CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

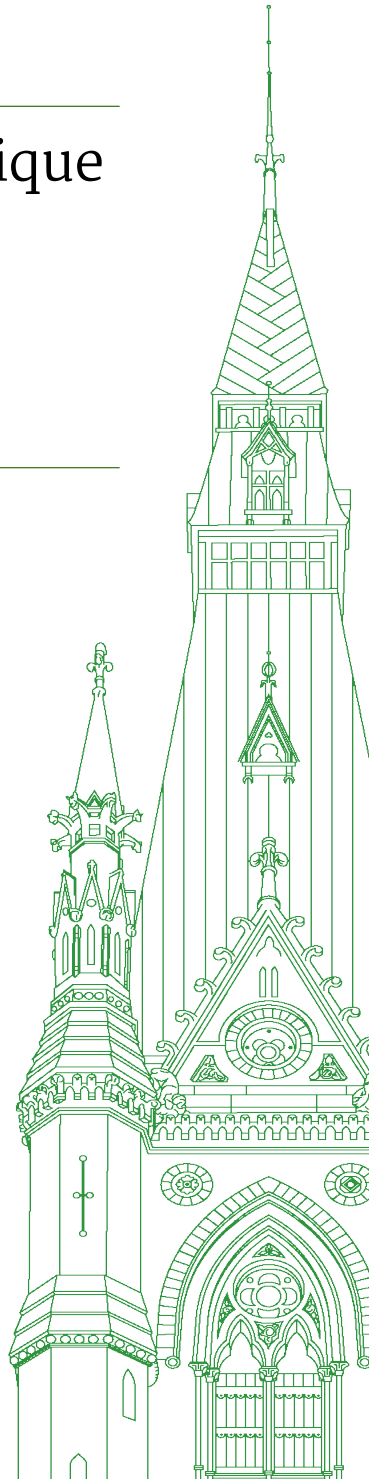
44e LÉGISLATURE, 1re SESSION

Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 021

Le mardi 3 mai 2022



Président : L'honorable Jim Carr

Comité permanent de la sécurité publique et nationale

Le mardi 3 mai 2022

● (1135)

[*Traduction*]

Le président (L'hon. Jim Carr (Winnipeg-Centre-Sud, Lib.)): Bonjour à tous. La séance est ouverte.

Je présente mes excuses aux témoins pour notre retard. Comme vous le savez, nous avons été retenus par un vote. C'est le moment de l'année où nous en avons plusieurs. Ils sont aléatoires, et nous devons simplement prendre les choses comme elles viennent.

Nous sommes maintenant prêts à commencer.

Bienvenue à la 21e réunion du Comité permanent de la sécurité publique et nationale de la Chambre des communes.

J'aimerais tout d'abord reconnaître que nous nous trouvons sur le territoire traditionnel non cédé du peuple algonquin.

La réunion d'aujourd'hui se déroule sous forme hybride, conformément à l'ordre de la Chambre du 25 novembre 2021. Certains membres sont présents dans la salle et d'autres utilisent l'application Zoom à distance. Les députés et les témoins qui participent virtuellement à la séance peuvent s'exprimer dans la langue officielle de leur choix. Vous avez le choix, au bas de votre écran, entre le son du parquet, l'anglais ou le français.

Conformément au paragraphe 108(2) du Règlement et aux motions adoptées par le Comité le jeudi 3 mars 2022, le Comité reprend son étude de l'évaluation de la posture de sécurité du Canada par rapport à la Russie.

Nous accueillons aujourd'hui, non pas par vidéoconférence, mais en personne, M. Charles Burton, agrégé supérieur au Centre for Advancing Canada's Interests Abroad de l'Institut Macdonald-Laurier, qui comparaît à titre personnel. De plus, nous accueillons Mme Jennifer Quaid, directrice exécutive d'Échange canadien de menaces cybernétiques, qui participe virtuellement, je crois. Nous entendrons également en personne le témoignage de M. Michael Doucet, directeur exécutif du Bureau du chef de la sécurité de l'information, chez Optiv Canada Federal.

Nos témoins auront chacun un maximum de cinq minutes pour faire leur déclaration préliminaire. J'en profite pour mentionner que ceci sera l'avertissement de 30 secondes. Je suis très rigoureux. Que ce soit lors des déclarations préliminaires ou des périodes de questions, je vais signaler qu'il ne reste que 30 secondes. Ce sera malheureusement le seul avertissement que vous recevrez.

J'invite maintenant M. Burton à prendre la parole pour un maximum de cinq minutes.

Nous vous écoutons, monsieur Burton.

M. Charles Burton (agrégé supérieur, Centre for Advancing Canada's Interests Abroad, Macdonald-Laurier Institute, à titre personnel): Merci, monsieur le président.

La menace que représente la Russie pour la sécurité publique et nationale du Canada a considérablement augmenté depuis que les démocraties occidentales ont réagi à l'invasion de l'Ukraine par la Russie en adoptant des mesures visant à déstabiliser l'économie russe et en fournissant des armes pour aider la défense ukrainienne. Peu importe ce que sera l'issue des souffrances de l'Ukraine, la Russie restera isolée par l'Occident et exclue des transactions financières et commerciales avec les lucratifs marchés de l'Europe. Je pense qu'il est juste de penser que Poutine bouillonne de colère, qu'il est agité et amer, et qu'il a les capacités de lancer de dangereuses attaques contre le Canada en représailles. Il est fort possible qu'il fasse front commun avec la Chine, ce qui aggravera la menace à laquelle nous faisons face.

Le Canada n'est pas suffisamment préparé pour réagir à l'éventail de menaces posées par la Russie, notamment aux attaques contre ses infrastructures essentielles, à l'espionnage et au sabotage. Nous sommes moins bien préparés que nos alliés.

Une grande préoccupation à cet égard est de savoir si la GRC, le Service canadien du renseignement de sécurité, ou SCRS, et le Centre de la sécurité des télécommunications, le CST, ont été suffisamment transparents envers le Parlement, représenté par votre comité de la Chambre des communes, sur les préoccupations en matière de sécurité publique et nationale. Nous savons que la GRC, le SCRS, le CST et le MDN recueillent beaucoup d'information sur les activités malveillantes de la Russie, mais lorsque le Parlement veut obtenir de l'information pour le guider dans l'élaboration d'une loi visant à protéger la sécurité publique et nationale, ces organismes sont trop souvent évasifs sous prétexte que l'information est trop délicate ou que sa divulgation révélerait des détails opérationnels susceptibles d'aider nos ennemis.

Il serait raisonnable de croire que le Groupe des cinq, dont le Canada fait partie, était au courant des ambitions mégalomanes entretenues par M. Poutine à l'égard de l'Ukraine. Les choses n'ont pas changé en Russie. C'est simplement notre compréhension qui s'est améliorée. Ces organisations connaissent les intentions de Poutine relativement à de futures invasions et ce que sont les menaces qu'il réserve au Canada, mais comment pouvons-nous nous préparer si elles refusent de communiquer leurs évaluations du renseignement sur ce à quoi nous devrions nous préparer? Trop souvent, les services de police et de sécurité du Canada considèrent que leur rôle principal est simplement de conserver des renseignements qu'ils peuvent échanger avec leurs organismes homologues. Encore une fois, ce problème est plus prononcé au Canada que chez nos alliés.

Par exemple, jusqu'à quel point le Canada a-t-il besoin, à titre de mesures de sécurité nationale, d'une loi sur le registre des agents étrangers ou de quelque chose comme la loi australienne sur le régime de transparence en matière d'influence étrangère? Je crois que cela est extrêmement urgent, surtout dans le contexte actuel, et le SCRS connaîtrait mieux que quiconque l'identité des Canadiens qui sont influents dans le processus stratégique du Canada et qui sont dans une situation de conflit d'intérêts qui menace la sécurité et la souveraineté du Canada parce qu'ils ont reçu des avantages d'un État étranger. Combien y en a-t-il? Jusqu'à quel niveau sont-ils? Si le SCRS possède ces renseignements, il devrait vous les transmettre.

Qu'en est-il de Cameron Ortis de la GRC? Que devrions-nous apprendre de son arrestation? Que se passe-t-il avec les laboratoires de Winnipeg? S'est-il produit un manquement à la protection de la sécurité nationale canadienne sur lequel le Parlement devrait se pencher? Il y a aussi l'affaire Quentin Huang. Comment se fait-il que, contrairement à ses alliés, le Canada n'arrive pas à poursuivre et à emprisonner les personnes qui transfèrent des technologies militaires du Canada à des agents d'un État étranger?

Permettez-moi d'ajouter un dernier point. Comme l'a étudié le Comité spécial sur les relations sino-canadiennes, les médias chinois au Canada sont fortement dominés par des éléments qui appuient le programme du Parti communiste chinois au Canada. Depuis le début des affrontements en Ukraine, les médias chinois et leurs mandataires au Canada répètent jour après jour, semaine après semaine et plus ou moins mot à mot, les théories de conspiration russes et la désinformation qui en découle. Cette désinformation russe discrédite l'intégrité des institutions démocratiques et judiciaires canadiennes et mine la loyauté d'un grand nombre de Canadiens d'origine chinoise envers le Canada.

Je suis d'avis que le Canada doit considérer tout cela avec beaucoup de sérieux et affecter des ressources et restructurer ses organismes de sécurité publique et nationale de façon à lui permettre de répondre beaucoup plus efficacement qu'il ne l'a fait jusqu'à maintenant.

Merci, monsieur le président.

● (1140)

Le président: Je vous remercie beaucoup.

J'aimerais maintenant inviter Mme Quaid à faire sa déclaration préliminaire.

Vous avez la parole pour cinq minutes, madame Quaid.

Mme Jennifer Quaid (directrice exécutive, Échange canadien de menaces cybernétiques): Merci, monsieur le président.

Je m'appelle Jennifer Quaid. Je suis directrice exécutive d'Échange canadien de menaces cybernétiques, ECMC.

ECMC est un organisme pancanadien à but non lucratif dont le mandat est d'aider les entreprises canadiennes à renforcer leur cyberrésilience grâce à la collaboration. Nous comptons 170 membres dans 15 secteurs. ECMC a été mis sur pied par quelques-unes des plus grandes entreprises du Canada, mais sa mission est d'aider les organisations de toutes tailles à réduire les risques financiers et opérationnels en obtenant des renseignements pertinents et opportuns sur les menaces. Nos membres participent parce qu'ils comprennent que la première chose à faire pour assurer la cyberrésilience de leurs organisations est de comprendre l'environnement des cybermenaces et son évolution constante.

La ministre de la Défense nationale du Canada a récemment déclaré que la cybersécurité est l'un des plus grands défis économiques et de sécurité nationale auxquels nous sommes confrontés. Comme vous le savez, les cybermenaces sont de plus en plus raffinées et omniprésentes. Propulsée par la croissance des technologies novatrices et leur adoption à l'échelle mondiale, la cybercriminalité est lucrative. Pour qui est-elle payante? Nous pouvons grosso modo grouper les auteurs de cybermenaces en deux catégories, soit les États-nations qui utilisent Internet pour se livrer à des activités d'espionnage et d'action politique, et les criminels qui utilisent la cybercriminalité à des fins lucratives.

C'est cet élément criminel qui a commercialisé la cybercriminalité. C'est maintenant une industrie à part entière. C'est un domaine dans lequel il est plus facile que jamais de se lancer. L'expertise technique n'est plus nécessaire. La cryptomonnaie facilite la perception des paiements, et il y a peu de risques de se faire prendre. Plusieurs pays laissent des groupes de cybercriminels opérer sur leurs territoires, mais il y a aussi des cybermilitants, c'est-à-dire des cyberattaquants qui ciblent l'injustice sociale, ainsi que l'omniprésente menace interne.

Les tensions géopolitiques persistantes en Russie et en Ukraine ont créé une occasion d'accroître le cybermilitantisme et l'activité criminelle. Les auteurs de menaces ciblent les infrastructures essentielles des deux côtés, détruisant les sites Web bancaires et perturbant les services gouvernementaux. L'organisation criminelle Conti appuie la Russie. Anonymous dit mener une guerre électronique contre Poutine. Bataillon Network 65 a volé et utilisé le code de Conti pour bloquer des fichiers dans des entreprises russes liées au gouvernement.

Les organisations canadiennes surveillent ce qui se passe en Ukraine et travaillent avec une vigilance accrue. Les membres d'ECMC, en collaboration avec le Centre canadien pour la cybersécurité, veillent à ce que les entreprises canadiennes puissent mieux se défendre contre ces cyberattaquants.

C'est un excellent exemple de ce que l'on peut faire dans le cadre d'un partenariat public-privé. Par l'entremise d'ECMC, le Centre canadien pour la cybersécurité peut diffuser de l'information aux entreprises de toutes tailles et de tous les secteurs. Nous pouvons ensuite aider nos membres à collaborer, à tirer parti de cette information et à l'utiliser de façon utile, mais la collaboration va plus loin que le simple partage de renseignements sur les menaces. Des professionnels échangent des pratiques exemplaires et analysent des problèmes cybernétiques qui seraient impossibles à résoudre par une seule organisation ou un seul secteur.

Il s'agit de collaborer avec les autres pour améliorer votre cyberrésilience, la résilience de votre chaîne d'approvisionnement, de vos clients et de l'économie canadienne. C'est une façon efficace de renforcer la capacité des équipes, un aspect de plus en plus important dans une économie où 25 000 postes sont à combler. Selon l'Autorité canadienne pour les enregistrements Internet, 25 % des organisations ont rapporté des atteintes à la sécurité des données, et les attaques ne cessent pas.

Que peut-on faire de plus? Pour beaucoup d'organisations, le partage serait plus facile si le gouvernement adoptait simplement des lois « d'exonération », c'est-à-dire des lois qui encourageraient les entreprises et les organisations à partager volontairement des renseignements en les protégeant contre les répercussions juridiques, à partager au-delà des exigences législatives. Vous pouvez également permettre à un plus grand nombre d'entreprises de se joindre à une organisation de collaboration en incluant l'adhésion dans les retombées industrielles et technologiques, il faut encourager l'échange d'information de toutes les façons possibles.

La collaboration en matière de cybermenaces et le renforcement de notre résilience collective sont essentiels pour prévenir, détecter et endiguer les cyberattaques dans le secteur privé. Nous réussirons beaucoup mieux si nous travaillons ensemble.

Merci.

● (1145)

Le président: Merci beaucoup.

J'aimerais maintenant inviter M. Michael Doucet à faire sa déclaration préliminaire. Il aura la parole pour un maximum de cinq minutes.

Nous vous écoutons, monsieur Doucet.

M. Michael Doucet (directeur exécutif, Bureau du chef de la sécurité de l'information, Optiv Canada Federal): Merci beaucoup.

Bonjour. C'est un honneur pour moi d'être ici ce matin pour m'exprimer au nom de mon organisation, Optiv.

Notre niveau de préparation à la grande variété de menaces posées par la Russie justifie la présente discussion, notre engagement collectif et notre volonté de nous concentrer sur le renforcement de nos systèmes, de notre préparation et de notre réponse. Optiv est heureuse de participer à cette discussion.

En tant que praticien ayant contribué à la sécurité nationale dans divers rôles au sein du gouvernement pendant 30 ans et qui travaille maintenant avec l'intégrateur spécialisé en cybersécurité depuis près de quatre ans, je suis particulièrement intéressé à l'approche que nous adoptons pour comprendre et contrer les cybermenaces posées par la Russie et d'autres États-nations qui veulent nous nuire. Cette menace fait fi de toutes les frontières, qu'elles soient nationales, provinciales, territoriales ou municipales.

La cybersécurité est un sport d'équipe qui exige une gouvernance mature, une attention bien ciblée, des mesures et des essais. La diligence continue doit être la norme.

Je vais maintenant vous parler un peu d'Optiv.

Optiv est un intégrateur de cybersécurité de renommée mondiale. Nous travaillons de concert avec des clients et des secteurs public, privé et sans but lucratif en vue d'assurer la gestion des cyberrisques et de fournir aux organisations des prévisions et des programmes qui accéléreront l'avancement des programmes. Nous proposons une variété de produits et de services cybernétiques, notamment le renseignement sur les menaces, la recherche de menaces, la réponse aux incidents, les services gérés et la gestion de l'identité et des données, pour n'en nommer que quelques-uns.

Dans le cadre de mon travail à Optiv à titre de directeur exécutif du Bureau du chef de la sécurité de l'information, j'ai la responsabilité d'encourager, à l'échelle pancanadienne, tous les secteurs et toutes les industries verticales à comprendre, à quantifier, à mettre à l'essai et à améliorer leur position de cyberdéfense. En général, nous adoptons une approche fondée sur le risque.

Qu'est-ce que je veux dire lorsque je parle d'une approche fondée sur le risque? Cela veut dire que les gens doivent d'abord comprendre leur programme cybernétique. Ce programme doit ensuite être évalué pour identifier les lacunes à corriger pour réduire les risques pour l'organisation. Ce travail est accompli dans un environnement changeant qui exige une diligence et des améliorations continues. Dans l'univers de la cybersécurité, le travail n'est jamais terminé. Les organisations ne peuvent pas s'accorder une journée de congé. Dans le domaine de la cybersécurité, les transformations numériques se produisent rapidement, elles sont essentielles à la mission et de plus en plus complexes. Il incombe à tous les intervenants et à tous les citoyens d'avoir une incidence positive sur notre environnement numérique.

Passons maintenant à l'important enjeu de notre niveau de préparation face aux menaces posées par la Russie, en considérant particulièrement la continuité des activités du gouvernement et des infrastructures essentielles. Le gouvernement fait évidemment partie des infrastructures essentielles, mais je voudrais parler plus précisément du gouvernement fédéral.

À un niveau élevé, quelle est la menace posée par la Russie? Examinons la menace initiale.

Avant l'offensive terrestre, le centre mondial de renseignement sur les menaces d'Optiv a diffusé à grande échelle un avis résumant les cyberincidents liés aux tensions continues en Ukraine, ainsi que la cyberactivité antérieure attribuée au gouvernement russe et au soutien des opérations militaires en Europe de l'Est. La cyberactivité et les opérations d'influence de la Russie contre l'Ukraine et l'OTAN visant à soutenir les manœuvres militaires de la Russie comprennent des attaques de type déni de service, des opérations psychologiques et des campagnes de désinformation utilisées comme prétexte aux activités militaires.

Passons maintenant à l'enjeu de notre état de préparation. Comment mesurons-nous le niveau de notre préparation? Lorsque les menaces et les besoins varient selon les infrastructures essentielles verticales, nous cherchons à adopter une approche horizontale en matière de cybersécurité. Les programmes de cybersécurité doivent être appropriés à la taille de chaque organisation, mais ils peuvent néanmoins faire l'objet de rapports uniformes. Je ne saurais trop insister sur ce point: chaque organisation. Il doit y avoir une évaluation. Il faut ensuite établir ce que doit être l'état final du programme de cybersécurité. S'il y a des divergences entre les deux, il faut prendre les mesures nécessaires pour corriger les lacunes.

Concrètement, qu'est-ce que cela signifie? Cela signifie que l'organisation doit évaluer son programme de cybersécurité, ses paramètres, ses lacunes et élaborer une stratégie en matière de cybersécurité. La stratégie servira ensuite à élaborer des programmes et des plans pour combler les lacunes. Il faut élaborer un plan d'intervention en cas d'incident et des plans de continuité pour assurer la poursuite des activités. Ce plan peut ensuite être complété par des mesures et un tableau de bord, et il doit être mis à l'essai pour s'assurer d'être prêt à répondre à un incident. Il faut ensuite évaluer et améliorer le programme de manière continue.

Il me fera plaisir de vous présenter des recommandations concrètes dans le cadre de nos discussions.

Je vais m'arrêter ici et je serai heureux de répondre à vos questions.

Je vous remercie.

● (1150)

Le président: Merci infiniment.

Vous n'aurez pas à attendre longtemps pour les questions, car nous allons commencer immédiatement.

Mme Dancho sera notre première intervenante.

Vous avez la parole pour six minutes, madame Dancho.

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

Je remercie nos témoins d'être avec nous aujourd'hui.

Monsieur Burton, mes premières questions s'adressent à vous et concernent les relations entre la Russie et la Chine, et en particulier la manière dont ces deux pays ont signé un pacte de sécurité, largement perçu comme allant à l'encontre de l'Amérique et de l'Occident. C'était en février. Puisque vous connaissez très bien la Chine grâce à votre expérience et à votre formation universitaire, j'aimerais avoir votre opinion — alors que nous étudions la posture de sécurité du Canada, et que nous parlons plus particulièrement de la Russie, — sur ce que pourrait être l'incidence de ce pacte de sécurité sur la façon dont le Canada devrait aborder sa propre sécurité?

● (1155)

M. Charles Burton: Je pense que c'est très préoccupant. Essentiellement, en raison de l'invasion, mal conseillée ou probablement non conseillée, de l'Ukraine par M. Poutine, la Russie sera considérablement affaiblie, tant sur le plan militaire parce qu'elle perd beaucoup d'éléments — elle a perdu le Moskva dans la mer Noire — que sur le plan économique. La Russie devra alors compter davantage sur la Chine pour l'exportation des produits de base qui assurent sa prospérité, à savoir le pétrole et les minéraux, et elle fera également confiance à la Chine pour aller à l'encontre de nos sanctions. La Chine a aidé la Corée du Nord à éviter efficacement les sanctions que nous avons tenté d'imposer à ce régime.

Je crois qu'il y aura certainement un moment où la Chine demandera un juste retour, c'est-à-dire qu'elle s'attendra à ce que la Russie l'aide à réaliser ses objectifs mondiaux, ce qui pourrait inclure une demande de soutien militaire russe pour mener de futures actions contre Taïwan et faire front commun avec la Russie en ce qui concerne les revendications territoriales dans l'Arctique.

Comme vous le savez, la Russie revendique à peu près tout ce qui se trouve sous le plateau continental canadien, et la Chine a les ressources et la capacité nécessaires pour commencer à exploiter les ressources dans l'Arctique. La Chine s'est récemment qualifiée d'« État du Proche-Arctique ». Je pense qu'elle est à peu près aussi près de l'Arctique que le Yémen, mais de toute façon, elle veut avoir accès à nos ressources nordiques à des fins stratégiques, aux ports, et à nos ressources naturelles.

Compte tenu du positionnement stratégique de la Russie, une collaboration entre ces deux pays serait une très mauvaise nouvelle pour le Canada. Comme je l'ai fait valoir dans un autre contexte, contrairement à d'autres témoins qui ont comparu devant le Comité, je crois vraiment que nous devons commencer à réfléchir à ce que nous pourrions faire pour assurer la protection de nos régions nordiques. Il ne s'agit pas vraiment de savoir si nous y consacrons 2 %, ou moins ou plus. Il s'agit en fait de savoir ce qu'il en coûtera pour rattraper des décennies de négligence en Arctique, surtout si la Russie et la Chine s'allient et commencent en fait à représenter une menace réelle avec le réchauffement climatique qui ouvre des voies de navigation aux navires chinois et russes de tous genres.

Mme Raquel Dancho: Je comprends.

Je voulais également vous poser une question précise au sujet de l'ambassadeur du Canada en Russie et de l'ambassadeur de la Russie ici au Canada, largement considéré comme ayant diffusé beaucoup de désinformation au Canada.

Le gouvernement libéral dit actuellement que nous ne pouvons pas expulser l'ambassadeur de la Russie parce que cela entraînerait l'expulsion de notre ambassadeur en Russie, et que dans ce cas, nous n'aurons plus d'observateur sur le terrain. Qu'en pensez-vous? Êtes-vous d'accord avec les libéraux à ce sujet?

M. Charles Burton: Je ne voudrais pas politiser la question en parlant d'un parti politique, mais je pense que si nous ne tenons pas les diplomates en poste au Canada responsables des activités contraires à leur statut diplomatique, qu'il s'agisse de menaces ou de harcèlement de personnes au Canada, ou de tentatives d'influencer le contenu des journaux canadiens, en particulier dans les médias de langue chinoise, en exerçant des pressions sur les annonceurs et les personnes qui ont peut-être des proches en Chine pour qu'ils ne parlent pas de certains sujets, ou qu'ils en parlent d'une certaine façon... Je crois que ces diplomates devraient être tenus responsables et que nous devrions les déclarer *persona non grata* et accepter les conséquences des expulsions réciproques.

Notre attitude passive à cet égard encourage simplement ces régimes à en faire plus. Je pense que nous devons y mettre fin. Je prévois que c'est ce qui se produira plus souvent en collaboration avec nos alliés, surtout en Europe, dans les prochains mois.

Mme Raquel Dancho: Merci, monsieur Burton.

Ma prochaine question s'adresse à Mme Quaid.

J'aimerais connaître votre point de vue sur le maillon le plus faible de la cybersécurité au Canada. À ma connaissance, nos très grandes entreprises ont une cyberdéfense plutôt solide, mais qu'en est-il de la chaîne d'approvisionnement de certaines de nos grandes sociétés qui travaillent avec les petites et moyennes entreprises? Pouvez-vous nous dire où, selon vous, nous devons renforcer nos défenses en matière de cybersécurité?

Mme Jennifer Quaid: Merci de votre question, madame Dancho.

Vous avez tout à fait raison. Les petites et moyennes entreprises représentent 98 % de notre économie. En fait, elles ne représentent pas seulement la chaîne d'approvisionnement des grandes sociétés, mais l'ensemble de l'économie. Elles sont sans aucun doute notre maillon le plus faible, bien que je déteste utiliser ce terme, car les récentes statistiques indiquent que 44 % d'entre elles n'ont aucune défense contre de possibles attaques cybernétiques.

Bon nombre de nos petites entreprises n'ont pas l'information. Elles n'ont pas l'impression d'être attaquées ou d'être la cible d'attaques. Ce qu'elles ne réalisent pas, c'est que le fait de posséder des données, quelles qu'elles soient, fait qu'elles sont des cibles.

Vous avez tout à fait raison. Quarante-quatre pour cent n'ont aucune forme de cyberdéfense et 60 % n'ont aucune assurance, et nous devons faire plus.

● (1200)

Mme Raquel Dancho: Je vous remercie beaucoup.

Le président: Merci.

J'aimerais maintenant inviter M. Chiang à prendre la parole pour six minutes.

Monsieur Chiang, vous pouvez commencer dès maintenant.

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

Je remercie les témoins d'avoir accepté de partager leur expertise avec nous aujourd'hui.

Ma question s'adresse à M. Doucet.

À votre avis, quelles sont les plus grandes menaces à la cybersécurité nationale du Canada en ce qui concerne la Russie? Quelles mesures proactives peuvent être prises pour éviter les menaces à la sécurité nationale du Canada et à nos infrastructures essentielles? Qu'est-ce que le Canada devrait faire pour se préparer et être en mesure de répondre à une attaque massive de la Russie contre notre cybersécurité?

M. Michael Doucet: Je vous remercie de votre question, qui en comporte, en fait, plusieurs.

Premièrement, d'un point de vue historique — ou quand j'ai commencé ma carrière au gouvernement —, quand nous examinions ces menaces, nous examinions certainement les États-nations, la menace russe, par exemple. Ces menaces étaient gérées par le gouvernement, mais elles n'étaient pas aussi généralisées dans le secteur privé. Aujourd'hui, cette menace contre les Canadiens constitue non seulement un problème de sécurité nationale pour les gouvernements mêmes, mais aussi un problème de sécurité nationale pour les infrastructures essentielles. Nous savons qu'elles n'appartiennent pas pour la plupart à l'État et que, dans beaucoup de cas, elles ne font pas nécessairement l'objet d'une réglementation officielle.

Le point faible, c'est l'inertie, c'est se dire que ce n'est pas la peine d'avoir un programme, de mesurer les risques, qu'on soit une petite, une moyenne ou une grande entreprise.

J'ai bien aimé les observations de Mme Quaid sur les petites et moyennes entreprises, les PME, mais j'aimerais aussi souligner que les grandes entreprises représentent potentiellement une cible plus lucrative pour ceux qui se livrent à des cyberattaques. Par conséquent, une menace persistante avancée, comme celle de la Russie, ou d'autres menaces qui engagent la responsabilité de certains États, est vraiment difficile à gérer. Nous devons être vigilants à 100 %, pas seulement à l'intérieur de l'organisation, mais avec tous les fournisseurs quand nous pensons aux menaces de tierces parties lorsque nous passons à d'autres plateformes, par exemple. C'est très important.

Maintenant, la question à un million ou peut-être à un milliard de dollars est, en fait, que faisons-nous face à cette menace? J'attirerai l'attention sur le rapport que le Comité des parlementaires sur la sécurité nationale et le renseignement a déposé assez récemment. Il y avait un cadre et des activités pour défendre les systèmes et réseaux du gouvernement. Le rapport a été déposé en février. C'est un rapport détaillé qui vaut la peine d'être lu. Soit dit en passant, toutes les recommandations ont été acceptées.

Le comité y soulève quelques questions, l'une étant ainsi formulée — et je cite le rapport mot pour mot —: « Les organisations protégées : des opinions divergentes. » À dire vrai, nous devons régler ce problème, du point de vue de la responsabilité comme de la reddition de comptes, mais nous devons aussi savoir quelles sont ces opinions divergentes. C'est très important pour nous.

Le rapport dit, par ailleurs, que les lacunes représentent une menace évidente. Nous savons que nous avons des lacunes. Il ne s'agit pas de montrer quiconque du doigt, mais nous savons qu'elles existent et que nous devons tout faire pour y remédier. Nous devons le faire de manière pragmatique lorsqu'il s'agit de menaces importantes.

La cybersécurité n'est pas, selon moi, une affaire de sommes dépensées, parce qu'on peut y consacrer des sommes colossales. Cela ne fait aucun doute. Encore une fois, la cybersécurité est une sorte de sport d'équipe et une question de dépenses faites là où il faut pour arriver au meilleur résultat pour les systèmes gouvernementaux, les systèmes des infrastructures essentielles ou les systèmes partagés.

Est-ce que cela vous aide, monsieur?

M. Paul Chiang: Merci beaucoup.

Pour aller plus loin, faudrait-il une réglementation pour garantir la cybersécurité au Canada, une réglementation pour le gouvernement, le secteur privé et le secteur public? Pensez-vous qu'il faudrait une réglementation?

Selon vous, que devrions-nous faire pour combler les lacunes que vous mentionniez?

● (1205)

M. Michael Doucet: Nous pouvons parler de la responsabilité de la réglementation.

Personnellement, je préfère ne pas trop réglementer. Pour revenir encore aux PME, ont-elles les ressources nécessaires pour s'adapter à la réglementation? C'est sans doute plus une question d'environnement favorable, d'environnement de communication. Qu'il s'agisse d'une petite ou d'une grande organisation, ou d'un propriétaire qui a un réseau chez lui, ce que nous avons tous, il existe de précieuses ressources, de Sécurité publique Canada à la GRC, et d'autres encore, pour nous aider à sécuriser nos systèmes. Pour les PME, ces ressources peuvent se révéler très utiles.

Pour ce qui est de combler les lacunes, franchement, il est possible de les combler, mais il faut les comprendre. Il faut comprendre quelles sont les lacunes, leurs conséquences, et il faut savoir qui veut vous nuire.

Je vous donnerai un exemple. Prenons le secteur financier par rapport au secteur agricole. Il peut y avoir différents auteurs de menaces qui s'en prennent à l'un ou à l'autre. Les éléments perturbateurs qui veulent seulement créer des perturbations s'en prendront à n'importe qui. Il faut repérer ses lacunes et y remédier.

La mauvaise nouvelle, c'est que le monde autour de nous évolue. Il change pendant qu'on remédie aux lacunes. Si j'évalue un système aujourd'hui, ou un système de systèmes, et qu'il me faut deux ans pour remédier aux lacunes relevées, ce qui n'est pas déraisonnable, quelles autres lacunes apparaîtront dans ce laps de temps, et comment faire pour me rendre utile et améliorer sans arrêt le programme?

Le président: Je vous remercie.

Je donne maintenant la parole à Mme Michaud pour six minutes.

Je me réjouis de vous revoir parmi nous. J'espère que vous vous sentez mieux. Bon retour au Parlement.

[*Français*]

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

Je suis heureuse d'être de retour, même si ma voix est encore un peu enrouée.

Je remercie les témoins d'être avec nous aujourd'hui, c'est très agréable de les voir en personne.

Monsieur Burton, vous êtes assurément un spécialiste de la Chine. Je vais vous poser quelques questions à cet égard un peu plus tard.

Dans votre allocution d'ouverture, vous avez dit que le Canada était inadéquatement préparé à réagir aux menaces en matière de sécurité ou de cybersécurité et qu'il était moins préparé que ses alliés.

Selon vous, qu'est-ce qui explique cela? S'agit-il d'un manque d'investissement d'une année à l'autre?

Que pouvons-nous faire pour nous rattraper?

Compte tenu de ce qui se passe en Ukraine, est-il trop tard ou avons-nous suffisamment de temps pour nous préparer adéquatement?

[*Traduction*]

M. Charles Burton: Par rapport à d'autres pays, le Canada se montre moins proactif pour ce qui est de poursuivre ou de dénoncer des éléments qui se livrent à du cyberespionnage. Les États-Unis ont identifié un certain nombre d'agents de l'armée de la République populaire de Chine qui se livraient à ce type d'activités.

Nous hésitons généralement à réagir, notamment avec les Chinois, en ce qui concerne des activités comme le cyberespionnage, le bâillonnement des médias en chinois ou, en fait, le harcèlement de personnes qui souhaiteraient peut-être s'exprimer. Elles sont harcelées soit par des agents chinois directement, soit de diverses manières sur Internet.

Il en est ainsi parce que le gouvernement cherche en priorité à promouvoir la prospérité dans nos relations avec la Chine et est prêt à tolérer ces sortes d'activités parce que le coût serait élevé pour la prospérité des entreprises canadiennes et du Canada.

Le gouvernement chinois a bien fait comprendre que si le Canada réprimait ce type d'activités des agents de l'État chinois au Canada ou les perturbations des réseaux informatiques, nous perdrions des contrats. Vous vous rappelez sans doute le piratage des données aérospatiales du CNRC ou, avant cela, le piratage du Conseil du Trésor ou d'autres ministères. À ce que j'ai entendu dire, ils étaient attribuables à l'État chinois, mais la Chine ne subit aucune conséquence à la suite de cette sorte d'activités.

C'est vraiment une question de volonté politique, et ce serait bien si le Comité commençait à comparer les politiques de pays d'optique commune, notamment des États-Unis, du Royaume-Uni et de l'Australie, en ce qui concerne ce genre d'activités. Nous sommes dans une situation tellement grave que je pourrais dire que le Groupe des cinq est réduit à trois.

Prenons le Dialogue quadrilatéral pour la sécurité. Le Canada n'en fait pas partie. Prenons l'activité de l'Australie, du Royaume-Uni et des États-Unis dans la région indo-pacifique, pour autant que je sache, le Royaume-Uni n'est pas un pays de l'Asie-Pacifique, contrairement au Canada. Alors, pourquoi les États-Unis et la Grande-Bretagne ont-ils décidé de ne pas nous inclure dans les récentes consultations entre les États-Unis et le Royaume-Uni sur Taïwan, de même que le Japon? Une partie de notre pays est plus proche géographiquement de la Chine que l'Australie. Pourquoi sommes-nous exclus?

Je pense que c'est parce que nous ne faisons pas notre part pour ce qui est de contrer les menaces à la sécurité publique et à la sécurité nationale, et nos alliés estiment que nous ne sommes plus des partenaires fiables, de même que la Nouvelle-Zélande, mais pour d'autres raisons. J'en suis tout à fait désolé, mais je ne crois pas qu'il soit trop tard. C'est le Parlement du Canada. Nous pouvons redresser la situation.

● (1210)

[*Français*]

Mme Kristina Michaud: Justement, vous avez mentionné les États-Unis, l'Australie et le Royaume-Uni.

Y a-t-il de bonnes pratiques qui sont mises en place par d'autres pays en ce moment et dont le Canada pourrait s'inspirer pour protéger les infrastructures essentielles et prévenir les cyberattaques?

[*Traduction*]

M. Charles Burton: Oui, si vous prenez le Royaume-Uni l'an dernier, il a expulsé trois espions qui se faisaient passer pour des journalistes travaillant au Royaume-Uni. Il a révélé qu'une agente de l'État chinois, Christine Lee, faisait de généreux dons à certains politiciens qui, ensuite, on l'imagine, faisaient passer les intérêts de la Chine avant ceux de leur propre pays.

Les États-Unis se préoccupent beaucoup plus de la fuite de hautes technologies qui faciliteraient l'utilisation d'une technologie à double usage à des fins militaires ou de technologies qui faciliteraient le cyberespionnage à partir d'universités. Le Canada ne réagit pas à des choses comme le rapport de l'Australian Strategic Policy Institute qui a révélé que des chercheurs de l'armée de la République populaire de Chine travaillent dans des domaines de technologie sensibles dans des universités canadiennes. Ils étaient entrés au Canada sous de faux prétextes en ne révélant pas leur statut d'officiers, et cela continue.

Pourquoi n'avons-nous pas fait plus au sujet de l'affaire Michael Chan en Ontario? Le Service canadien du renseignement de sécurité a dit qu'il avait eu souvent des contacts avec le consul général chinois, mais nous ne savons pas de quoi ils se parlaient. Il est important que le Parlement le sache.

Le président: Je vous remercie.

Je donne maintenant la parole à M. MacGregor pour six minutes.

Monsieur, vous avez la parole.

M. Alistair MacGregor (Cowichan—Malahat—Langford, NPD): Je vous remercie, monsieur le président.

Comme mes collègues, je remercie les témoins de comparaître devant le Comité afin de nous aider dans cette étude.

Monsieur Burton, je commencerai par vous.

Vous avez parlé dans vos observations préliminaires de la relation entre le Service canadien du renseignement de sécurité, la GRC et le Centre de la sécurité des télécommunications, le CST, ainsi que du fait que le Parlement du Canada ne sait pas toujours vraiment ce que ces différents organismes de sécurité nationale font.

Je tiens à préciser à ce propos que la loi qui a autorisé le Comité des parlementaires sur la sécurité nationale et le renseignement doit faire cette année l'objet d'un examen législatif. Il me semble que cet examen se prête à notre étude actuelle, car, comme vous le disiez, nous sommes malheureusement mal préparés à contrer bon nombre des menaces à la sécurité.

Que recommanderiez-vous d'inclure dans cet examen? Le modèle actuel de surveillance parlementaire joue-t-il son rôle? Qu'aimeriez-vous voir fait différemment? Y a-t-il d'autres modèles, par exemple au Congrès des États-Unis ou au Parlement du Royaume-Uni, dont nous devrions nous inspirer?

M. Charles Burton: La réponse est oui. En particulier, l'Australie, le Royaume-Uni, les États-Unis et aussi les pays scandinaves ont beaucoup à nous apprendre pour ce qui est de bien faire la distinction entre ne pas révéler d'informations qui représenteraient une menace pour la sécurité nationale du Canada et ne pas dire quand l'organisme de sécurité ne protège pas, en fait, ses propres insuffisances dans l'exécution de ses tâches telles qu'elles sont décrites dans les mandats des ministres qui les supervisent.

Au Canada, à mon avis, il est beaucoup trop poliment convenu avec les organismes de sécurité qu'ils ne peuvent pas vous dire telle ou telle chose. Il s'agit, selon moi, d'une question culturelle. À dire vrai, j'ai l'impression que, dans une certaine mesure, ils regardent de haut les comités parlementaires et font le maximum pour vous en dire le moins possible de crainte que, si vous découvriez quelque chose, leur réputation en soit ternie ou des évaluations passées soient remises en question.

Je suis d'avis qu'il faut être davantage convaincus que les parlementaires gardent le secret. Nous devons examiner les types de comités parlementaires ou du congrès qui existent ailleurs. Nous devons faire de notre mieux pour voir s'il est possible de faire en sorte que les comités canadiens soient plus à même d'éclairer les décisions sur les mesures législatives à prendre en comprenant parfaitement ce qui se passe.

Je ne crois pas que l'affaire Cameron Ortis serait étouffée aussi longtemps dans un autre pays, ou que Quentin Huang, qui aurait transféré des technologies militaires à l'État chinois...

● (1215)

M. Alistair MacGregor: Je suis désolé de vous interrompre, monsieur Burton, mais j'ai peu de temps et je souhaite entendre Mme Quaid.

Madame Quaid, vous avez mentionné dans vos observations préliminaires que la cybercriminalité paie et que les cryptomonnaies facilitent le paiement. Vous savez certainement que les cryptomonnaies sont un sujet d'actualité sur la scène politique canadienne depuis plusieurs semaines.

Le professeur Robert Huebert a comparu devant le Comité. Il dit que les crimes financiers sont difficiles à évaluer au Canada à cause du manque de transparence et de visibilité des transactions financières dans notre pays. Selon lui, il faut plus de transparence.

Que souhaiteriez-vous que le Comité recommande précisément, compte tenu de cette remarque et aussi par rapport aux cryptomonnaies? Sur quoi le gouvernement fédéral doit-il mettre plus l'accent pour augmenter la transparence et la visibilité?

Mme Jennifer Quaid: Je suggérerais de commencer par des dispositions législatives d'exonération. Il faut que ce soit plus facile pour les organisations victimes d'attaques, quelle qu'en soit la méthode, de non seulement les signaler, mais aussi de rapporter ce qui s'est passé. Cela rend les menaces transparentes et aide d'autres organisations. Pour faire écho aux propos de M. Doucet, il s'agit d'un sport d'équipe. Si nous nous informons mutuellement de ce qui nous arrive et des moyens utilisés pour pénétrer nos systèmes, nous empêcherons d'autres attaques.

Je crois que c'est la chose la plus facile à faire, adopter des dispositions d'exonération.

Quant aux cryptomonnaies, ce sont les banques qui pourraient vous répondre. Il n'y a pas de transparence en la matière. C'est la nature même de la chose. Il est très difficile de savoir qui a été payé, combien, par qui et à quel moment.

M. Alistair MacGregor: Pour conclure, monsieur Doucet, vous avez déclaré que la cybersécurité, ce n'est pas tant une affaire de moyens financiers qu'un sport d'équipe et qu'il existe des ressources.

Étant donné l'augmentation du financement du CST annoncée dans le budget — une somme importante —, que pensez-vous que notre comité devrait recommander sur la manière d'utiliser cet argent? Êtes-vous satisfait de l'affectation prévue des fonds? Voulez-vous plus de précisions? Votre opinion m'intéresse.

M. Michael Doucet: Je vous remercie de ces questions.

Pour ce qui est des fonds alloués au CST, je m'intéresserais aux résultats en ce qui concerne la cybersécurité canadienne — des résultats concrets dans ses secteurs d'activité, c'est-à-dire dans presque tout le pays.

Le président: Je suis désolé, monsieur. Il vous reste 10 secondes.

M. Michael Doucet: Je pense que nos dépenses doivent être axées sur les résultats. Je pense aussi que nous devons faire très attention à adapter l'organisation en fonction des menaces actuelles et futures et non du passé.

Le président: Merci beaucoup.

M. Michael Doucet: Merci.

Le président: Chers collègues, passons à la deuxième série de questions. Nous aurons suffisamment de temps pour tous les partis. Il y aura quatre interventions et nous commencerons par M. Van Popta.

Monsieur, vous avez cinq minutes. Allez-y dès que vous êtes prêt.

● (1220)

M. Tako Van Popta (Langley—Aldergrove, PCC): Merci, monsieur le président.

Je remercie tous les témoins de leur présence et de nous faire profiter de leur sagesse et de leurs connaissances.

Je commencerai par vous, monsieur Burton.

Dans votre témoignage, en réponse à une question précédente, vous avez mentionné que la GRC, le SCRS et le CST, le Centre de la sécurité des télécommunications, détiennent de l'information, mais se montrent généralement évasifs avec nous. Vous demandez comment nous pouvons, en tant que parlementaires, nous préparer à des menaces si ces organismes ne nous informent pas.

On nous dit, au Parlement, que c'est précisément la raison d'être du CPSNR — le Comité des parlementaires sur la sécurité nationale et le renseignement. Que pensez-vous de l'efficacité de ce comité?

M. Charles Burton: Je suis d'avis qu'il vaudrait mieux que ces questions soient examinées par un comité du Parlement — des personnes détenant une cote de sécurité —, avec peut-être quelques séances à huis clos, non publiques. Je préférerais que cela fasse partie du processus parlementaire normal. Je ne connais pas d'autre pays qui ait un processus comparable au nôtre et je me demande s'il peut être aussi efficace que les comités d'autres parlements pour ce qui est de garantir que les organismes chargés de la sécurité publique et de la sécurité nationale rendent des comptes au Parlement et fournissent aux parlementaires l'information dont ils ont besoin pour rédiger ou modifier des lois afin de mieux contrer les menaces.

Nos lois sur le transfert à des pays étrangers de technologies classifiées en sont un exemple. J'ai eu le privilège de préparer quelques dossiers avec la GRC à ce sujet. Quand les dossiers ont été transmis au ministère de la Justice — dans les deux cas que je connais —, rien n'a été fait parce que nos lois sont trop faibles et parce qu'il a été conclu qu'il serait impossible de faire rendre des comptes aux personnes soupçonnées d'avoir trahi notre pays en transmettant des technologies classifiées aux agents d'un État étranger.

Les lois d'autres pays qui ont plus de succès à cet égard sont plus fermes que les nôtres. Les Britanniques et les Américains traitent des dizaines de cas par an. Quand avez-vous entendu parler pour la dernière fois de quelqu'un qui a été accusé de trahison au Canada? À ma connaissance, ce n'est jamais arrivé. C'est un problème, car cela signifie que notre pays est considéré comme un bon endroit pour qui veut profiter de nos technologies de pointe, par des moyens légitimes ou pas, et il ne devrait pas en être ainsi.

M. Tako Van Popta: Je vous remercie, monsieur Burton.

Monsieur Doucet, je vous pose aussi la question pour savoir si vous avez un autre point de vue sur l'efficacité ou l'utilité du CPSNR en lieu et place d'autres comités qui reçoivent des rapports.

M. Michael Doucet: Certainement, et merci. J'avais bien peur que vous me posiez cette question. J'ai passé la majorité de ma carrière fédérale au sein de cette communauté, alors je vous donnerai une perspective un peu différente.

Sans vouloir vous offenser, je n'accuserais pas nécessairement la communauté de se montrer évasive. Toutefois, je l'accuserais peut-être de surclassifier l'information. Je crois que c'est une question de culture organisationnelle.

Quand j'ai rejoint les rangs du CST le 2 avril 1988, je n'avais pas le droit de dire à ma famille combien de personnes y travaillaient. Il y avait tellement de choses que nous… Nous étions derrière un rideau de fer. Il y avait cette sorte de chape de secret, la notion du « besoin de savoir ». Appelez cela comme vous voulez. La communauté doit mûrir à cet égard.

Si nous voulons vraiment mobiliser les infrastructures essentielles, les acteurs de ces infrastructures peuvent obtenir des cotes de sécurité. Nous pouvons leur fournir de l'information classifiée. Le gouvernement peut faire cela. C'est possible. Nous devons déclassifier au besoin. Disposer d'informations utiles sur des menaces sans pouvoir agir n'est pas une situation idéale. Voilà ce que je pense.

Pour ce qui est du Comité des parlementaires sur la sécurité nationale et le renseignement, je peux vous dire que, personnellement, j'ai sauté de joie quand il a été créé. Pour moi, c'était un formidable pas en avant. C'était bien pour nous et bien pour le Canada. Est-ce qu'il faut y apporter de légères modifications avec le temps? C'est possible, mais cela demeure une très bonne structure pour le Parlement.

Le président: Monsieur, il vous reste 10 secondes et vous les redonnez au Comité. Nous vous remercions chaleureusement de votre générosité.

Passons tout de suite à Mme Damoff.

Vous avez cinq minutes. Allez-y dès que vous êtes prête.

● (1225)

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

Merci à tous les témoins.

Monsieur Burton, c'est toujours un plaisir de vous voir et je vous remercie de votre présence aujourd'hui. Dans votre témoignage, vous avez parlé de la relation entre la Chine et la Corée du Nord. L'isolement de la Russie n'est pas près de se terminer. Je crois que vous avez aussi mentionné que la Russie et la Chine se rapprocheront davantage et que la Russie deviendra dépendante de la Chine.

Que recommanderiez-vous au gouvernement canadien pour garantir la sécurité de nos infrastructures essentielles dans le contexte de ce rapprochement entre la Russie et la Chine?

M. Charles Burton: Je crois que nous avons fait une bonne chose. J'ai été très heureux de la place réservée aux minéraux critiques dans le budget du gouvernement. À mesure que la situation évoluera, et parce que je crois que la Russie resserrera son alliance avec la Chine, il sera difficile pour nous d'imposer des sanctions secondaires à la Chine si elle fait avec la Russie ce qu'elle fait avec la Corée du Nord, c'est-à-dire faciliter le contournement des sanctions que nous imposons à la Russie pour essayer de l'amener à se conformer aux normes de l'ordre international fondé sur les règles. Ce sera plus difficile.

Si le monde se divise en deux camps, celui des autocraties et des pays avec lesquels la Russie et la Chine peuvent créer diverses alliances… La Chine sait très bien s'y prendre pour rallier le soutien de pays membres des Nations unies qui bénéficient de son programme d'infrastructures de La Ceinture et la Route. Si nous nous trouvons dans ce genre de situation, il est important de veiller à ce que nos chaînes d'approvisionnement soient une question de sécurité nationale, de sorte que nous soyons à l'abri de toute coercition de la part de pays qui nous menaceraient, si nous contrarions leurs objectifs politiques dans notre pays, de ne pas nous fournir l'élément dont nous avons besoin. Nous l'avons vu avec les sanctions de la Chine sur le canola et la viande au moment du fiasco de l'arrestation de Meng Wanzhou et lors de l'incarcération totalement injustifiée et brutale de Michael Kovrig et Michael Spavor.

Nous devons examiner la situation sérieusement. Nous devons examiner les évaluations du SCRS: elles sont essentielles pour que vous compreniez ce que le Canada doit faire. Ce ne sera pas sans coût. Il est inutile de prétendre que cela n'arrive pas, car cela arrive bel et bien. Nous devons faire les choix difficiles qui sont nécessaires pour protéger notre pays et, par conséquent, d'autres pays qui sont des alliés qui partagent nos vues.

Mme Pam Damoff: Merci, monsieur Burton.

Monsieur Doucet et madame Quaid, les États-Unis envisagent de rendre obligatoire de signaler toute attaque contre des infrastructures essentielles et je me demande si vous pensez que le Canada devrait faire la même chose.

Avant que vous répondiez, monsieur Doucet, vous avez mentionné que vous espériez formuler plusieurs recommandations au Comité dans votre témoignage. Si vous pouviez nous les fournir par écrit, si vous n'avez pas pu le faire durant votre témoignage, ce serait fantastique.

Monsieur Doucet, peut-être pouvons-nous commencer par vous.

M. Michael Doucet: Bien sûr. Je serais certainement en faveur de la déclaration obligatoire pour certains intervenants des infrastructures critiques; quand on considère les 10 secteurs qu'englobent les infrastructures critiques, ce sont de très grands secteurs, et l'agriculture en fait partie. Allons-nous exiger une déclaration obligatoire de la part d'un producteur laitier possédant un troupeau de 60 bêtes? Il faut user de prudence.

Cela dit, si nous implantons un régime de déclaration obligatoire, il faut absolument s'assurer de protéger la déclaration, la source de la déclaration, les actions postérieures à la déclaration, etc., et trouver un moyen de diffuser ces renseignements à l'échelle nationale, parce que nous voulons tout d'abord éviter que l'information communiquée par les organisations qui signalent des bris de sécurité soit réacheminée là où il ne faut pas. Une fois ces renseignements regroupés, cela fait beaucoup d'information.

Mme Pam Damoff: Je n'ai plus qu'une vingtaine de secondes. Je suis désolée, madame Quaid.

Voulez-vous intervenir?

Mme Jennifer Quaid: Certainement. La déclaration obligatoire est un bon concept. Elle aide clairement le gouvernement à comprendre l'ampleur de la menace, mais à défaut de diffuser l'information tirée de cette déclaration obligatoire à l'ensemble de l'économie pour l'aider à se défendre contre cette même menace, alors la même chose se reproduira encore et encore. Il ne sert à rien...

● (1230)

Le président: Merci beaucoup.

J'inviterais maintenant Mme Michaud à poursuivre l'échange.

Vous avez deux minutes et demie.

[*Français*]

Mme Kristina Michaud: Je vous remercie, monsieur le président.

Monsieur Doucet, on sait que les cyberattaques sont en hausse depuis quelques années déjà et que la situation a été exacerbée par le conflit en Ukraine. D'ailleurs, c'est ce que nous apprend le Service canadien du renseignement de sécurité.

Vous avez parlé de recommandations que vous aimeriez faire au gouvernement, non seulement pour protéger nos institutions gouvernementales, mais aussi pour protéger les entreprises privées qui peuvent avoir une incidence importante au Canada.

Quelles sont ces recommandations que nous pourrions présenter au gouvernement?

[*Traduction*]

M. Michael Doucet: Je recommanderais tout d'abord au gouvernement, en tant qu'intervenant des infrastructures critiques, de bien faire les choses, de se pencher sur la série de rapports à ce sujet et d'y affecter une équipe-choc, et d'examiner comment s'y prendre pour mieux protéger l'infrastructure gouvernementale.

Comme je l'ai mentionné plus tôt, le Comité a produit un rapport très largement accepté, qui couvre 169 organisations fédérales. D'après moi, la première étape consisterait à comprendre les principales menaces qui pèsent sur chacune de ces 169 organisations pour nous assurer qu'elles déclarent ces menaces, qu'elles cernent les lacunes et qu'elles déterminent comment elles vont combler ces lacunes.

Je pense qu'on peut très difficilement approcher les fournisseurs d'infrastructures critiques pour leur dire comment procéder, si on ne le fait pas soi-même. Le financement, les équipes et les individus sont là pour ça d'après moi. Les équipes interministérielles n'ont pas toujours un fonctionnement harmonieux. Les membres viennent de cultures différentes, ils ont des mandats différents, mais je crois qu'il faut vraiment s'assurer de le faire.

En premier lieu, le gouvernement doit bien faire les choses.

Ensuite, bien sûr, nous devons examiner la manière dont nous fournissons, dont le gouvernement fournit, des conseils et des orientations aux fournisseurs d'infrastructures critiques et aux autres parties concernées. Je voudrais vraiment qu'on se penche sur le nombre d'organisations qui supportent des cyberenvironnements, comme l'Échange canadien de menaces cybernétiques, l'ECMC, et d'autres, et sur la façon dont nous pouvons harmoniser ce niveau d'appui à la population et aux infrastructures canadiennes.

Si je dis cela, c'est parce qu'il existe une multitude d'organisations. Certains agents de sécurité se demandent vraiment à qui ils devraient s'adresser, parmi cette multitude. Où peuvent-ils obtenir ces précieux renseignements, et auprès de quel partenaire de confiance? Voilà quelques-unes de mes recommandations.

Le président: Merci beaucoup.

Monsieur MacGregor, vous conclurez les échanges avec ce groupe de témoins. Vous avez deux minutes et demie.

M. Alistair MacGregor: Merci, monsieur le président.

Monsieur Doucet, j'aimerais poursuivre avec vous. Vous avez parlé de l'agriculture. C'est en fait le deuxième secteur dont je suis le critique. Je connais le rythme vertigineux des progrès technologiques dans l'agriculture. De nombreuses machines sont utilisées dans l'agriculture moderne, l'agriculture de précision. Je pense notamment à la technologie des chaînes de blocs. Les machines sont désormais en mesure de communiquer avec la société mère, et les agriculteurs ont accès à des données en temps réel non seulement sur la croissance de leurs cultures, mais également sur les dosages appropriés de pesticides et d'engrais à épandre.

Dans la foulée de ce que vous avez dit à Mme Michaud, pouvez-vous nous parler de certaines des vulnérabilités présentes dans les champs agricoles du Canada? Nous pouvons peut-être faire quelques recommandations à cet égard, parce que l'agriculture est un pilier de notre économie et que nous avons de grands projets pour développer encore ce secteur. Le Canada est un acteur de premier plan sur la scène agricole mondiale.

M. Michael Doucet: Exactement. Merci pour cette question.

J'ai un fils qui habite la Saskatchewan, et pour cette raison je m'intéresse vraiment au secteur agricole, dont l'importance est manifeste quand on parcourt les régions rurales de cette province. C'est évident quand on regarde l'agriculture moderne.

Je dirais que l'agriculture moderne, à l'échelle où elle est actuellement pratiquée au Canada... et évidemment, il y a de nombreux capteurs dans les champs. L'agriculteur moderne utilise maintenant les technologies opérationnelles plutôt que le tracteur et la charrue. Il y a les données, il y a les données critiques, et il y a aussi les données qui, si elles étaient manipulées, pourraient vraiment influencer les résultats de l'entreprise agricole.

Je pense que pour l'agriculteur canadien sophistiqué, il doit travailler en partenariat avec les fournisseurs de biens et de services agricoles. Il faut tenir compte de ce qu'on appelle le risque de tierce partie, et de la façon dont il pourrait toucher votre organisation, toucher votre exploitation agricole.

Qu'est-ce qu'il faut chercher? Je crois qu'il faut chercher la valeur. Il faut poser exactement les questions qu'on pose aux fournisseurs. Pour les grands agriculteurs, ils doivent chercher à s'associer avec les autres acteurs qui les aideront à prendre ces décisions, car ils sont très vulnérables du point de vue de ce qu'on appelle la technologie opérationnelle.

● (1235)

Le président: Merci beaucoup. Nous sommes rendus à la fin du groupe de témoins et à la fin de la séance. Encore une fois, nous nous excusons de ce début tardif. C'est notre réalité maintenant. Le Comité vous remercie grandement de votre sagesse et du temps que vous nous avez consacré. C'est un travail très important.

Au nom de l'ensemble du Parlement, je vous remercie de votre témoignage et de votre contribution à ce processus démocratique.

Chers collègues, nous passerons très rapidement au prochain groupe de témoins. Le greffier me dit que c'est dans moins de cinq minutes. On se revoit très bientôt.

● (1235)

(Pause)

● (1240)

Le président: Nous sommes prêts à commencer. Nous procéderons de la même manière qu'avec le premier groupe de témoins, soit un premier tour de table complet et ensuite les quatre premiers intervenants du deuxième tour.

La séance est ouverte. Durant cette deuxième heure, nous entendrons M. Frédéric Cuppens, professeur à Polytechnique Montréal, Mme Nora Cuppens, professeure à Polytechnique Montréal, et M. Jonathan Paquin, professeur titulaire au Département de science politique de l'Université Laval, qui disposeront chacun de cinq minutes pour leur exposé.

Nous pouvons commencer immédiatement. Je prierais le professeur Cuppens de commencer. Lequel, me demanderez-vous? Allons-y avec M. Frédéric Cuppens, pour cinq minutes.

Quand vous voudrez.

[*Français*]

M. Frédéric Cuppens (professeur, Polytechnique Montréal, à titre personnel): C'est madame Cuppens qui commencera.

Mme Nora Cuppens (professeure, Polytechnique Montréal, à titre personnel): Bonjour à tous.

Je vais commencer, puisque mon collègue Frédéric Cuppens et moi avons préparé une présentation commune.

Merci à tous de nous accueillir à ce comité. Je vais présenter le contexte et M. Cuppens vous donnera quelques recommandations.

Le contexte, nous le connaissons tous. Il s'agit, d'une part, de l'invasion de l'Ukraine par la Fédération de Russie et, d'autre part, de l'aide apportée par les pays occidentaux et l'Organisation du traité de l'Atlantique Nord, ou OTAN, aux Ukrainiens pour pallier cette invasion. Maintenant, on se demande si on doit craindre des représailles sous forme de cyberattaques. En d'autres mots, la guerre qui se passe sur le terrain va-t-elle se déplacer vers le cyberespace?

La Russie a démontré sa capacité à mener une cyberguerre avec des groupes de cyberattaquants très organisés. Nous en connaissons et en avons identifié plusieurs. Il y a APT28, qui a mené une cyberattaque contre TV5 Monde, APT29, une autre organisation plutôt russe, notamment connue pour son ingérence dans les élections américaines de 2016, l'unité de renseignement militaire russe 74455, qui a mené des cyberattaques contre des infrastructures critiques à l'aide des logiciels BlackEnergy et Industroyer, ainsi que le groupe Conti, que l'on connaît notamment pour son affiliation au rançongiciel Ryuk.

Rappelons que, bien avant le déclenchement de l'attaque militaire contre l'Ukraine, les tensions entre les États-Unis et la Russie étaient extrêmement élevées. À la suite de l'attaque contre la société SolarWinds, le président Biden avait qualifié le président Poutine de tueur. Il a utilisé d'autres qualificatifs depuis. Les cyberattaques venant de la Russie risquent donc de se multiplier et de s'intensifier, visant particulièrement ceux qui aident les Ukrainiens, comme les pays occidentaux, dont fait partie le Canada. Quelles sont les cibles et les menaces? C'est la question que nous nous posons. Les formes que peut prendre cette cyberguerre sont très diverses, les plus connues étant l'exfiltration de données, les attaques par déni de service, la fraude et, bien évidemment, le sabotage.

Aujourd'hui, ce qui est le plus visible et qui est une forme de la cyberguerre, c'est la guerre de l'information, donc la désinformation. Il faut s'attendre à ce que cette guerre de l'information continue et à ce que les fausses nouvelles pullulent. Cependant, plusieurs experts s'accordent pour dire que les effets de ces cyberattaques sont, pour le moment, limités. Peu après le début du conflit en Ukraine, on a vu le groupe Conti, dont j'ai parlé tout à l'heure, revendiquer l'attaque informatique contre l'aluminerie Alouette, dont vous avez sûrement entendu parler. La semaine dernière, il y a aussi eu l'attaque contre Rideau Hall, qui a eu un effet très symbolique, mais pour le moment, l'implication de la Russie dans cette attaque n'est pas vraiment confirmée.

On peut désormais se poser la question suivante: pourquoi la Russie n'a-t-elle encore lancé aucune cyberattaque majeure?

Nous n'avons pas la réponse, mais nous pouvons formuler deux hypothèses. La première est que, comme une guerre traditionnelle, une cyberguerre se prépare. On a vu que la préparation sur le terrain est un peu chaotique. La Russie n'avait peut-être pas préparé la cyberguerre, ou elle attend peut-être le bon moment pour la lancer. La deuxième, c'est que le déclenchement d'une cyberattaque massive par l'un des deux camps serait sans doute vu comme un franchissement de la fameuse ligne rouge, ce qui conduirait inévitablement à une escalade conflictuelle.

Les infrastructures critiques sont donc une priorité. On peut craindre particulièrement des attaques par sabotage de ces infrastructures. Il va sans dire que notre éloignement géographique n'entre pas en ligne de compte en matière de cybermenaces. Certains experts n'ont d'ailleurs pas hésité à comparer l'arme cybernétique à l'arme nucléaire comme arme de dissuasion, comparant le pouvoir des cyberattaques à celui que pourrait avoir une bombe atomique.

Dans ce contexte, on peut d'ailleurs souligner deux contre-vérités qui sont très fréquemment répandues. La première, c'est qu'une infrastructure qui n'est pas connectée à Internet est protégée des cyberattaques par ce que l'on appelle généralement l'isolement physique. C'est faux, et on le sait parfaitement depuis les attaques par le ver Stuxnet, qui ciblaient des centrales nucléaires.

La deuxième contre-vérité est qu'un scénario de liquidation à la *Die Hard 4* , qui aurait pour objectif de ruiner économiquement un pays...

● (1245)

Le président: Il vous reste 10 secondes.

Mme Nora Cuppens: D'accord.

C'est du cinéma, mais c'est également faux. Toutes les étapes du scénario sont donc possibles et réalisables.

[*Traduction*]

Le président: Merci beaucoup.

[*Français*]

Mme Nora Cuppens: Je donne maintenant la parole à M. Cuppens, qui va présenter nos recommandations.

[*Traduction*]

Le président: Merci.

J'accorde maintenant cinq minutes à M. Cuppens pour présenter son exposé.

Vous avez la parole, monsieur.

[*Français*]

M. Frédéric Cuppens: Un scénario de liquidation comme celui présenté dans le film est malheureusement tout à fait envisageable. On parle d'attaques contre le trafic routier, le trafic aérien, les systèmes de télécommunications, les médias, les systèmes de distribution d'énergie, les systèmes financiers, la Bourse. Il y a déjà eu des exemples dans le monde pour illustrer la possibilité de ces cyberattaques. Nous considérons que c'est juste une question de préparation et de moyens pour mettre en œuvre ce genre d'attaques de grande ampleur. Naturellement, c'est compliqué pour des individus isolés, mais, à l'échelle d'un pays, cela devient malheureusement tout à fait envisageable.

Dans ce contexte, nous formulons certaines recommandations. Il y a naturellement des recommandations de base. La première recommandation est d'arrêter d'utiliser les logiciels provenant de la Russie, notamment quand il s'agit de logiciels de sécurité. Plusieurs pays ont déjà recommandé d'arrêter l'utilisation d'un célèbre fabricant russe d'antivirus.

Selon la deuxième hypothèse, les cyberattaques peuvent provenir de n'importe où dans le monde, pas seulement de la Russie. Par exemple, récemment, il a été démontré que le groupe Conti avait à sa tête une jeune fille de 12 ans, qui habitait au Mans, en France.

Ensuite, il est absolument nécessaire d'élever globalement le niveau de sécurité de l'ensemble du Canada. Cela passe par une mobilisation générale de l'ensemble des ressources pour pouvoir faire face aux cyberattaques et aux besoins urgents pour ce qui est de fédérer et de coordonner les expertises en cybersécurité sur les plans industriel, universitaire et gouvernemental.

Nous suggérons également une prise en main par le pouvoir régalien des choses relevant de la cybersécurité des infrastructures critiques. C'est ce qu'ont déjà fait plusieurs pays et c'est ce qu'a fait la France avec la Loi de programmation militaire 2019-2025.

En ce qui nous concerne, à Polytechnique, nos efforts portent à la fois sur la recherche et sur la formation. Quant à la formation, il est extrêmement important de développer un programme qui s'adresse aux formations initiales, soit le baccalauréat et la maîtrise, mais aussi à la formation continue en mettant en place des certificats et des microprogrammes, ainsi qu'un programme de perfectionnement pour les formations courtes de un à cinq jours.

Pour ce qui est de la recherche, nous croyons beaucoup à la nécessité de développer les travaux sur l'arme cybernétique comme arme de dissuasion. Cela passe par l'élaboration de solutions pour répondre prioritairement aux besoins que je vais énumérer.

Premièrement, il y a l'attribution, c'est-à-dire la capacité de remonter à la source réelle d'une attaque. Ce n'est pas un problème trivial; l'attribution est un problème central si nous voulons développer une doctrine d'utilisation de l'arme cybernétique.

Deuxièmement, il y a la menace interne. Beaucoup de travaux concernent aujourd'hui la protection et la détection contre les menaces externes. Cependant, une cyberattaque de grande ampleur, comme celle que nous venons d'évoquer, nécessitera très probablement des relais internes dans les infrastructures cibles de l'attaque. Il est donc très important d'élaborer des solutions de supervision de la menace interne pour gérer non seulement les cas de malveillance, mais aussi les cas de négligence. Malheureusement, les menaces internes sont souvent liées à de la négligence.

Troisièmement, des paramètres pour mesurer l'effet réel d'un scénario de cyberattaque sont absolument nécessaires pour développer une doctrine de cyberdissuasion respectant les principes de proportionnalité de la riposte.

Quatrièmement, il y a la cyberrésilience, c'est-à-dire la capacité de résister à une cyberattaque. Polytechnique a déjà travaillé sur plusieurs secteurs critiques, comme la finance, la chaîne d'approvisionnement, la défense, le secteur maritime et l'aéronautique.

En conclusion, je dirai que, pour répondre à ces différents besoins, l'élaboration de solutions adaptées reposant notamment sur l'intelligence artificielle fait partie de nos priorités.

Je vous remercie de votre attention.

● (1250)

[*Traduction*]

Le président: Merci beaucoup.

J'invite maintenant M. Paquin à prendre la parole pour un maximum de cinq minutes.

Quand vous voudrez.

[*Français*]

M. Jonathan Paquin (professeur titulaire, Département de science politique, Université Laval, à titre personnel): Mesdames et messieurs les députés, c'est un privilège et un honneur de témoigner devant vous aujourd'hui.

Les faits laissent croire que Moscou est une menace à la sécurité de notre pays. D'abord, au cours des 15 dernières années, la Russie a mené des cyberattaques contre les infrastructures essentielles des pays hostiles à ses intérêts. Puisque le Canada est actuellement très hostile aux intérêts de Moscou, il est potentiellement une cible de choix pour le Kremlin. D'ailleurs, le ministre des Affaires étrangères russe Sergueï Lavrov déclarait tout récemment à un média italien que « [l]es Américains, et en particulier les Canadiens, ont joué un rôle de premier plan dans la formation de divisions ultraradicales ouvertement néonazies en Ukraine ». Cela en dit assez long sur la perception russe de notre rôle dans le conflit.

Moscou finance des campagnes de manipulation de l'information, ou de désinformation, contre les institutions démocratiques en Occident. Son objectif est clair, on l'a dit et redit, c'est de désinformer et de diviser nos concitoyens afin d'affaiblir nos institutions démocratiques. Ces activités ont été largement documentées au cours des dernières années.

Depuis le début de l'invasion de l'Ukraine, le régime de Poutine a menacé à de nombreuses reprises d'avoir recours à des armes nucléaires tactiques ou stratégiques parce qu'il juge que l'OTAN mène une guerre par procuration contre la Russie.

En conséquence, depuis le 24 février dernier, nous devons être très vigilants à l'égard des différentes menaces que pose le Kremlin à notre sécurité. Notre vigilance doit être encore plus grande maintenant que les pays occidentaux ont revu à la hausse leurs objectifs dans le conflit ukrainien et qu'ils cherchent ouvertement à affaiblir les capacités de la Russie. Cette nouvelle posture plus offensive contribue à l'escalade des tensions avec la Russie. Puisque le Canada y souscrit pleinement, le Kremlin est une menace grandissante pour notre sécurité.

J'estime que la meilleure posture de sécurité que le Canada doit avoir par rapport à la Russie combine la dissuasion par représailles, ce qui est possible, compte tenu notamment de l'article 5 du Traité de l'Atlantique Nord, organisation dont le Canada est membre depuis de nombreuses années, et la dissuasion par le déni, c'est-à-dire par la cyberrésilience, par l'éducation à la désinformation et par une défense continentale renouvelée.

J'estime aussi que la principale menace pour le Canada est celle des cyberattaques contre nos infrastructures essentielles. Le gouvernement canadien doit accroître ses investissements pour renforcer la sécurité de ces infrastructures et pour nous rendre toujours plus résilients par rapport aux attaques russes. L'idée, c'est de décourager le Kremlin de mener de telles attaques, sachant que leurs succès sont probablement faibles ou peu probables. C'est la dissuasion par le déni.

En ce qui concerne les campagnes de manipulation de l'information perpétrée par Moscou, leur effet est moins immédiat et plus diffus que celui des cyberattaques. Je suis d'avis que le Canada est assez bien outillé pour faire face à cette désinformation, parce qu'il est relativement peu vulnérable. Cela me fera plaisir d'en parler davantage.

Enfin, malgré les déclarations inquiétantes de Poutine, l'utilisation d'armes de destruction massive par la Russie représente un risque moins important pour le Canada que celui des cyberattaques. Néanmoins, puisque l'évolution de la guerre en Ukraine est imprévisible, le gouvernement canadien a la responsabilité d'investir davantage dans la modernisation du commandement et du contrôle par le truchement de l'organisation Commandement de la défense aérospatiale de l'Amérique du Nord, ou NORAD. Nous devons avoir un excellent système de surveillance pour détecter rapidement les missiles russes et, notamment, les missiles hypersoniques. D'ailleurs, la ministre de la Défense nationale y a déjà fait allusion, et des annonces devraient être faites prochainement, ce qui est de très bon augure.

Selon moi, le moment est aussi venu de reconsidérer notre participation au bouclier antimissile nord-américain, puisque Washington n'est pas tenu de défendre le territoire canadien en cas d'attaques de missiles russes.

Je vais m'arrêter ici, mais c'est avec plaisir que je répondrai de mon mieux à vos questions.

● (1255)

[*Traduction*]

Le président: Merci beaucoup.

Nous allons maintenant faire un tour complet. Commençons avec M. Lloyd, pour six minutes.

M. Dane Lloyd (Sturgeon River—Parkland, PCC): Merci, monsieur le président.

Merci aux témoins de leur présence aujourd'hui.

Ma première question s'adresse à Mme Cuppens.

Certains de vos propos ont vraiment piqué mon intérêt. Vous avez dit que les Russes avaient revendiqué une cyberattaque contre Rideau Hall, mais que vous ne pouviez pas confirmer pour l'instant s'ils étaient réellement à l'origine de l'attaque.

D'après vous, pourrait-il arriver que les Russes revendiquent des attaques dont ils ne sont pas responsables, pour semer la confusion au Canada?

[*Français*]

Mme Nora Cuppens: Je vous remercie de la question.

La question de l'attribution est un gros problème, parce qu'il n'est pas facile de remonter à la source. Ces groupes d'attaquants, même s'ils sont identifiés et même si l'on arrive à savoir qui ils sont, revendiquent rarement leurs actions. Quand ils les revendiquent, ils essaient de faire de la provocation. Quand ils prennent cette décision de revendiquer leurs actions, ils attendent une réaction. En ce qui a trait à l'attaque contre Rideau Hall, ils ne vont pas la revendiquer, mais ils laissent planer suffisamment de doute pour que l'on suppose que cela vient de là. Il faut faire attention quand il s'agit de ce type d'attaque.

● (1300)

[*Traduction*]

M. Dane Lloyd: Selon ce que vous dites — et ce que j'essaie de confirmer —, pensez-vous que les Russes, dans le but de semer la désinformation, la peur et la confusion, revendiqueront parfois la responsabilité d'attaques avec lesquelles ils n'ont en fait rien à voir? S'agit-il d'une forme de désinformation que nous devons surveiller?

Faut-il simplement prendre au pied de la lettre ce qu'ils disent quand ils revendiquent une attaque, ou bien est-il toujours important de procéder à une attribution pour confirmer ou infirmer s'ils sont à l'origine de l'attaque?

[*Français*]

Mme Nora Cuppens: Pour les attaques terroristes, c'est la même chose. Dès qu'il y a une attaque, les terroristes la revendiquent, qu'elle soit liée à leur mouvement ou pas. Je crois que j'ai répondu à la question, mais je vais y répondre de façon plus affirmative.

Oui, ils peuvent revendiquer une attaque ou faire croire qu'ils sont derrière telle ou telle attaque, justement pour susciter de la crainte. Ils veulent envoyer le message selon lequel, si nous entreprenons une action, ils peuvent mener une contre-action qui aura un effet très important. On nous donne un exemple par cette attaque, même si ce ne sont pas les Russes qui en sont à l'origine. Cela crée, comme vous venez de le dire, un climat de crainte. On annonce que l'on peut avoir un effet important au moyen d'une réaction ou d'une cyberattaque.

[*Traduction*]

M. Dane Lloyd: Merci de votre réponse.

Monsieur Cuppens, un des apparents atouts stratégiques des démocraties occidentales est la solidité de l'écosystème du secteur des technologies de l'information, une solidité qui, je l'espère, recouvre également aussi bien les capacités cyberoffensives que les capacités cyberdéfensives.

Quelles mesures recommanderiez-vous pour que le Canada puisse préserver et renforcer ses atouts stratégiques dans ces domaines? Faudrait-il investir davantage dans l'éducation, pour former des ingénieurs capables de construire cette infrastructure? Faudrait-il établir un crédit d'impôt pour encourager le secteur privé à investir dans les capacités de cybersécurité du Canada?

D'après vous, qu'est-ce que le gouvernement pourrait faire pour favoriser une robuste réponse combinée du secteur privé et du secteur public et l'émergence d'un solide écosystème de cybersécurité?

[*Français*]

M. Frédéric Cuppens: La première recommandation a trait à l'information, qui est effectivement un élément central. Il faut former plus d'ingénieurs experts en cybersécurité, que ce soit pour la protection, la détection ou l'utilisation d'armes plus offensives. Dans le cadre de notre recherche, nous travaillons davantage sur les postures défensives. Nous avons parlé de cyberrésilience et de solutions de détection de la menace interne. C'est effectivement…

[*Traduction*]

Le président: Je suis désolé, monsieur, mais pourriez-vous parler plus près du microphone?

Oui, c'est sûrement mieux.

[*Français*]

M. Frédéric Cuppens: Nous travaillons davantage sur la posture défensive afin de renforcer la cyberrésilience et de mettre au point des outils de détection de menaces externes et de menaces internes. Pour travailler là-dessus, il faut bien…

[*Traduction*]

M. Dane Lloyd: Désolé de vous interrompre. Puisqu'il ne me reste qu'une minute, pourriez-vous ultérieurement nous faire parvenir vos recommandations par écrit? Je vous en serais reconnaissant.

Ma dernière question est la suivante. Il y a quelques années, un pipeline américain, le pipeline Continental je crois, a subi une panne qui a complètement bouleversé l'infrastructure énergétique et fait grimper en flèche les prix de l'essence. Nous sommes actuellement en période de forte inflation. Les approvisionnements en pétrole et en énergie sont très restreints.

Que peut faire le gouvernement pour renforcer notre infrastructure de transport de l'énergie pour la protéger contre une attaque de ce type?

[*Français*]

M. Frédéric Cuppens: Je ne sais pas à qui s'adresse la question.

[*Traduction*]

Le président: À qui s'adressait la question?

M. Dane Lloyd: À M. Cuppens.

Le président: Monsieur Cuppens, malheureusement vous n'avez que 10 secondes pour répondre.

● (1305)

[*Français*]

M. Frédéric Cuppens: En ce qui a trait aux transports, l'essentiel est de travailler sur la chaîne d'approvisionnement qui se fait à l'aide du transport multimodal. En réalité, les vulnérabilités se remarquent généralement à la frontière de deux modes de transport, par exemple du passage du transport maritime vers le transport ferroviaire ou du transport ferroviaire vers le transport routier. C'est à ces étapes de transition dans la chaîne de transport multimodal que se trouvent les vulnérabilités, et c'est sur celles-ci qu'il faut travailler en priorité.

[*Traduction*]

Le président: Merci beaucoup.

Monsieur McKinnon, à vous maintenant la parole pour un tour de six minutes. Vous pouvez débuter quand vous voulez.

M. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.): Merci.

Je vais commencer par M. Paquin. J'aimerais des précisions sur une de vos remarques concernant l'OTAN et l'article 5. Si je ne m'abuse, vous avez dit qu'on pouvait invoquer l'article 5 pour justifier une réponse à une attaque contre nous. Selon ma compréhension de l'article 5, ce n'est pas qu'il justifierait une réponse de notre part à une attaque contre nous, mais qu'il nous obligerait à répondre à une attaque visant l'un ou l'autre des autres membres de l'OTAN.

Voulez-vous dire qu'en cas de cyberattaque contre l'un de nos alliés de l'OTAN, l'article 5 nous obligerait d'y répondre?

[*Français*]

M. Jonathan Paquin: C'est une question très importante.

Au sein de l'OTAN, on se questionne de plus en plus sur les conséquences des cyberattaques, parce que l'on sait qu'elles peuvent prendre une ampleur considérable. Effectivement, selon la position croissante de l'OTAN, une cyberattaque d'envergure au sein d'un pays contre ses installations ou ses infrastructures essentielles pourrait être considérée comme une attaque contre l'un des membres de l'Organisation.

Par ailleurs, l'article 5 du Traité de l'Atlantique Nord ne prévoit pas que tous les membres de l'Alliance entreront automatiquement en confrontation militaire contre l'État qui aura perpétré la menace. Il prévoit plutôt que chaque membre aura la responsabilité de prendre les moyens jugés appropriés pour venir en aide à l'État qui est victime d'une cyberattaque.

Le principal problème qui se pose relativement aux cyberattaques et à l'OTAN est celui de l'attribution, comme l'ont mentionné mes collègues M. Cuppens et Mme Cuppens. Cela veut dire qu'il faut être en mesure de démontrer hors de tout doute qu'une cyberattaque majeure a été perpétrée par le Kremlin, par exemple au Canada, par les pouvoirs publics, et non par des pirates qui agissent de manière autonome ou indépendante sur le territoire russe. Cette démonstration n'est pas facile à faire.

Cela pourrait avoir pour effet d'amener les États membres à débattre la question de savoir si c'est vraiment le cas, et cela perd donc énormément de sa pertinence.

[*Traduction*]

M. Ron McKinnon: Merci, monsieur Paquin.

Je passerai maintenant à Mme Cuppens. Certains des témoins précédents ont indiqué qu'un de nos problèmes, au Canada, est l'absence d'agence centrale chargée de coordonner et de gérer, dans l'ensemble de la société, la réponse aux attaques possibles. Le CST joue à cet égard un rôle très restreint.

Croyez-vous que le CST devrait assumer ce rôle, ou bien avez-vous des commentaires sur la prémisse de départ?

[*Français*]

Mme Nora Cuppens: Je vous remercie de la question.

Je viens de l'Europe, et c'est vrai qu'en France, notamment, il y a l'Agence nationale de la sécurité des systèmes d'information qui joue un rôle d'observatoire ainsi qu'un rôle régalien, comme M. Cuppens l'a évoqué tout à l'heure. Il nous faudrait donc une institution semblable qui opérationnaliserait, en quelque sorte, la protection de nos systèmes et de nos infrastructures. Cela pourrait être le Centre de la sécurité des télécommunications.

On a plein de règles en matière d'hygiène informatique et de règles qui nous disent comment on doit se protéger ou réagir contre des attaques, mais il n'y a pas d'obligation d'appliquer ces règles de protection, de détection et de réponse aux intrusions. La mise en place d'une telle institution qui jouerait un rôle de cybersurveillance et d'observatoire, qui pousserait la réglementation et qui vérifierait que les règles sont appliquées me semble être d'une importance primordiale pour nous assurer que nous avançons sur le bon chemin.

On me dira qu'il est compliqué pour les petites ou moyennes entreprises d'appliquer certaines règles. Toutefois, on pourrait les associer à une entité qui fait de la cybersurveillance pour les aider à acquérir peu à peu cette protection. On a parlé de la chaîne d'approvisionnement, tout à l'heure. Les attaques ne visent pas les entités de front, elles viennent toujours par des tiers, notamment dans la chaîne d'approvisionnement. Il s'agit donc généralement des entités les moins sécurisées.

● (1310)

[*Traduction*]

M. Ron McKinnon: Vous avez mentionné, bien sûr, les petites entreprises et le reste. Le producteur laitier ou le garagiste du coin sont branchés à Internet et ils sont peut-être eux-mêmes vulnérables, ou encore ils peuvent servir de passerelle vers la vulnérabilité d'une autre personne. Ce type de protection, la détection d'une attaque, exige une série de compétences très spécialisées et hyperpointues.

Comment ces types d'entreprises et d'organisations vont-elles se protéger elles-mêmes, et par conséquent protéger le réseau, contre les attaques?

[*Français*]

Mme Nora Cuppens: Je peux répondre de deux façons à la question. La première est une réponse classique que tout le monde connaît...

[*Traduction*]

Le président: Je suis désolé. Il y a deux façons, mais seulement dix secondes.

[*Français*]

Mme Nora Cuppens: Il s'agit de prendre des mesures en matière d'hygiène informatique.

La deuxième a trait à l'externalisation. Quand on ne sait pas comment s'y prendre, on demande l'aide d'experts. L'approche consiste à externaliser ce travail en le confiant à des entités qui, elles, savent comment s'y prendre. L'entreprise est alors un point d'entrée.

[*Traduction*]

Le président: Merci.

Madame Michaud, à vous la parole pour six minutes.

[*Français*]

Mme Kristina Michaud: Je vous remercie, monsieur le président.

Je remercie les témoins d'avoir accepté notre invitation à comparaître devant le Comité.

Monsieur Paquin, j'ai l'impression que c'est dans une autre vie que vous étiez mon professeur à l'Université Laval. Vous m'en avez appris beaucoup sur la politique étrangère des États-Unis, et je suis certaine que votre expertise sur la sécurité canadienne, entre autres, pourra profiter grandement au Comité.

Au début du conflit en Ukraine, vous avez mentionné que, depuis la Seconde Guerre mondiale, on cherchait désespérément à éviter un conflit entre deux superpuissances nucléaires et que c'était la raison pour laquelle les puissances occidentales ne voulaient pas aller au-delà des sanctions économiques, par exemple.

De quelle façon la Russie pourrait-elle réagir à ces sanctions économiques, et de quelle façon le Canada devrait-il se préparer?

Selon vous, le Canada est-il suffisamment préparé par rapport à une éventuelle attaque, quelle qu'elle soit?

M. Jonathan Paquin: Je vous remercie de la question, madame la députée. C'est avec plaisir que je vous revois dans un contexte autre que le contexte universitaire.

Pour répondre à votre question, je dirai qu'il est très important que le Canada fasse tout en son pouvoir pour que le conflit en Ukraine reste limité au territoire ukrainien. Tant et aussi longtemps que nous nous concentrons sur des sanctions économiques et que nous nous rappelons que notre objectif est d'aider les Ukrainiens à libérer leur territoire, au nom du droit international et au nom des valeurs libérales, selon moi, les choses se passeront relativement bien.

Le problème que je vois, c'est que, depuis une semaine ou deux environ, nous assistons à l'apparition d'une nouvelle stratégie occidentale par rapport à l'Ukraine. L'objectif n'est plus seulement d'aider les Ukrainiens à se défendre, mais il est également d'affaiblir la Russie.

La ministre des Finances et vice-première ministre du Canada, Mme Chrystia Freeland, disait dans son discours, lorsqu'elle a présenté le budget fédéral le 7 avril dernier, que les démocraties, dont le Canada, ne seraient libres que lorsque le tyran russe aurait été vaincu.

Bien sûr, nous pouvons considérer que ce genre de rhétorique est légitime, mais le signal que cela envoie, c'est que nous sommes non pas dans une logique de libération de l'Ukraine, mais vraiment dans une logique plus offensive, qui a pour objectif d'affaiblir la Russie. Cela peut amener la Russie à contre-attaquer. Nous savons que la Russie se sent humiliée et c'est certainement vrai, pour de nombreuses raisons, en ce qui concerne le président Poutine, et ce, depuis au moins une trentaine d'années. Si la Russie, à cause de nos actions en Ukraine, notamment par la livraison d'armes lourdes — et c'est ce que le Canada fait à l'heure actuelle avec ses alliés — devait perdre la guerre ou si la Russie ne devait pas être en mesure de gagner dans l'Est et dans le Sud du pays, il y a fort à parier qu'il y aura des mesures de représailles, et que, essentiellement, les Russes ne maintiendront pas le statu quo.

Je pense qu'il pourrait y avoir des cyberattaques, non pas contre de petites ou moyennes entreprises, qui ne sont pas intégrées, en quelque sorte, aux grandes chaînes de valeur, mais contre les infrastructures essentielles. C'est la raison pour laquelle je considère que les pouvoirs publics doivent absolument accroître les investissements, non seulement pour sécuriser l'espace numérique du Canada, mais aussi pour accroître la coordination avec les principales entreprises canadiennes et la coordination avec les provinces, les territoires et nos principaux partenaires, dont les États-Unis et le Royaume-Uni.

● (1315)

Mme Kristina Michaud: Je vous remercie beaucoup.

Vous avez touché à un point assez important dans votre allocution d'ouverture lorsque vous avez parlé du rôle que jouait le Canada dans ce conflit et de la perception de ce rôle.

Nous savons que la Chine et l'Inde, notamment, n'ont pas dénoncé l'invasion russe en Ukraine.

Quelle incidence pourrait avoir cette diffusion de la perception russe sur d'autres puissances mondiales quant au rôle joué par le Canada? De quelle façon cela pourrait-il venir déséquilibrer l'ordre mondial, selon vous?

Sommes-nous à l'abri de ce genre de campagne de désinformation à l'échelle mondiale?

M. Jonathan Paquin: Je vous remercie de la question.

Avant le 24 février dernier, plusieurs observateurs se demandaient si les États occidentaux, dont le Canada, étaient prêts à aller suffisamment loin pour défendre les valeurs qui les habitent. Plusieurs en doutaient. Le président Poutine et le président chinois, Xi Jinping, en doutaient.

À mon avis, la situation en Ukraine montre que les pays occidentaux, le Canada et les autres membres de l'OTAN, plus particulièrement, sont en mesure d'accroître leur cohésion quant à leurs interventions ainsi que leur collaboration lorsqu'il y a, en quelque sorte, péril en la demeure. Cela est important. C'est un moment décisif, parce que le message que nous envoyons à des États comme la Chine, par rapport à Taïwan, c'est que nous sommes prêts à prendre les moyens nécessaires, que nous sommes prêts, à la limite, à mener une guerre par procuration pour défendre nos alliés, nos partenaires démocratiques. Le message est très clair de la part du gouvernement canadien. Le Canada a une approche assez dichotomique, pour ne pas dire manichéenne, pour ce qui est des bonnes démocraties par opposition aux autocraties, qui ne sont pas bonnes.

Le Canada a une position très claire sur cette situation. Cela n'a pas toujours été le cas. On s'est longtemps demandé où logeait le Canada.

[*Traduction*]

Le président: Vous avez dix secondes, s'il vous plaît.

[*Français*]

M. Jonathan Paquin: Le Canada peinait à aller de l'avant avec des positions claires et affirmées. Maintenant, il a fait son lit, et le monde connaît la position du Canada sur ces questions.

[*Traduction*]

Le président: Merci beaucoup.

Monsieur MacGregor, la dernière tranche de ce tour vous revient. Vous avez six minutes, quand vous serez prêt.

M. Alistair MacGregor: Merci beaucoup, monsieur le président.

Merci également à tous nos témoins, qui ont aidé à guider le Comité tout au long de cette étude.

Madame Cuppens, je souhaiterais commencer par vous.

Dans votre exposé, vous avez évoqué la guerre de l'information qui fait rage actuellement, et la responsabilité de la Russie à cet égard. Ici au Canada, à la fin de février, nous avons observé un virage de la part d'un grand nombre des groupes impliqués dans les manifestations anti-vaccination. Soudainement, à l'aube de la guerre en Ukraine, il y a eu un glissement notable vers une position pro-russe. Ces groupes ont commencé à relayer et à vraiment promouvoir la propagande russe. Ce virage s'est opéré quasiment du jour au lendemain, dès le début de la guerre en Ukraine.

Madame Cuppens, quelles leçons pouvons-nous en tirer?

Je suppose que cette situation témoigne du niveau d'implication de la Russie dans l'émergence de cette mésinformation et sa diffusion au Canada. Je crois que pour beaucoup d'entre nous, il s'agit d'une menace à notre démocratie, si nous ne pouvons même pas nous mettre d'accord sur une même série de faits.

De plus, quels programmes et politiques le gouvernement fédéral peut-il concrètement mettre en œuvre pour combattre ce problème, où un acteur étatique très hostile aux intérêts du Canada intervient dans nos affaires intérieures et exploite ces divisions dans notre démocratie?

● (1320)

[*Français*]

Mme Nora Cuppens: Je vous remercie de la question.

Il est vrai que nous revenons toujours à ce problème, que nous avons tous les trois mentionné depuis le début de cette séance, soit l'aspect de l'attribution.

Dans le cadre de nos travaux en cybersécurité, nous faisons souvent des corrélations pour essayer de voir s'il y a une intrusion ou une attaque en cours, quelle est la cible et quel est l'objectif en matière de sécurité. Le raisonnement est le même. Cela se déplace du cyberespace vers le terrain de tous les jours, d'où les manifestations et ainsi de suite.

Il est donc difficile de dire si les motivations, ou les raisons, qui ont mené à ces manifestations, sont forcément liées au Kremlin, aux Russes ou à d'autres événements de ce type. Il y a aussi les initiatives isolées. Même si des personnes sont prorusses, elles peuvent prendre des initiatives personnelles pour aider à aller dans le sens de la Russie.

Il n'est pas facile de dire si c'est une initiative russe qui a mené à des manifestations de ce type. Il est difficile aussi de corréler le moment où cette invasion russe a démarré, le 24 février, et certains événements qui se sont produits sur le terrain en lien avec les manifestations ou en lien avec des attaques contre des infrastructures liées au secteur de l'énergie en Ukraine, des opérateurs ou des satellites, car il ne faut pas oublier l'aspect spatial.

La question est en cours de traitement, et nous n'avons pas encore trouvé la réponse à cet aspect de l'attribution, qui permet de mener des enquêtes. Dès lors que nous aurons déterminé l'attribution, cela fera intervenir d'autres aspects juridiques et d'autres responsabilités...

[*Traduction*]

M. Alistair MacGregor: Merci, madame Cuppens.

Je suis désolé de vous interrompre, mais il ne me reste que deux minutes. J'aimerais m'adresser à M. Cuppens.

Vous avez mentionné la loi française sur la cybersécurité. Je pense que vous faites référence à la protection de l'information sur les infrastructures critiques. La France a désigné 12 secteurs, soit l'alimentation, la santé, l'eau, les télécommunications et la radiodiffusion, l'espace et la recherche, l'industrie, l'énergie, les transports, les finances, l'administration civile, les activités militaires et la justice. Vous avez utilisé cela comme exemple. Le Canada doit prendre l'initiative au niveau fédéral dans l'établissement de la cybersécurité.

Quel type de recommandation souhaiteriez-vous que le Comité formule au gouvernement fédéral? Aimeriez-vous que nous imitions le modèle français et que nous introduisions ici une loi fédérale qui imposerait vraiment ce niveau d'exigence minimum dans ces secteurs?

Nous aimerions avoir votre éclairage à ce sujet.

[*Français*]

M. Frédéric Cuppens: Je n'ai pas la réponse à la dernière partie de la question.

Par contre, il y a effectivement des choses intéressantes dans la démarche proposée dans le cadre de la Loi de programmation militaire 2019-2025, notamment la notion d'opérateurs d'importance vitale, ou OIV.

En France, une entreprise dont les activités sont en lien avec un secteur d'activités critique a l'obligation, une fois qu'elle a été désignée comme OIV, de mettre en place un certain nombre d'obligations pour être en conformité avec cette loi de programmation militaire. Ce n'est pas une déclaration spontanée de l'entreprise; c'est une obligation imposée par l'État une fois qu'elle a été désignée comme OIV. Cela concerne naturellement les grandes entreprises, mais cela englobe aussi les petites ou moyennes entreprises à partir du moment où l'une de ces entreprises exerce des activités en lien avec un secteur d'activités critique.

[*Traduction*]

Le président: Vous avez 10 secondes.

[*Français*]

M. Frédéric Cuppens: En ce qui concerne la sécurité des activités d'importance vitale, ou SAIV, chaque secteur relève d'un ministère. La responsabilité du ministère est de s'assurer que les OIV rattachés à son ministère sont en conformité avec la Loi.

[*Traduction*]

Le président: Merci beaucoup.

Chers collègues, il nous reste encore trois ou quatre minutes. Nous n'avons pas le temps d'effectuer un autre tour. Certains d'entre nous ont un arrêt incontournable dans deux minutes. Je tiens à remercier les témoins, et à m'excuser de la précipitation des échanges. C'est à cause d'un vote qui était requis au début de la séance. Je m'en excuse.

Au nom de tous les membres du Comité, je tiens à remercier tous les témoins qui nous ont fait profiter de leur expérience, de leur expertise et de leur sagesse pour jeter un éclairage sur un aspect aussi important des politiques publiques canadiennes.

Merci à tous de votre contribution.

Chers collègues, nous vous reverrons jeudi. La séance est levée.