CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

44e LÉGISLATURE, 1re SESSION

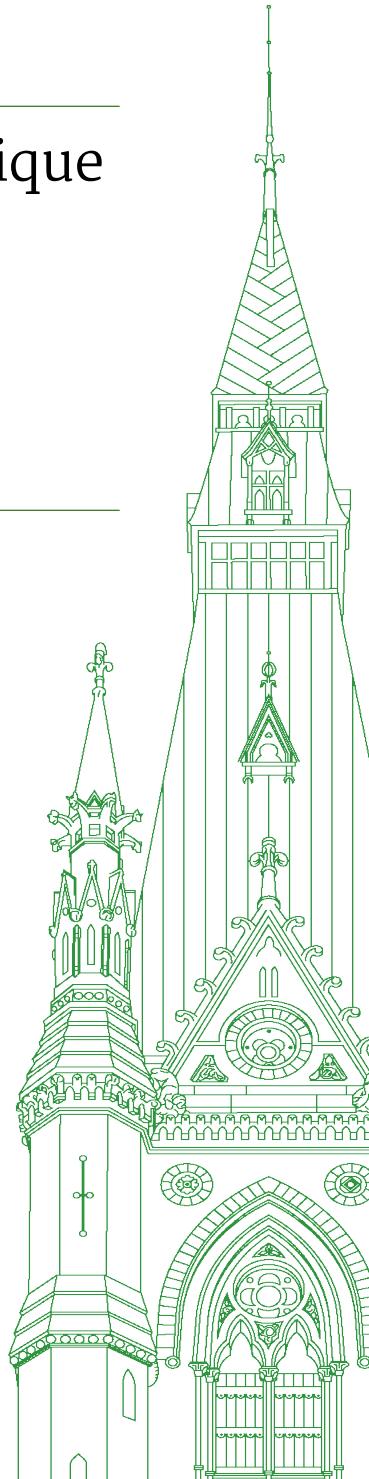
Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 029

PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY

Le jeudi 9 juin 2022



Président : L'honorable Jim Carr

Comité permanent de la sécurité publique et nationale

Le jeudi 9 juin 2022

● (1105)

[*Traduction*]

Le président (L'hon. Jim Carr (Winnipeg-Centre-Sud, Lib.)): Bonjour à tous. La séance est ouverte. Bienvenue à la 29e réunion du Comité permanent de la sécurité publique et nationale de la Chambre des communes.

Je tiens d'abord à souligner que je vous parle depuis le territoire visé par le Traité 1 et la patrie du peuple métis.

Conformément à l'ordre adopté par la Chambre le 25 novembre 2021, la séance d'aujourd'hui se déroule en format hybride, c'est-à-dire que des députés sont présents dans la salle alors que d'autres participent à distance au moyen de l'application Zoom.

En vertu du paragraphe 108(2) du Règlement et des motions adoptées par le Comité le jeudi 3 mars 2022, le Comité poursuit son évaluation de la posture de sécurité du Canada par rapport à la Russie.

Nous accueillons ce matin l'honorable Mario Mendicino, ministre de la Sécurité publique, qui est accompagné de représentants de l'Agence des services frontaliers du Canada, ou l'ASFC, du Service canadien du renseignement de sécurité, le SCRS, du ministère de la Sécurité publique et de la Protection civile et de la Gendarmerie royale du Canada.

Bienvenue à tous et à toutes.

J'invite maintenant le ministre Mendicino à nous présenter ses observations préliminaires.

L'hon. Marco Mendicino (ministre de la Sécurité publique): Merci beaucoup, monsieur le président.

Bonjour, chers collègues. Avant d'aller plus loin, j'aimerais vous présenter rapidement les gens qui sont avec moi pour répondre aux questions du Comité et lui transmettre l'information dont il a besoin. Il s'agit de MM. Denis Beaudoin et Michael Duheme de la GRC; de M. Rob Stewart, mon sous-ministre; de M. John Ossowski, président de l'Agence des services frontaliers du Canada; et de Mme Michèle Tessier du Service canadien du renseignement de sécurité.

Je suis ravi d'être des vôtres aujourd'hui pour la poursuite de votre évaluation de la posture de sécurité du Canada par rapport à la Russie. Je tiens à vous dire d'entrée de jeu à quel point je suis bouleversé, comme je sais que nous le sommes tous, par les événements qui ont cours en Ukraine. Il n'y a pas de mots pour bien décrire les horreurs de cette guerre qui sème la dévastation dans l'ensemble du pays et le désespoir de ceux qui sont toujours vivants et qui souffrent en raison de ces attaques brutales.

Le 4 mai dernier, j'ai eu le plaisir de rencontrer l'ambassadrice désignée de l'Ukraine au Canada, Mme Yulia Kovaliv, pour prêter une oreille attentive à ses préoccupations et voir comment le Canada pourrait appuyer encore davantage son pays. Nous avons aussi parlé de la nécessité de contrer les campagnes de désinformation et d'ingérence étrangère menées par la Russie. L'invasion illégale de l'Ukraine par la Russie aura de lourdes conséquences géopolitiques à long terme et met directement en péril l'ordre international fondé sur des règles.

Cette situation nous a rappelé que la communauté internationale est plus forte lorsqu'elle agit de concert pour défendre nos valeurs communes. Elle a aussi souligné le fait que nous ne sommes pas à l'abri des menaces à notre propre sécurité, ici même au Canada. Les activités hostiles d'acteurs étatiques étrangers comme la Russie peuvent entraîner des risques considérables pour notre sécurité nationale. Il s'agit notamment de cyberactivités malveillantes, y compris les cyberattaques; de menaces pour nos infrastructures essentielles, comme nos frontières, nos ponts et nos centrales électriques; de campagnes de mésinformation et de désinformation; d'espionnage; et d'ingérence étrangère.

[*Français*]

Le Canada prend toutes ces menaces très au sérieux, et le portefeuille de la Sécurité publique est bien équipé pour y faire face en temps de paix ou en temps de guerre, même si le volume de menaces et leur complexité ont augmenté au cours des dernières années. Au sein du portefeuille de la Sécurité publique, le SCRS, la GRC, l'ASFC et Sécurité publique Canada jouent tous un rôle important.

Le SCRS enquête sur les menaces, conseille le gouvernement et, au besoin, prend des mesures pour réduire les menaces à la sécurité du Canada.

La GRC est également un acteur important dans les efforts du Canada pour contrer les activités hostiles des acteurs étatiques. Elle enquête sur les infractions criminelles liées à l'ingérence étrangère ainsi que sur la cybercriminalité et sur les allégations de crimes de guerre.

[*Traduction*]

L'Agence des services frontaliers du Canada travaille sans relâche pour assurer la sécurité de nos frontières qui sont confrontées à un large éventail de menaces. Elle aide aussi le gouvernement à donner suite à son engagement d'offrir aux ressortissants ukrainiens admissibles l'accès à un processus d'immigration accéléré. L'ASFC jouera également un rôle clé dans l'application des mesures législatives que j'ai annoncées la semaine dernière pour empêcher l'entrée au Canada de Russes faisant l'objet de sanctions. Il n'est pas question d'offrir ici un refuge sûr à ces gens-là.

L'ASFC collabore étroitement avec le SCRS et d'autres partenaires pour effectuer des contrôles de sécurité et mobiliser des agents de liaison à l'étranger afin d'offrir le soutien nécessaire. L'ASFC et la GRC jouent un rôle important dans le cadre de mise en œuvre des sanctions pour veiller à ce que ceux qui se sont rendus complices de l'invasion russe aient des comptes à rendre.

Comme vous le savez très bien, le Canada a déjà imposé cette année des sanctions à 700 particuliers et entités, en plus d'adopter des mesures ciblant des biens et des secteurs en particulier, tout cela en étroite coordination avec la communauté internationale.

Monsieur le président, j'aimerais vous entretenir brièvement des moyens à notre disposition pour réagir à certaines menaces mettant en péril notre cybersécurité et nos infrastructures essentielles. Les cyberactivités malveillantes qui ciblent les systèmes assurant le bon fonctionnement de nos infrastructures essentielles sont pour nous une préoccupation de tous les instants. Elles ont des répercussions sur les entreprises, les Canadiens, notre économie et tous les ordres de gouvernement. Nous savons depuis longtemps que la Russie dispose de cybercapacités considérables, l'histoire nous ayant appris qu'elle n'hésite pas à les utiliser de façon irresponsable et sans se soucier des conséquences.

Sécurité publique Canada collabore avec d'autres ministères et agences du gouvernement ainsi qu'avec les alliés internationaux du Canada afin de dénoncer les États ou les acteurs parrainés par un État lorsqu'il est possible de leur attribuer en toute confiance la responsabilité d'une cyberactivité malveillante. Nous avons la chance d'avoir au Canada une Stratégie nationale de cybersécurité qui permet de protéger les Canadiens. Cette stratégie a déjà donné lieu à l'établissement du Centre canadien pour la cybersécurité, une instance unique faisant autorité pour offrir au Canada et aux Canadiens le soutien et les conseils techniques avisés dont ils ont besoin.

Le Centre diffuse des avis publics, notamment concernant la menace russe, et communique de précieuses informations sur les cybermenaces aux propriétaires et aux exploitants des infrastructures essentielles du Canada. Notre Stratégie nationale de cybersécurité a aussi mené à la création d'un groupe national de coordination contre la cybercriminalité à la GRC. Ce groupe coordonne les opérations policières à l'encontre des cybercriminels, notamment à l'échelle internationale, et travaille en partenariat étroit avec les autres forces de l'ordre pour contrer les menaces découlant de la cybercriminalité sans frontière.

Dans le contexte de l'invasion de l'Ukraine par la Russie, le gouvernement a intensifié ses actions auprès des secteurs responsables de nos infrastructures essentielles. Ainsi, il y a quelques semaines à peine, nous avons tenu une réunion du réseau multisectoriel sur les infrastructures essentielles pour discuter avec les différentes parties prenantes des menaces qui pèsent sur l'industrie canadienne et des mesures d'atténuation à prendre.

Monsieur le président, tous ces efforts sont soutenus par le budget de 2022 qui prévoit un financement de près de 700 millions de dollars sur une période de cinq ans pour appuyer notre lutte contre la cybercriminalité, protéger les systèmes essentiels du gouvernement et du secteur privé, et accroître notre résilience collective. Nous demeurons fermement résolus à lutter contre l'ingérence étrangère de tout État qui voudrait s'en prendre au Canada.

Nous allons continuer de condamner l'invasion russe et d'appuyer le peuple ukrainien tout en poursuivant nos efforts conjoints avec nos alliés de partout dans le monde qui partagent notre détermination à défendre la paix, la démocratie et l'ordre international fondé sur des règles.

Je vous remercie.

● (1110)

Le président: Merci beaucoup, monsieur le ministre. Je vous suis reconnaissant de vous en être tenu comme toujours au temps imparti.

Nous allons maintenant passer au premier tour de questions. La première période de six minutes va à Mme Dancho

Mme Raquel Dancho (Kildonan—St. Paul, PCC): Merci, monsieur le président.

Merci, monsieur le ministre, d'être des nôtres aujourd'hui, et merci également à tous ceux qui vous accompagnent. Merci de travailler aussi fort pour nous garder en sécurité.

Monsieur le ministre, vous avez beaucoup parlé de cybersécurité, et je vais avoir des questions à ce sujet.

J'aimerais toutefois que nous traitions d'abord de la visite du premier ministre au centre de commandement du NORAD au Colorado. Vous êtes bien sûr le ministre de la Sécurité publique, ce qui englobe la sécurité frontalière, comme vous l'avez mentionné, le SCRS et tout le reste, mais je pense que vous reconnaîtrez, compte tenu de la menace que fait peser l'agression russe, qu'il y a bien sûr chevauchement entre votre ministère et celui de la Défense dirigé par la ministre Anand. Je suis persuadée que vous avez eu des discussions quant aux mesures à prendre pour assurer la sécurité du Canada si le pire devait se produire — une cyberattaque ou une éventualité encore plus effrayante, comme une attaque par un missile.

J'aurais une question à ce propos, car c'est la première fois depuis des décennies qu'un premier ministre du Canada visite le centre de commandement. À mes yeux, cela semble témoigner très clairement de toute l'importance que votre gouvernement accorde à la mise à niveau du NORAD.

Est-ce que je me trompe?

L'hon. Marco Mendicino: Je pense que votre interprétation est assez juste, madame Dancho. J'abonde également dans le sens du préambule à votre question quant aux inquiétudes que nous cause la tournure que prennent actuellement les affaires géopolitiques.

Je tiens à vous remercier en même temps que les autres membres du Comité pour cette étude de l'invasion illégale de l'Ukraine par la Russie. J'estime en outre qu'il est extrêmement important de nous pencher sur l'état de quelques-unes des plateformes internationales multilatérales mises en place après la Seconde Guerre mondiale, comme le NORAD et l'OTAN, car nous voulons non seulement aider le peuple ukrainien à défendre sa souveraineté, mais aussi protéger les démocraties de toute la planète. La visite du premier ministre au NORAD, la première du genre depuis un bon moment déjà, comme vous l'avez souligné, témoigne bien de cet engagement.

Mme Raquel Dancho: Nous pouvons constater que l'invasion en cours incite certains pays à revoir en profondeur leurs investissements dans la défense et la sécurité nationale. Ainsi, l'Allemagne a annoncé des dépenses militaires de 140 milliards de dollars afin de respecter son engagement de 2 %. La Suède et la Finlande vont pour leur part joindre les rangs de l'OTAN.

Dans ce contexte, estimez-vous que le Canada devrait dépenser les 15 milliards de dollars nécessaires à la mise à niveau des systèmes de défense du NORAD?

L'hon. Marco Mendicino: Madame Dancho, je pense que notre gouvernement est tout à fait conscient de la nécessité de veiller à ce que les Forces armées canadiennes et le ministère de la Défense nationale, de même que les différentes agences de sécurité publique représentées ici, disposent des ressources nécessaires pour défendre les intérêts du Canada aussi bien ici qu'à l'étranger…

● (1115)

Mme Raquel Dancho: Croyez-vous que ces organisations disposent actuellement de ressources suffisantes?

L'hon. Marco Mendicino: Nous avons pris des mesures très concrètes dans le budget de 2022 pour faire en sorte que ces organisations continuent de pouvoir compter sur les outils dont elles ont besoin. Ainsi, ce montant de 700 millions de dollars dont j'ai parlé pour la protection de nos cyberinfrastructures essentielles n'est que l'un des nombreux investissements que nous avons consentis. Le budget prévoit également des ressources additionnelles pour la GRC et l'ASFC de même que pour mon ministère, ce qui va directement dans le sens de l'objet de votre étude.

Mme Raquel Dancho: Ce sont là des investissements importants pour la cybersécurité, et je vais y revenir, mais je suis convaincue que vous avez entendu les critiques formulées il y a quelques jours par David Cohen, l'ambassadeur des États-Unis au Canada, qui estime que le récent budget de votre gouvernement ne prévoit pas les investissements nécessaires pour nos forces militaires et notre défense.

Pouvez-vous nous dire si vous croyez que nous devrions dépenser davantage, et convenez-vous que nous devrions atteindre la cible de 2 %?

L'hon. Marco Mendicino: Je vous dirais d'abord que j'ai eu l'occasion de discuter avec l'ambassadeur Cohen, et que j'estime que son affectation à titre d'ambassadeur au Canada est la plus récente d'une longue lignée témoignant des liens très étroits qui unissent nos deux pays.

Dans le cadre de nos efforts constants pour veiller à ce que les membres de nos forces armées ainsi que nos agences nationales de sécurité puissent compter sur les ressources nécessaires, nous nous montrons très transparents quant à l'utilisation optimale de ces ressources. Il est impératif pour nous d'appuyer le NORAD et de nous donner les moyens de protéger nos infrastructures essentielles, notamment au chapitre de la cybersécurité, et nous prévoyons dans le budget des investissements suffisants à cette fin.

Mme Raquel Dancho: M. Cohen a été très critique à l'endroit des investissements de votre gouvernement qu'il juge insuffisants par rapport à ce qu'il considère être raisonnable pour garantir la vigueur de notre défense commune de l'Amérique du Nord.

Des témoins nous ont aussi dit que le Canada contribue dans une large mesure aux efforts de renseignement déployés par le Groupe des cinq, mais pourrait en faire davantage. On m'a essentiellement expliqué que l'on tire de cet exercice l'équivalent de ce qu'on y investit, et que nous sommes loin d'investir suffisamment, ce qui explique pourquoi nous n'avons pas été invités, par exemple, à joindre les rangs de l'AUKUS, comme vous le savez sans doute.

Pouvez-vous nous parler des échanges que vous avez avec le SCRS? Leur avez-vous octroyé un budget supplémentaire? Ne pensez-vous pas que nous devrions en faire davantage afin de devenir un intervenant mieux reconnu lorsque vient le temps de contribuer aux services de renseignement du Groupe des cinq et des instances semblables?

L'hon. Marco Mendicino: Permettez-moi de dire deux choses très rapidement, car je crois qu'il y a deux volets à votre question.

Premièrement, pour ce qui est de la coopération avec les États-Unis et avec nos autres alliés, je vous dirais que nous avons des relations exceptionnellement étroites avec nos voisins américains, particulièrement aux fins du renseignement, et j'estime essentiel de maintenir de tels liens, au sein du Groupe des cinq comme sur d'autres tribunes, surtout à la lumière de l'évolution des menaces pour notre sécurité nationale.

À ce titre, je tiens à féliciter encore une fois les membres du Comité pour leur étude des menaces particulières découlant de l'invasion de l'Ukraine par la Russie.

Mme Raquel Dancho: Merci, monsieur le ministre.

L'AUKUS est un accord de coopération entre l'Australie, le Royaume-Uni et les États-Unis pour l'approvisionnement militaire et la mise en commun du renseignement. Vous êtes bien sûr l'élu officiellement responsable du SCRS. Pouvez-vous nous expliquer pourquoi nous avons été exclus de cet accord? Vous vous dites très satisfaits de notre contribution, mais les États-Unis ne nous ont pourtant pas intégrés à cet accord.

L'hon. Marco Mendicino: Sans vouloir commenter, au nom d'autres pays, les relations multilatérales ou bilatérales qu'ils pourraient choisir d'établir, je tiens simplement à répéter que nous avons des relations exceptionnellement solides, et pas seulement avec les États-Unis. Par exemple, j'ai eu la chance de rencontrer très récemment certains de nos homologues australiens, qui étaient de passage pour parler de la solide collaboration qui existe en matière de renseignement.

En plus du forum du Groupe des cinq, nous entretenons des relations bilatérales très fortes avec d'autres pays et démocraties aux vues similaires afin de nous assurer de combattre les nouvelles menaces qui surgissent sur le plan géopolitique...

Mme Raquel Dancho: Je suis désolée. Merci.

J'en viens à ma dernière question. Les experts en cybersécurité nous ont dit que nous devions investir plus d'argent pour protéger nos petites et moyennes entreprises au chapitre de la cybersécurité. Les nouveaux fonds que vous avez annoncés pour la cybersécurité aident-ils les PME?

Le président: Je regrette, madame Dancho, mais nous sommes...

Mme Raquel Dancho: Je suis désolée. C'est ma dernière question technique. Peut-il simplement répondre?

Le président: Vous avez 10 secondes, monsieur.

L'hon. Marco Mendicino: Il y a beaucoup de choses à dire, mais très brièvement, oui, certains des investissements prévus dans le budget de 2022 profiteront évidemment au travail des organismes qui sont représentés ici, notamment le SCRS et l'ASFC. La cybersécurité est un secteur qui touche bon nombre des différents portefeuilles qui sont représentés autour de cette table.

Le président: Merci beaucoup.

Je cède maintenant la parole à M. Chiang, qui dispose de six minutes.

La parole est à vous, monsieur.

M. Paul Chiang (Markham—Unionville, Lib.): Merci, monsieur le président, et bonjour aux témoins.

Bonjour, monsieur le ministre. Merci de vous joindre à nous aujourd'hui. C'est un plaisir de vous revoir.

Monsieur le ministre, vous avez insisté sur la menace que représente la désinformation russe visant à exploiter et à amplifier les divisions qui existent déjà au Canada. Dans le budget de 2022, le gouvernement propose de dépenser « 10 millions de dollars sur cinq ans [...] afin qu'il coordonne, élabore et mette en œuvre des mesures pangouvernementales visant à lutter contre la désinformation et à protéger la démocratie. »

● (1120)

L'hon. Marco Mendicino: Je suis convaincu que les membres du Comité et tous les parlementaires sont conscients des risques et des menaces considérables que représente la Russie. Sa récente invasion en Ukraine est le reflet de la campagne de déstabilisation dans laquelle elle s'est engagée. Elle a non seulement un effet brutal et profondément négatif sur le peuple ukrainien, mais elle a aussi le potentiel de déstabiliser les choses ailleurs, y compris ici, au Canada.

Par exemple, les efforts déployés par la Russie pour faire croire qu'elle est entrée en Ukraine afin de dénazifier le pays ou qu'elle a agi en représailles à la suite d'attaques ukrainiennes et russes... sont tout à fait faux. La prolifération de ces récits en ligne fait son chemin au Canada, et nous devons donc demeurer très vigilants à cet égard.

Le budget de 2022 prévoit des investissements qui aideront à répondre aux préoccupations relatives à la désinformation et à la mésinformation, et les organismes qui sont représentés ici sont très investis dans ce travail.

M. Paul Chiang: Merci, monsieur le ministre.

Qu'a fait le gouvernement pour contrer la désinformation?

L'hon. Marco Mendicino: Il y a un certain nombre de choses. J'en ai parlé dans ma déclaration.

Tout d'abord, je dirai que, de façon générale, nous avons une stratégie nationale de cybersécurité et un plan d'action national en matière de cybersécurité, et bon nombre des fonctionnaires ici présents participent à ce travail.

Ainsi, la GRC serait en mesure d'enquêter sur toute ingérence étrangère et, éventuellement, d'intenter des poursuites aux termes du Code criminel. Dans le cadre de son travail, le SCRS est en mesure de détecter les menaces possibles à la sécurité nationale, qu'il s'agisse d'ingérence étrangère, de désinformation ou d'information malveillante. Quant à l'ASFC, son travail consiste à assurer l'intégrité et la sécurité de nos efforts au moment d'accueillir des Ukrainiens qui ont dû fuir leurs maisons parce qu'elles ont été détruites.

Voilà donc l'architecture stratégique au sein de laquelle nous coordonnons nos efforts dans l'ensemble du gouvernement pour faire face aux menaces qui résultent de l'incursion illégale de la Russie en Ukraine.

M. Paul Chiang: Merci, monsieur le ministre.

Je cède le reste de mon temps de parole à M. Noormohamed.

M. Taleeb Noormohamed (Vancouver Granville, Lib.): Merci, monsieur Chiang; merci, monsieur le président, et merci aux témoins et au ministre d'être des nôtres aujourd'hui.

Si je peux me permettre, j'aimerais présenter une motion à ce stade-ci, mais je voudrais commencer par dire quelques mots en guise d'introduction.

Le Comité a effectué un travail exceptionnel pour trouver des moyens de collaborer. En déposant la motion qui suit, je demande le consentement unanime pour en faire la proposition. Cette motion se rapporte au fait que nous avons constaté une ruée vers l'achat d'armes à feu. Elle ne vise pas à usurper ou à remplacer le débat important que nous devons tenir sur le projet de loi C-21, mais je souhaite présenter la motion suivante et je demanderai le consentement unanime du Comité à cet égard.

La motion se lit comme suit:

> Que le Comité fasse rapport de ce qui suit à la Chambre: Que, conformément à l'article 118 (4)(b)(ii) de la Loi sur les armes à feu (1998), le Comité permanent de la sécurité publique et nationale a décidé de ne pas mener d'enquêtes ou d'audiences publiques sur le projet de règlement déposé et renvoyé au Comité le 30 mai 2022.

La traduction et le texte original de la motion ont été transmis au greffier.

Je soumets cette motion au Comité simplement parce que je crois qu'il est important que nous donnions notre consentement unanime pour aller de l'avant, en reconnaissant la qualité du travail du Comité. C'est vraiment en réaction à la ruée vers l'achat d'armes à feu, ce qui est alarmant.

Je sais qu'un certain nombre de députés de tous les partis ont soulevé cette question. J'ai eu des discussions avec des députés de l'opposition, ainsi qu'avec d'autres, qui ont exprimé de graves et profondes inquiétudes à ce sujet. Je présente donc cette motion au Comité et je demande la collaboration de tous pour obtenir le consentement unanime.

Je vous remercie, monsieur le président.

Le président: D'accord, chers collègues, nous sommes saisis d'une motion. Il faut le consentement unanime pour continuer.

Le député a-t-il le consentement unanime pour aller de l'avant avec sa motion?

M. Dane Lloyd (Sturgeon River—Parkland, PCC): Non.

● (1125)

Le président: D'accord. Je suppose donc que nous nous occuperons de l'avis de la motion à la prochaine réunion du Comité et que nous en débattrons à ce moment-là.

Monsieur le greffier, est-ce bien cela? Très bien.

Puisqu'il n'y a pas de consentement unanime et que le temps de parole de l'intervenant précédent est écoulé, je cède la parole à Mme Michaud, qui dispose de six minutes.

La parole est à vous.

[*Français*]

Mme Kristina Michaud (Avignon—La Mitis—Matane—Matapédia, BQ): Merci, monsieur le président.

Je remercie les témoins de leur présence.

C'est agréable de vous voir en personne, monsieur le ministre.

J'aimerais vous poser une question concernant les décrets secrets que votre gouvernement a adoptés depuis 2015. On parle de 72 décrets secrets. Il s'agit d'une forte hausse comparativement au nombre de décrets secrets adoptés par le gouvernement conservateur de Stephen Harper. Normalement, pour justifier l'adoption d'un décret secret, on doit citer la sécurité nationale ou militaire, ou encore soutenir que le décret est lié aux examens relatifs à la sécurité nationale des investissements étrangers dans des compagnies canadiennes. Plus de la moitié de ces décrets ont été adoptés depuis le début du mois d'avril...

[*Traduction*]

M. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.): Excusez-moi, monsieur le président. J'invoque le Règlement. Je présente mes excuses à Mme Michaud, mais la sonnerie d'appel se fait entendre. Je me demande si nous pouvons obtenir le consentement unanime pour continuer jusqu'à la fin du premier tour avant de suspendre la séance pour le vote.

Le président: Y a-t-il consentement unanime pour que nous poursuivions la séance?

Le greffier du Comité (M. Wassim Bouanani): Oui.

Le président: D'accord, alors poursuivons.

Madame Michaud, vous avez la parole.

[*Français*]

Mme Kristina Michaud: Merci, monsieur le président.

Un de ces décrets a été adopté entre le 28 janvier et le 1er février 2022 et un autre a été adopté autour de la mi-février, ce qui correspond à peu près au début de la manifestation des camionneurs.

Un autre décret a été adopté à un moment où la communauté internationale commençait à s'inquiéter de voir la Russie s'apprêter à envahir l'Ukraine, autour du 24 février. D'autres décrets ont été adoptés à partir du moment où la Russie a effectivement envahi l'Ukraine.

En réponse à cela, votre gouvernement a dit qu'il plaidait la transparence. S'il voulait faire preuve de transparence, pourquoi a-t-il eu recours aux décrets secrets?

Puisque votre gouvernement en a adopté davantage que les gouvernements précédents, a-t-on des raisons de croire qu'il y a des menaces réelles à la sécurité nationale et que vous désirez garder ces informations confidentielles?

Pourriez-vous nous en dire davantage sur l'application de ces décrets?

L'hon. Marco Mendicino: Je vous remercie de la question, madame Michaud. Cela me donne l'occasion de réaffirmer l'importance de protéger le principe d'un gouvernement ouvert et transparent. Ce principe s'applique à tous nos dossiers. Cependant, comme vous l'avez mentionné, nous devons aussi appliquer d'autres principes pour protéger nos intérêts relativement aux enjeux de sécurité nationale.

Cette décision a été prise pour protéger non seulement les principes, mais aussi tous les Canadiens et Canadiennes.

Mme Kristina Michaud: Devons-nous comprendre que certaines informations sont gardées secrètes parce que le Canada craint des répercussions en lien avec ce qui se passe en Ukraine? La Russie mène des campagnes de désinformation et procède à des cyberattaques. Devons-nous comprendre que le choix de garder secret ce genre de décret est en lien avec cette situation?

L'hon. Marco Mendicino: Le gouvernement considère différents facteurs avant de décider d'appliquer les principes relatifs à la sécurité nationale. Cela dit, nous tentons toujours de transmettre le maximum d'information au public lorsque nous décidons de recourir à ces décrets, afin de respecter la valeur importante d'avoir un gouvernement ouvert et transparent.

Mme Kristina Michaud: À la fin du mois de mai dernier, un groupe de travail de l'Université d'Ottawa, auquel contribuent notamment quatre anciens conseillers en sécurité nationale, deux anciens directeurs du Service canadien du renseignement de sécurité, d'anciens ambassadeurs, d'anciens sous-ministres à la retraite ainsi que des universitaires, a réalisé une étude concluant que le Canada n'était pas prêt à faire aux menaces, notamment celles de la Russie. Ces experts disaient qu'on n'était pas prêt à affronter ce nouveau monde et que, de toute urgence, il fallait repenser notre sécurité nationale. Un des constats est que l'invasion russe en Ukraine démontre les menaces directes qui pèsent sur les intérêts du Canada. La Chine pourrait également représenter un défi à long terme, d'après eux.

Comment réagissez-vous à ces critiques d'anciens experts gouvernementaux qui disent que notre sécurité nationale n'est pas au point, en ce moment?

● (1130)

L'hon. Marco Mendicino: Tout d'abord, je connais certains des auteurs de cette étude, et je veux les remercier de leur travail et de leur contribution. J'ai eu l'occasion de consulter plusieurs de leurs recommandations. Cela vaut la peine de considérer d'autres études et de chercher des solutions que le gouvernement peut intégrer à sa stratégie. Cette étude arrive à un bon moment, parce que le gouvernement est en train de moderniser sa stratégie en matière de cybersécurité. C'est une très bonne chose qu'on ait fait cette étude. Cela dit, nos agences font aussi beaucoup de bon travail.

[*Traduction*]

Le président: Merci, monsieur le ministre.

J'invite maintenant M. MacGregor à prendre la parole. Vous avez six minutes pour poser vos questions.

M. Alistair MacGregor (Cowichan—Malahat—Langford, NPD): Merci beaucoup, monsieur le président.

Bienvenue à nouveau, monsieur le ministre. Je suis heureux de vous revoir.

Nous avons entendu un certain nombre de témoins de tous les horizons, ainsi que de nombreux experts. Nous avons eu la chance d'entendre leurs témoignages devant notre comité au sujet de la menace posée par la cybercriminalité dans le contexte canadien. En ce qui concerne la situation au Canada, il y a un centre de coordination contre la cybercriminalité au sein de la GRC, ainsi que le Centre de la sécurité des télécommunications, qui dirige le Centre canadien pour la cybersécurité.

Monsieur le ministre, comme vous le savez, le gouvernement fédéral est une grosse machine, si bien qu'on risque parfois de travailler en vase clos. Le CST relève de la ministre de la Défense. L'unité de la GRC relève, pour sa part, du ministère de la Sécurité publique. En tant que membre du Comité, je voudrais savoir comment ces deux ministères veillent à l'harmonisation du travail effectué par ces deux organismes, tout en évitant le double emploi. Parfois, des choses peuvent nous échapper lorsque nous avons affaire à deux ministères différents.

Pouvez-vous nous expliquer comment ces ministères et leurs organismes respectifs travaillent ensemble pour régler ce problème bien réel?

L'hon. Marco Mendicino: C'est une excellente question, monsieur MacGregor. Pour commencer, je tiens à souligner que la stratégie nationale sur la cybersécurité et le plan d'action national en matière de cybersécurité sont deux instruments de politique que nous utilisons pour coordonner ces efforts. Entre autres, mon sous-ministre, Rob Stewart, joue un rôle de président d'une tribune qui réunit différents fonctionnaires de tout le gouvernement, y compris ceux du ministère de la Défense nationale. Nous avons ainsi le moyen de mettre en commun l'information, de coordonner les efforts, de repérer les menaces et de déterminer la meilleure façon d'instaurer des stratégies d'atténuation.

Vous avez tout à fait raison. Il est important que ces efforts se poursuivent afin d'éviter une forme de cloisonnement, qui peut mener à la fragmentation d'une réponse coordonnée.

M. Alistair MacGregor: Je vous remercie.

Nous savons que le gouvernement russe a des liens étroits d'alliance et de coordination avec plusieurs organisations criminelles. Il s'est associé à ces organisations criminelles pour qu'elles fassent le sale boulot à sa place. Cela a souvent des conséquences bien réelles dans le monde entier, y compris ici, au Canada.

Certains témoins nous ont dit que le gouvernement fédéral et les entreprises sous réglementation fédérale — les banques canadiennes, etc. — disposent d'une sécurité de très haut niveau. Ce qui pose problème, ce sont les organisations et les gouvernements infranationaux: les systèmes de soins de santé provinciaux, la cybersécurité de nos grandes villes, et même les grandes entreprises.

Premièrement, que faites-vous pour vous attaquer à ce problème?

Deuxièmement, certains témoins ont réclamé le signalement obligatoire des incidents. Parfois, les entreprises répugnent à déclarer qu'elles ont été prises en otage par un rançongiciel. Elles estiment qu'il est plus facile de payer la personne et de ne pas signaler l'incident. Elles peuvent également être menacées de dommages supplémentaires si elles le signalent aux autorités.

Quelles mesures prenez-vous à l'égard de ces deux questions?

● (1135)

L'hon. Marco Mendicino: Encore une fois, je ne saurais trop insister sur l'importance, dans le contexte géopolitique actuel, d'être sur un pied d'alerte face à d'éventuelles attaques menées par des acteurs étatiques hostiles, comme la Russie, sous forme de cyberattaques ou de rançongiciels, qui visent non seulement des cibles potentiellement précieuses pour les intérêts canadiens, comme les infrastructures essentielles, mais aussi des cibles infranationales, d'autres ordres de gouvernement et d'autres secteurs de l'économie. Une grande partie de ce travail est mené par le Centre canadien pour la cybersécurité, qui relève du CST, où nous collaborons avec l'industrie et les chefs de file de l'économie pour leur fournir des conseils pratiques et sensés sur la meilleure façon de protéger leurs entreprises.

M. Alistair MacGregor: En ce qui a trait au signalement obligatoire des incidents, selon un vieux dicton, « nous ne savons pas ce que nous ne savons pas ». Or, nous savons, grâce à d'autres études, que Statistique Canada a des lacunes en matière de données sur les crimes violents qui pourraient avoir été commis avec des armes à feu. Il y a certainement lieu d'apporter des améliorations dans ce domaine.

Si nous ne connaissons pas vraiment toute l'ampleur du problème, et si certaines entreprises ne dénoncent pas de tels incidents, quelles mesures le gouvernement prend-il pour rendre obligatoire le signalement des cas de cybercriminalité?

L'hon. Marco Mendicino: Je vous remercie de votre question complémentaire. Je m'apprêtais justement à parler de la façon dont nous collaborons avec les chefs de file de l'économie et de l'industrie pour encourager le signalement et dissiper leurs craintes quant aux stéréotypes ou aux préjugés.

M. Alistair MacGregor: « Encourager » n'est pas la même chose que « rendre obligatoire ».

L'hon. Marco Mendicino: Vous avez raison d'établir cette distinction, et c'est certainement une question à laquelle nous réfléchissons au sein du gouvernement. Je tiens à ajouter que le CCC — le Centre canadien pour la cybersécurité — publie également une évaluation des cybermenaces nationales. C'est là un autre outil que peuvent utiliser les chefs de file de l'industrie, de l'économie et des autres ordres de gouvernement. Nous essayons donc d'offrir un soutien par l'entremise de cet organisme gouvernemental.

M. Alistair MacGregor: Le signalement obligatoire des incidents est-il à l'ordre du jour?

L'hon. Marco Mendicino: Je crois absolument que c'est quelque chose que nous devons envisager, à coup sûr. C'est une option que nous examinons très attentivement.

M. Alistair MacGregor: D'accord.

Monsieur le président, je vous cède mes 10 dernières secondes.

Le président: Je vous remercie.

Nous passons maintenant à la deuxième série de questions.

Le premier intervenant est M. Lloyd, qui dispose de cinq minutes.

Monsieur le greffier, je suppose que vous surveillez le temps qui reste avant la tenue du vote?

M. Ron McKinnon: Monsieur le président, j'invoque le Règlement. Nous avons obtenu le consentement unanime pour terminer le premier tour, de sorte que nous puissions suspendre la séance et passer au vote.

Le président: Oui. Si telle est la volonté du Comité, nous pouvons faire une pause maintenant et reprendre après que tout le monde a eu l'occasion de voter.

Les députés vont-ils voter à distance, ou comptent-ils se rendre à l'édifice de l'Ouest?

Mme Pam Damoff (Oakville-Nord—Burlington, Lib.): Les deux, monsieur le président.

Le président: Je vois. Dans ce cas, je crois qu'il serait prudent de suspendre la séance jusqu'à ce que les députés aient eu l'occasion de voter. Nous reprendrons dès que les députés auront regagné leur siège.

Le Comité suspend maintenant ses travaux pour permettre aux députés de voter.

[*La séance se poursuit à huis clos.*]