that you will do in the future, so thank you very much.

(The committee continued in camera.)

M. McGuinty : On obtient régulièrement de la documentation, par exemple, du Royaume-Uni. Son comité est actif depuis des décennies. On partage où et comme on le peut. Évidemment, nous ne sommes pas en mesure de partager l'information confidentielle. Nous apprenons l'un de l'autre. Il existe un partenariat, mais nous sommes différents. La structure du comité de l'Australie n'est pas le même que le nôtre; ce n'est pas du tout la même chose. En Nouvelle-Zélande, on se réunit peut-être deux ou trois fois par année et la présidence est assumée par le premier ministre.

Tout dépend du pays dont on parle. Je crois que les gens sont de plus en plus conscients de cette question du cyberrisque et des cyberattaques. Je sais qu'à l'échelle internationale, les Nations unies sont en train de négocier au moins une et peut-être même deux conventions qui traiteraient de cette question.

[*Traduction*]

Le président : Si vous voulez bien m'accorder une autre minute, j'ai une brève question à vous poser, en complément de celles que vous avez reçues.

Vous avez dit, monsieur le président, que le CST se livre à des « opérations défensives proactives ». Je crois que c'est le terme que vous avez employé. Cela comprend-il les mesures qui réduiraient la capacité d'un agresseur connu à attaquer nos infrastructures essentielles?

M. McGuinty : Je ne sais pas si vous essayez délibérément d'être difficile ou autre, monsieur le président. Il faudrait que j'essaie de répondre à cette question...

Le président : Je comprends.

M. McGuinty : Il faudrait que j'étudie cet examen un peu plus attentivement pour vous donner une réponse précise.

Le président : D'accord, très bien. Merci.

Voilà qui met fin à la comparution de notre groupe de témoins. J'aimerais vous remercier, monsieur McGuinty, ainsi que vous, sénatrice Lankin, que nous sommes ravis d'avoir parmi nous, madame Inman et monsieur Bhatia. Nous vous sommes très reconnaissants de vos contributions et du temps que vous nous avez accordé pour nous faire part de votre expérience. Nous vous remercions de votre travail au sein du CPSNR. Nous savons que c'est une tâche qui se rajoute à votre travail quotidien et à vos lourdes responsabilités. Nous vous sommes reconnaissants de votre travail, et je vous remercie au nom de notre comité, du Sénat du Canada et des Canadiens. Nous vous souhaitons beaucoup de succès dans vos travaux futurs, qui sont importants. Merci beaucoup.

(La séance se poursuit à huis clos.)