



CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la défense nationale

NDDN



NUMÉRO 089



1^{re} SESSION



42^e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 29 mars 2018

Président

M. Stephen Fuhr

Comité permanent de la défense nationale

Le jeudi 29 mars 2018

• (0845)

[Traduction]

Le président (M. Stephen Fuhr (Kelowna—Lake Country, Lib.)): Bonjour. Bienvenue à tous au Comité de la défense ce matin pour notre dernière séance consacrée aux relations du Canada avec l'OTAN. Cette étude a été longue, mais elle porte sur un sujet important. Je suis très heureux d'accueillir nos derniers témoins.

Tout d'abord, de l'OTAN, nous accueillons Jamie Shea, secrétaire général adjoint délégué, Défis de sécurité émergents. Puis, Madeleine Moon, députée de Bridgend, à Londres, au Royaume-Uni, témoignera à titre personnel, tout comme Rafal Rohozinski, consultant principal, Conflits futurs et cybersécurité, à l'Institut international d'études stratégiques.

Merci à tous d'être là aujourd'hui. Nous entendons d'abord Jamie Shea.

Monsieur, vous avez la parole pour votre déclaration d'ouverture.

[Français]

M. Jamie Shea (secrétaire général adjoint délégué, Division Défis émergents de sécurité, Organisation du Traité de l'Atlantique Nord): Monsieur le président, je tiens d'abord à vous remercier de votre gentille invitation à participer à cette séance du Comité. Même si je ne suis pas présent parmi vous, mais que je participe à la réunion par le truchement d'une vidéoconférence, je suis très honoré d'avoir l'occasion de m'adresser à vous.

Avant de me lancer dans ma déclaration préliminaire, je voudrais remercier vivement le Haut-commissariat du Canada au Royaume-Uni d'avoir facilité cette communication aujourd'hui. Je me trouve non pas à l'État-major de l'OTAN à Bruxelles, mais bien à Londres, au Haut-commissariat du Canada au Royaume-Uni.

Je m'exprime en français simplement pour vous montrer que je suis tout à fait prêt à répondre aussi bien en anglais qu'en français aux questions qui me seront posées pendant la période réservée à cette fin. Cependant, comme je peux parler deux fois plus vite en anglais, je vous demanderais d'être indulgents en me permettant de vous livrer mes observations préliminaires en anglais.

[Traduction]

Tout d'abord, si j'ai bien compris, monsieur le président, vous vous intéressez aujourd'hui à ce qui relève du cyberspace, comme la cyberdéfense et la cybersécurité. C'est par là que je vais commencer, mais au préalable, je tiens à dire, moi qui travaille à l'OTAN depuis très longtemps, que ma division, qui est chargée des nouveaux défis en matière de sécurité, s'occupe d'un vaste éventail de questions, y compris le cyberdomaine, mais aussi de la lutte contre le terrorisme, de la politique nucléaire et des prévisions stratégiques.

Si, par la suite, les membres du Comité veulent élargir la discussion pour aborder d'autres aspects des politiques actuelles de l'OTAN, je les invite à le faire. Je serai heureux de m'affranchir de cette réserve et de parler de ces autres questions.

Pour ce qui est du cyberdomaine, on pourrait en parler pendant des années, parce que c'est un sujet complexe et qui évolue rapidement. Permettez-moi au moins d'essayer de vous donner une idée de la position de l'OTAN. Pour nous, le cyberspace présente trois grands défis stratégiques. Premièrement, pour paraphraser un sociologue américain, Clay Shirky, « voici que tout le monde raplique ».

Pour la première fois, le cyberspace permet à presque n'importe qui dans le monde de devenir un acteur stratégique, et cela, à très peu de frais, par rapport à ce que les États avaient l'habitude de dépenser pour se doter de capacités importantes. Le cyberspace permet à n'importe qui d'attaquer n'importe quoi de n'importe où et en tout temps. Ce sont tous les refuges classiques de sécurité qui disparaissent: les obstacles géographiques, les frontières et les déclarations de neutralité.

Pour la première fois, les États ou les organisations comme l'OTAN doivent tout défendre en tout temps, alors que la politique de sécurité, comme vous le savez, a permis pendant des siècles de définir un adversaire et un accès stratégique et de concentrer la plupart des ressources sur certains points névralgiques. Maintenant, il faut prendre des décisions difficiles sur le choix des priorités, qu'il s'agisse des infrastructures essentielles, du secteur civil, du secteur bancaire ou des télécommunications, au gré du déplacement constant d'un secteur à l'autre des menaces liées au cyberspace. Il faut une grande souplesse pour être en mesure de suivre l'évolution de la menace, d'autant plus qu'une entreprise comme Symantec repère plus de deux millions de nouveaux maliciels sur le marché chaque année.

Le deuxième problème, bien sûr, c'est que la dimension cybernétique efface la vieille distinction entre guerre et paix. Nous sommes condamnés à vivre dans une sorte de zone grise permanente qui n'est ni la paix ni la guerre, où tout est attaqué et où nous faisons l'objet d'attaques majeures ou mineures, tous les jours de la semaine. La plupart de ces attaques se situent sous le seuil traditionnel de l'article 5 de l'OTAN, qui était clairement défini d'après le nombre de chars qui traversent une frontière définie.

Le cyberspace se trouve dans ce genre de zone grise où il est parfois difficile de dire ce qu'est une attaque armée ou son équivalent ou ce qu'est une attaque hostile, et ce qui est simplement une nuisance. Par conséquent, il est difficile de savoir comment réagir, parce que, d'une part, on veut que l'intervention ait un impact et que, d'autre part, on veut éviter une escalade vers une crise d'une ampleur probablement plus grande que ce qu'on souhaite.

Il y a des problèmes liés à la classification des attaques, à la façon de désigner leur origine et à la rapidité avec laquelle il faut le faire, à la solidité de la preuve nécessaire avant de pouvoir désigner l'auteur et de définir la réponse qui convient. Diplomatique? Économique? Militaire, même? L'OTAN a certainement dit, à son sommet au pays de Galles, en 2014, qu'à un certain seuil, une cyberattaque pourrait effectivement être considérée comme l'équivalent d'une agression armée et, par conséquent, provoquer le recours à l'article 5 et une riposte de l'OTAN. Toutefois, ce seuil demeure ambigu, car nous croyons que l'ambiguïté sert les fins de dissuasion.

● (0850)

Le troisième et dernier point stratégique, au sujet du cyberdomaine, c'est qu'on ne peut manifestement pas recourir aux outils qu'on possède normalement au sein de sa propre organisation. En ce qui concerne la défense collective classique — et le Canada participe, bien sûr, à la direction de la division multinationale en Lettonie en ce moment —, nous avons dans notre propre organisation les chars d'assaut, les avions et l'artillerie dont nous avons besoin, même si parfois nous aimerions que ce matériel soit plus moderne, davantage prêt à servir.

Dans le cyberspace, nous constatons que, pour être efficaces, nous devons dépendre des autres, par exemple du secteur privé, qui est responsable de 90 % des réseaux et d'où provient la plus grande partie de l'innovation et du cyberrenseignement. Dans ce domaine, l'efficacité dépend de la capacité de former ces partenariats, de persuader d'autres personnes d'apporter leur aide et de construire un véritable écosystème pour relever le défi.

Ce sont là trois messages d'introduction.

Très brièvement, que fait l'OTAN? Il y a quatre domaines. Je me ferai un plaisir, bien sûr, d'en discuter avec tous les membres du Comité de façon aussi détaillée que possible.

Premièrement, nous devons évidemment défendre nos propres réseaux. Cela semble simple. C'est le point de départ, mais dans une organisation complexe comme l'OTAN, ce n'est pas si simple. Nous avons 55 sites à protéger. Nous possédons 35 systèmes de TI différents. Certains sont nouveaux et d'autres anciens. Bien sûr, quand on combine l'ancien et le nouveau dans le cybermonde, on a beaucoup plus d'interfaces et donc beaucoup plus de vulnérabilités et de surfaces d'attaque. Ces dernières années, nous avons mis sur pied une capacité complète d'intervention en cas d'incidents informatiques à l'OTAN, le NCIRC, basé au SHAPE, à Mons, qui assure une protection de nos réseaux civils et militaires 24 heures sur 24, sept jours sur sept.

Un deuxième volet fait intervenir les milieux du renseignement, qui lancent des alertes stratégiques en cas de cyberattaques, ainsi que les services techniques. Dans le cyberdomaine, surtout pour la gestion des incidents, il est très important de s'assurer que ce qu'on observe correspond à ce qu'on entend. Autrement dit, le renseignement correspond à ce qu'on observe dans les réseaux, parce qu'un élément pourrait alerter l'autre. Nous avons donc une cellule d'analyse des cybermenaces qui rassemble ces communautés.

Monsieur le président, comme vous l'avez vu lorsque vous et les membres du Comité avez visité le siège de l'OTAN à Bruxelles, nous avons créé une division conjointe du renseignement et de la sécurité précisément pour intégrer davantage les renseignements nationaux à l'OTAN afin que nous puissions avoir une meilleure

connaissance de la situation et établir une meilleure corrélation entre les données que nous recevons.

Bien sûr, dans ce domaine aussi, comme vous le savez — et c'est vrai pour nous tous — une partie du travail de protection consiste à repérer les dépendances critiques. On s'étonne souvent de constater, lorsqu'on pense avoir défini le cyberécosystème, identifié tous les réseaux critiques et assuré partout un même niveau de protection, qu'il existe un nouveau risque lié à la chaîne d'approvisionnement provenant d'un autre système et dont on se rend compte qu'il est relié au sien et dont on ignore le niveau de sécurité. Cette redéfinition constante est également importante.

Le deuxième niveau de nos efforts, c'est l'aide aux alliés. Nous voulons vraiment être au cœur d'un certain nombre de services de cyberdéfense qui pourraient aider nos alliés à devenir plus résilients à l'échelle nationale et à tirer des enseignements des technologies les uns des autres, des personnes en place, des processus, des méthodes de sensibilisation et des expériences de chacun, de façon que nous puissions de plus en plus comparer les normes de façon objective en permettant aux alliés de s'évaluer volontairement et de comparer leurs résultats à ceux des autres.

Il s'agit d'un engagement en matière de cyberdéfense qui en est à sa deuxième année. En fait, j'espère que, dans les prochains jours, le rapport du Canada, son auto-évaluation pour le deuxième cycle, arrivera au siège de l'OTAN. Bien sûr, nous allons le comparer à ce que le Canada nous a dit il y a à peine un an. Je sais, d'après vos propres activités nationales des derniers mois, qu'il y a eu une intensification des efforts dans ce domaine. Par conséquent, je suis sûr que vous avez beaucoup de nouveautés intéressantes à nous signaler.

● (0855)

L'engagement, comme je l'ai dit, permet une analyse comparative complète, c'est-à-dire qu'il permet à l'OTAN d'avoir un aperçu complet des forces ou des faiblesses de nos alliés dans le domaine informatique et, par conséquent, de donner des réactions et des conseils; et il encourage les pays à consacrer davantage de ressources à la cybersécurité en déterminant les priorités clés de l'OTAN et à assurer une plus grande cohésion au niveau national entre les divers ministères. De nombreux alliés nous ont dit que cet engagement était le premier bilan exhaustif qu'on leur demandait de faire.

Très brièvement, avant de terminer, deux derniers éléments. Troisièmement, il y aura peut-être des questions et des discussions, parce que c'est ce qu'il y a de plus ambitieux et exigeant. Lors de notre sommet de Varsovie en 2016, nous avons déclaré que le cyberspace était un domaine opérationnel. Autrement dit, nous devons intégrer le monde virtuel et le cyberspace aux quatre domaines traditionnels de la gestion des crises et des conflits: air, mer, terre et espace. Nous devons faire du cyberspace le cinquième domaine et, par conséquent, comprendre les implications des conflits dans cet espace et voir quels instruments et quelle doctrine il nous faut pour intervenir, étant donné que tous les conflits futurs auront probablement, ou inévitablement, une cyberdimension. Par conséquent, comment le cyberspace peut-il se situer auprès de la dissuasion nucléaire, de la défense classique et de la défense antimissile dans la posture de l'OTAN? Que peut-on faire? Qu'est-ce qu'on ne peut pas faire? De quelles capacités nouvelles avons-nous besoin?

Vous avez probablement vu, monsieur le président et mesdames et messieurs les membres du Comité, que nous avons maintenant convenu d'établir un centre des cyberopérations et d'intégrer à la posture de l'OTAN les contributions nationales volontaires en ce domaine que des alliés qui ont ces capacités seraient disposés à mettre à notre disposition. Ce travail se poursuit.

Voici mon dernier point. À l'OTAN, nous voulons bien sûr apporter une dimension politique à la question du cyberdomaine au lieu de nous limiter aux aspects militaire et technique. En effet, comme dans tous les autres secteurs de l'engagement de l'OTAN, nous considérons que notre sécurité dépend des initiatives politiques, des initiatives de contrôle des armements, des mesures de renforcement de la confiance et des restrictions convenues, et pas seulement de la mise au point de nouvelles armes. Nous sommes donc très engagés — même si nous ne négocions pas — dans tout le domaine du droit international qui s'applique au cyberspace, et nous cherchons comment nous pouvons collaborer avec l'UE, l'ONU, l'OCDE et d'autres institutions.

Si cela intéresse le Comité, je le renvoie aux deux manuels de Tallinn que notre centre d'excellence a produits sur le droit international régissant le cyberspace. Ils contribuent à faire avancer ce débat intellectuel.

Je vais m'arrêter ici, mais j'espère que nous pourrions avoir ensuite avec le Comité une bonne discussion fructueuse sur l'orientation que vous souhaitez prendre.

Merci encore de m'avoir fait l'honneur de m'inviter à traiter de cette question ce matin.

Le président: Merci beaucoup, monsieur Shea.

Madame Moon, vous avez la parole.

● (0900)

Mme Madeleine Moon (députée de Bridgend, United Kingdom, à titre personnel): Merci.

Je ne peux pas prétendre à autant d'érudition et d'aisance que M. Shea, surtout en français. Je peux vous dire quelques mots en gallois, mais mon français est assez limité.

Merci de m'avoir invitée à comparaître devant le Comité permanent de la défense nationale. Je tiens pour commencer à souligner brièvement le rôle crucial que le Canada a joué dans la création de l'OTAN et de son Assemblée parlementaire.

On pourrait soutenir que l'Alliance a commencé lorsque le Canada a accepté d'envoyer plus d'un million de personnes pour servir durant la Seconde Guerre mondiale, dont plus de 14 000 soldats qui se sont joints aux alliés en Normandie le 24 juin 1944.

Dans toute l'Alliance de l'OTAN, nous nous souvenons du travail d'Escott Reid, de Lester B. Pearson et de Louis St. Laurent, qui ont lancé l'idée d'une alliance militaire temporaire dans la région de l'Atlantique Nord pour assurer la stabilité de la démocratie et de la liberté en Europe de l'Ouest, face à la menace communiste. Le Traité de l'Atlantique Nord a été signé le 4 avril 1949 et comprenait l'article 2, qu'on a fini par appeler « l'article canadien ». L'enthousiasme et l'engagement du sénateur canadien Wishart McLea Robertson et du député britannique sir Geoffrey de Freitas ont été à l'origine du premier rassemblement de parlementaires, en juillet 1955, pour créer la conférence des parlementaires de l'OTAN, précurseur de l'actuelle Assemblée parlementaire de l'OTAN. Le sénateur Robertson a été élu premier président de la nouvelle Assem-

blée en 1955 et il a été le premier de nombreux présidents, vice-présidents et rapporteurs canadiens importants qui ont servi l'Alliance et l'Assemblée.

Je voudrais vous parler des pressions qui s'exercent aujourd'hui. J'ai l'intention de me concentrer sur le rôle de l'OTAN dans les domaines maritime et spatial, et sur la promotion d'un programme axé sur les femmes, la paix et la sécurité. J'ai préparé, au nom du Comité de la sécurité de la défense, des rapports sur les domaines maritime et spatial. Je vais vous en entretenir.

Le secteur maritime d'abord, car, à bien des égards, l'OTAN a été principalement une alliance maritime. Le lien transatlantique est vital pour tous les États membres, mais il a longtemps été négligé. On a dit qu'il est impossible de gagner une guerre dans l'Atlantique, mais qu'on peut certainement y en perdre une. Le contrôle de la mer est essentiel aux communications et à la liberté de mouvement, deux aspects cruciaux de l'efficacité opérationnelle de l'OTAN. Les forces navales de l'Alliance garantissent la défense stratégique de l'OTAN et sont essentielles à la promotion et à la protection des intérêts politiques, économiques et diplomatiques.

Toutefois, dans l'ensemble, les marines des États membres ont diminué de taille, en grande partie en raison, comme dans la plupart des domaines, de l'augmentation des coûts et de la grande technicité des navires. Cela a eu deux effets majeurs: les marines alliées se sont contractées et les écarts de capacité ont augmenté. Un navire, aussi perfectionné soit-il, ne peut se trouver qu'à un seul endroit à la fois. Résultat de cette évolution, les États-Unis sont maintenant le seul État membre à avoir une capacité vraiment complète.

Pourquoi l'environnement maritime est-il si crucial à l'échelle locale et mondiale? À l'heure actuelle, 95 % du commerce se fait sur des routes maritimes, 80 % des hydrocarbures sont transportés par mer et 95 % du trafic Internet passe par des câbles sous-marins. Un examen plus attentif montre que 80 % du commerce maritime passe par huit goulots d'étranglement, dont trois sont cruciaux pour l'OTAN dans la Méditerranée, la mer Noire et la mer Rouge.

Les chiffres montrent que la liberté des mers est un facteur clé pour les intérêts économiques mondiaux. Mais elle est bien plus que cela. La liberté des mers est également une norme mondiale et elle peut être un moyen de renforcer l'ordre international.

Comme 80 % de la population mondiale vit à moins de 60 milles de la côte, que 75 % des grandes villes du monde sont situées sur le littoral et que l'utilisation des couloirs de navigation augmente de 4,7 % par année, le domaine maritime ne fait que devenir de plus en plus critique pour l'Alliance.

Les menaces en mer s'aggravent. Voici un exemple. Au fur et à mesure que l'océan Arctique devient navigable, le concept de bastion est renforcé par la présence accrue de sous-marins russes. La menace pour les détroits GIUK et nos câbles sous-marins ne cesse de croître. Tous les aspects de la capacité navale sont un catalyseur essentiel de la dissuasion et des manifestations de la volonté et du pouvoir politiques.

● (0905)

Les ressources navales fournissent également la capacité de gérer les crises en fournissant des capacités expéditionnaires, le contrôle et l'interdiction de l'espace maritime ainsi qu'un soutien logistique nécessaire aux opérations amphibies, notamment en faisant respecter les embargos et des zones d'exclusion aérienne et en assurant une aide humanitaire. Les forces navales offrent souvent le moyen le plus facile et le plus rapide pour assurer la sécurité commune en collaborant avec des partenaires au renforcement des capacités, à l'instruction et aux exercices interarmées et, moins directement, par l'entremise de la diplomatie navale.

Je vais simplement mentionner brièvement la sécurité dans les ports, un domaine auquel nous devons accorder plus d'attention.

Passons maintenant à la nouvelle frontière, celle de l'espace. C'est un domaine compliqué, mais de plus en plus important. Au cours des dernières années, l'espace est devenu un pilier clé de la défense de l'OTAN. Il joue, de plus en plus, un rôle de premier plan dans le débat sur la politique et la planification en matière de sécurité, et il est un élément fondamental de la géopolitique mondiale.

Les coûts de fonctionnement dans l'espace sont élevés et, à ce titre, le programme se prête à la collaboration, plutôt qu'à la concurrence, entre les membres de l'Alliance. C'est, sans doute, ce que reflètent les efforts déployés en faveur d'un code de conduite dans l'espace. En ce qui concerne l'OTAN, l'Alliance n'a aucune politique spatiale officielle, mais elle a publié une doctrine alliée interarmées sur les opérations aériennes et spatiales. Il s'agit là d'un domaine que l'OTAN doit maintenant chercher à consolider.

La situation actuelle dans l'espace est complexe. Les constellations de satellites sont maintenant essentielles au fonctionnement efficace des infrastructures modernes, tant militaires que civiles. En effet, l'un des défis est l'impossibilité de distinguer les engins spatiaux civils et militaires les uns des autres. On estime que 40 % de tous les satellites sont militaires, mais cela ne veut pas dire que les engins civils ne peuvent pas servir à des fonctions militaires.

Au cours des deux dernières décennies, les possibilités se sont multipliées. Une multitude de nouveaux intervenants, tant nationaux que commerciaux, congestionnent et polluent les trois principales orbites géocentriques. Cela s'explique en partie par le fait que presque tous les pays ont maintenant un satellite ou un intérêt dans l'espace. Nous avons maintenant environ 1 100 satellites en orbite; certains disent qu'il y en a jusqu'à 1 500. De plus, ces dernières années, de nouveaux acteurs commerciaux dynamiques ont déclenché une deuxième course spatiale. Les coûts, même s'ils sont encore élevés, diminuent, ce qui ouvre l'espace à beaucoup plus de participants et à beaucoup plus de menaces et de problèmes potentiels.

Enfin, au moment de la signature du Traité de l'Atlantique Nord, les femmes abandonnaient les nombreux rôles essentiels qu'elles avaient joués dans les forces armées pendant la Seconde Guerre mondiale. Il a fallu du temps avant que l'important rôle des femmes en matière de paix et de sécurité ne revienne à l'ordre du jour politique. En 2000, la résolution 1325 du Conseil de sécurité des Nations unies encourageait les États membres à faire participer les femmes aux initiatives multilatérales de sécurité comme les accords de paix, les missions de paix et les programmes de désarmement, de démobilisation et de réintégration, et à intégrer dans ces initiatives une perspective axée sur l'égalité des sexes.

D'autres résolutions portent maintenant sur la violence sexuelle dans le contexte d'un conflit armé et reconnaissent la violence

sexuelle comme une grave violation des droits de la personne et du droit international. La reconnaissance du rôle des femmes dans le rétablissement après un conflit et leur intégration active dans la consolidation de la paix, le maintien de la paix et la gestion de l'aide s'accroît.

Plus récemment, le programme a élargi son approche jusque-là limitée aux femmes et aux filles pour prendre aussi en compte les répercussions des conflits sur les relations entre les hommes et les femmes. On reconnaît que la violence sexuelle dans les conflits touche les hommes et les garçons, et ceux qui sont traumatisés en tant que témoins forcés de violence sexuelle contre des membres de leur famille. Le programme souligne également le rôle positif que les hommes et les garçons jouent dans la promotion de l'égalité entre les sexes pendant les efforts de reconstruction. Nous reconnaissons maintenant que les efforts d'édification de la paix doivent bénéficier à la fois aux hommes et aux femmes également.

L'OTAN a adopté tous ces objectifs et les résolutions subséquentes à différents niveaux des structures et des activités de l'Alliance. Le rapport de l'Assemblée parlementaire de 2013 faisait état de neuf stratégies déployées par les parlements des pays membres de l'OTAN, stratégies qui contribuent à la promotion, à la mise en œuvre et à la surveillance du Programme sur les femmes, la paix et la sécurité. Dans quatre domaines, le gouvernement s'est engagé à apporter des changements: l'égalité hommes-femmes parmi les leaders parlementaires, les initiatives législatives, l'influence et la surveillance au moyen de débats, de questions et de rapports et l'engagement de la société civile.

● (0910)

Cette mise à jour a été publiée en 2015. La Commission sur la dimension civile de la sécurité réalisera une autre enquête cette année. Les résultats seront présentés à Halifax par Clare Hutchinson, la représentante de l'OTAN pour le Programme sur les femmes, la paix et la sécurité, qui sera des nôtres pour commenter les résultats.

Je terminerai sur cette note positive. Le Canada est un membre clé de l'Alliance depuis sa création, et j'ai de nombreux collègues canadiens.

Je me ferai un plaisir de répondre à vos questions.

Le président: Merci beaucoup, madame Moon.

Monsieur Rohozinski, vous avez la parole.

M. Rafal Rohozinski (consultant principal, Conflits futurs et cybersécurité, Institut international d'études stratégiques, à titre personnel): Merci beaucoup. C'est un honneur et un privilège de comparaître devant le Comité ce matin.

J'aimerais faire quelques brèves observations sur la position que j'adopte à l'égard de ces questions — autrement dit, d'où je viens — et sur l'importance de s'attaquer à cette question en tant qu'enjeu fondamental pour les relations du Canada avec l'OTAN et la sécurité nationale du Canada.

Mes observations de ce matin s'appuieront essentiellement sur quatre activités auxquelles j'ai participé au cours des 10 dernières années.

Tout d'abord, au cours des 10 dernières années, j'ai été l'un des coresponsables d'un processus diplomatique nommé la voie 1.5 avec le Conseil de sécurité russe de l'Internet qui a traité de la question des normes cybernétiques et de la cybersécurité. Initialement lancé par l'OTAN il y a 10 ans, le processus s'est poursuivi depuis, en tant qu'activité visant à susciter l'engagement, année après année, ce qui a créé un point de convergence pour au moins comprendre les aspects normatifs de l'utilisation du cyberspace en matière de sécurité.

Deuxièmement, je suis également coresponsable, avec des collègues américains et britanniques, de l'établissement d'un dialogue de la voie 1.5 sur l'utilisation militaire du cyberspace entre les États-Unis, la Fédération de Russie et la République populaire de Chine.

Troisièmement, je suis conseiller à titre de citoyen auprès de la Direction exécutive de la lutte contre le terrorisme des Nations unies dont le mandat est de combattre l'extrémisme violent et l'utilisation du cyberspace par les terroristes et qui réunit des partenaires de l'industrie et des États-nations autour de ces questions.

Enfin, je suis un expert du groupe de travail de la Banque mondiale sur l'économie numérique, qui tente de quantifier les répercussions économiques des technologies de l'information et des communications à l'échelle mondiale.

La raison pour laquelle tout cela est important est la suivante. Comme M. Shea l'a souligné, l'OTAN a déclaré que le cyberspace était un domaine opérationnel pour les pays de l'OTAN, et pourtant c'est dans ce domaine que nous avons le moins d'expérience pour ce qui est de comprendre les leviers de l'escalade et de la désescalade. C'est aussi un domaine qui a vu le jour à une époque où les tensions et la dégradation des canaux de communication entre les pays de l'OTAN et ses partenaires potentiels sont les plus fortes.

Dans mes observations, j'aimerais aborder deux sujets distincts. Le premier consiste simplement à comprendre l'incidence du cyberenvironnement sur la sécurité nationale dans son ensemble. Si nous ne comprenons pas cet impact, il est difficile de faire la distinction entre les problèmes qui sont purement nationaux et ceux qui peuvent être influencés ou aggravés par des partenaires externes. Je veux aussi parler de l'enchevêtrement dangereux entre la cybersécurité et la sécurité au niveau technique et social, c'est-à-dire son incidence sociale et politique. J'aimerais ensuite parler brièvement des répercussions que cela a maintenant sur la position de l'OTAN vis-à-vis de la cybernétique en ce qui concerne l'association de notre point de vue sur notre propre état de préparation et aussi nos relations avec des concurrents potentiels dans ce domaine.

La première chose à reconnaître, c'est que les bases sur lesquelles nous avons bâti l'économie mondiale et l'économie canadienne sont peu solides. À l'heure actuelle, selon les projections de la Banque mondiale, 26 % du PIB mondial dépendra de l'économie numérique d'ici 2025. Sur un PIB mondial de 107 billions de dollars, 1 billion de dollars est consacré à la cybersécurité. Pourquoi en est-il ainsi? D'après les statistiques publiées par le Council of Economic Advisers à la Maison-Blanche la semaine dernière, une somme se situant entre 57 et 106 milliards de dollars est attribuée aux pertes liées à la cybercriminalité chaque année aux États-Unis. Cela se produit parce que l'infrastructure d'Internet à la base a été conçue pour la résilience plutôt que pour la sécurité. La technologie ou la réglementation connexe comporte moins de mesures de sécurité que si je construisais une voiture. Pour construire une voiture,

je dois mettre une ceinture de sécurité. Si je construis l'équivalent dans le cyberspace, j'installe effectivement un siège éjectable.

Permettez-moi de vous présenter trois données statistiques qui montrent à quel point nous sommes mal préparés à faire face aux problèmes fondamentaux de sécurité sur Internet. Ce sont trois données liées à un pourcentage de 90 % que vous pouvez facilement garder à l'esprit. Les chiffres sont peut-être un peu dépassés, ils datent d'environ 12 mois, mais ils sont quand même utiles.

Premièrement, 90 % des logiciels malveillants, qui sont conçus pour causer des préjudices sur Internet, utilisent un seul canal de communication, connu sous le nom de DNS, et pourtant plus des deux tiers des entreprises du classement Fortune 100 n'ont aucun point de vue sur ce canal dans leur posture de sécurité. Demandez-vous, si 90 % de la menace peut venir d'un seul canal, pourquoi seulement un tiers des entreprises les plus importantes en Amérique du Nord ont une perspective sur ce canal?

Deuxièmement, 90 % de toutes les industries prévoient intégrer l'Internet des objets dans leur infrastructure, et pourtant, plus de 80 % d'entre elles n'ont absolument aucune assurance que les mesures de sécurité qu'elles ont mises en place leur donneront une idée de la sécurité qui découlera de l'Internet des objets. La raison en est que nous n'avons tout simplement pas réussi à comprendre ce qui est considéré comme un mauvais trafic, un trafic malveillant sur Internet. Cela n'existe pas encore. C'est une lacune de l'industrie, un secteur dans lequel la technologie évolue plus rapidement que la réglementation existante.

- (0915)

Le troisième pourcentage, qui est le plus important, est que 90 % de toutes les atteintes à la cybersécurité passent par le vecteur humain. Autrement dit, les acteurs des atteintes ne se servent pas de la technologie, mais plutôt du comportement humain et de la faiblesse humaine pour entrer dans un système. Si vous posez la question à n'importe quel ingénieur, vous apprendrez que vous ne pouvez pas concevoir une solution de sécurité contre un problème humain. Il s'agit d'un problème de réglementation pour lequel nous n'avons pas défini des règles proportionnelles à l'importance de l'infrastructure que nous avons actuellement et dont dépend notre économie.

De plus, il y a eu un enchevêtrement dangereux entre les capacités et leurs répercussions sociales. Très franchement, au cours des cinq ou six dernières années, les deux tiers de l'humanité sont allés sur Internet, dans le monde entier. De ce nombre, presque tous sont aussi des utilisateurs des médias sociaux. En fait, pour de nombreux pays, comme la Birmanie/le Myanmar, le Bangladesh et d'autres, le premier contact que les gens ont eu avec Internet s'est fait sur Facebook. En outre, plus de la moitié de cette population en ligne a moins de 25 ans. Ils sont les électeurs qui votent pour la première fois.

L'an dernier, on nous a demandé de faire une étude pour l'ONU au Bangladesh sur l'utilisation d'Internet par les terroristes, et ce que nous avons constaté était tout à fait prévisible. Il y a des communautés terroristes qui utilisent Internet, qui parlent des choses violentes, terribles, qui font de la propagande, mais au bout du compte, ces groupes sont assez petits.

Ce que nous avons constaté, cependant, à une échelle beaucoup plus grande, c'est que les partis politiques traditionnels utilisent maintenant Internet et les médias sociaux comme groupe de discussion. Ils sont en train de diffuser des messages et de voir si ces messages suscitent une forme quelconque de soutien populaire. Cela signifie qu'il y a eu une intégration graduelle de l'extrémisme dans l'ensemble du spectre politique. Cela peut vous sembler familier, et il le faudrait, car les mêmes tendances ont eu des répercussions sur la politique canadienne et sur la politique de pays comme les États-Unis.

La raison pour laquelle c'est important, c'est que si nous nous concentrons sur l'incidence de l'Internet simplement du point de vue de l'ingérence des États internationaux, nous passons à côté d'un aspect très, très important, soit la façon dont Internet change la politique au sein de nos propres pays, en l'absence de toute forme d'ingérence étrangère.

En terminant, j'aimerais vous faire part de certains faits.

D'après les témoignages entendus par le comité sénatorial du renseignement des États-Unis, nous savons que les campagnes combinées d'Hilary Clinton et de Donald Trump ont coûté 81 millions de dollars en publicité sur Facebook. Il s'agit d'argent dépensé pour des publicités sur Facebook, à l'abri des comités d'action politique. Le même témoignage indique que le bureau russe de recherche sur Internet, à Saint-Petersbourg, a dépensé environ 46 000 \$ pour des publicités sur Facebook. Même si nous gonflons ce chiffre à 1,5 million de dollars, disons, nous parlons d'une somme d'argent très différente. À moins que nous ne soyons prêts à admettre le fait que les Russes sont beaucoup plus habiles que les agents politiques américains en matière de messages politiques, pour faire élire leurs candidats, nous devons faire très attention à la façon dont nous considérons l'ingérence étrangère ou l'ingérence comme un facteur décisif dans les relations internationales. Cela ne veut pas dire que cela ne s'est pas produit.

En quoi tout cela est-il lié à la position de l'OTAN en matière de cybernétique? Tout d'abord, il est important de reconnaître que les vulnérabilités que je viens de décrire sont des vulnérabilités que nous partageons tous et qui ont très peu à voir avec une menace extérieure, mais beaucoup plus avec une menace décrite dans une bande dessinée de Pogo en 1936, qui disait simplement: « Je vois l'ennemi et c'est nous. » Tant et aussi longtemps que nous ne serons pas en mesure de renforcer notre propre cadre réglementaire national, il devient de plus en plus difficile de faire face aux répercussions potentielles d'un acteur externe instable.

De plus, les problèmes de défense du cyberspace que j'ai décrits dans les trois exemples précédents, liés au pourcentage de 90 %, touchent essentiellement tous les pays de l'OTAN. Le défi supplémentaire que nous devons relever, c'est que l'interopérabilité de l'OTAN et l'élaboration de doctrines militaires appropriées pour remédier à ces vulnérabilités sont tout simplement sous-développées, et pourtant elles se produisent à un moment où nous traversons une période de grande confrontation avec un autre acteur en particulier.

Il est important de reconnaître que la Russie fait partie des 140 pays que l'IISS a désignés comme étant en train de développer des cybercapacités. Cela signifie que le spectre de la menace ne concerne plus qu'un seul pays. En outre, il est important de reconnaître que, depuis 1997, la Fédération de Russie est l'un des rares États qui ont utilisé le mécanisme des Nations unies pour tenter de définir une voie pour aborder la question de la stabilité dans le cyberspace au moyen d'une approche fondée sur les traités, qui s'at-

taque aux enjeux en amont et en aval du DCA, le droit des conflits armés.

● (0920)

Pourquoi est-il important de s'attaquer à ce problème dès maintenant? Même si je n'ai pas de recommandations à faire au Comité sur les mesures que nous devrions prendre, je peux exprimer clairement ce que nous ne devrions pas faire. Il s'agit, entre autres, de ne pas affaiblir le fonctionnement des mesures de renforcement de la confiance qui nous donnent l'occasion de discuter des répercussions du cyberspace sur les relations entre les États de l'OTAN et l'ensemble des pays de l'OTAN et, deuxièmement, de ne pas couper les canaux visant un engagement, afin d'être en mesure de discuter de ces questions et trouver un terrain d'entente.

C'est important pour plusieurs raisons, mais peut-être que l'une d'entre elles est la plus importante pour nous. La Fédération de Russie, qui est l'objet de la plupart de nos préoccupations dans le domaine cybernétique, a très manifestement lié le risque d'escalade entre le cyberspace et le nucléaire. Pour la Russie, la menace à la sécurité nationale s'étend à ces deux domaines critiques.

Nous avons passé de nombreuses années avant et après 1989 à créer des mesures de renforcement de la confiance dans la chaîne de sécurité nucléaire. La loi Nunn-Lugar adoptée aux États-Unis en est une manifestation. Elle a permis la mise en place de plusieurs points de discussion, plusieurs brise-lames, si vous voulez, pour que nous puissions aborder cette question. On est en train de les annuler, et on ne les remplace par rien d'autre.

De plus, nous n'avons pas eu de canal actif pour discuter des questions cybernétiques avec les Russes depuis un certain nombre d'années, que ce soit de façon bilatérale ou, surtout, dans le cadre d'une séance multilatérale. S'il y a une chose que nous ne devrions pas faire, c'est de nous engager dans une escalade sans réfléchir à notre objectif final. Qu'essayons-nous de réaliser? Qu'est-ce qui constitue la dissuasion dans le cyberspace, et cela existe-t-il si nous n'avons pas été en mesure de définir, d'un point de vue stratégique, ce que la cybernétique signifie pour nous?

Le plus important, c'est qu'en l'absence d'une politique, nous ne devrions pas nous lancer dans un jeu dangereux avec une puissance nucléaire sans stratégie et sans plan de ce que nous voulons, en tant que pays et en tant que membre de l'Alliance.

Merci.

Le président: Merci beaucoup. C'était fascinant, et j'espère qu'il y a de bonnes questions qui nous permettront d'obtenir plus de renseignements.

Je vais céder la parole à M. Robillard pour sept minutes.

Vous avez la parole.

[Français]

M. Yves Robillard (Marc-Aurèle-Fortin, Lib.): Merci, monsieur le président.

Ma question s'adresse à M. Rohozinski.

Dans votre article intitulé « *The internet has made nuclear war thinkable — again* », vous expliquez que le monde nucléaire et le monde numérique sont de plus en plus interreliés. Pourriez-vous nous donner plus de détails sur les liens qui relient le cyberspace aux armes nucléaires?

[Traduction]

M. Rafal Rohozinski: La question porte sur l'interrelation entre le nucléaire et le numérique dans le développement de nouvelles catégories d'armes nucléaires, et pour ce qui est des acteurs en cause. Nous ne sommes pas dans un cours de physique, mais une caractéristique des armes nucléaires, et particulièrement des armes thermonucléaires, est leur capacité de générer une impulsion électromagnétique.

Les armes à impulsion électromagnétique sont des armes qui ont été optimisées à cette fin, et qui présentent la caractéristique de pouvoir porter atteinte à tout système électrique insuffisamment protégé. Pour les pays et les économies de plus en plus tributaires de l'économie numérique et des technologies numériques, la dissuasion n'est plus seulement définie par la capacité de dissuader un acteur qui peut causer des dommages considérables dans le domaine physique. Nous pouvons menacer des centaines de villes avec des armes nucléaires, mais une seule arme à impulsion électromagnétique peut produire des effets de masse qui provoqueraient le chaos dans une vaste gamme d'infrastructures.

Ainsi, le seuil pour que les pays se joignent à un club d'élite et aient la capacité de tenir en otage l'économie numérique mondiale pour une rançon est beaucoup moins élevé que jadis. La Corée du Nord n'a pas besoin de se doter des milliers d'armes nucléaires pour menacer le monde. Il lui suffit de quelques armes nucléaires capables de produire ce genre d'effet.

Deuxièmement, et c'est peut-être plus important dans la perspective des relations OTAN-Russie, la Fédération de Russie et les États-Unis travaillent à la modernisation de leurs capacités nucléaires. Cela comprend le remplacement des systèmes de commandement et de contrôle vieux de plusieurs décennies qui fonctionnaient jadis de façon analogue beaucoup plus robuste. On craint que cette modernisation inspire la mise en oeuvre de technologies qui seront beaucoup plus vulnérables aux effets pouvant être générés par des armes nucléaires conçues pour produire une impulsion électromagnétique et, ensuite, que l'un des moyens d'exercer la dissuasion ne soit plus seulement nucléaire, mais puisse être lui-même cybernétique. En d'autres termes, une cyberattaque contre l'infrastructure de commandement et de contrôle serait peut-être un meilleur moyen de gérer la situation qu'un plafonnement égal du nombre de missiles.

Cette interaction commence à se manifester. C'est certainement ce qui s'est produit dans le cas de la Corée du Nord, mais j'ajouterais qu'elle s'accroîtra nécessairement avec la modernisation des arsenaux nucléaires des deux camps.

• (0925)

[Français]

M. Yves Robillard: Merci.

La question suivante s'adresse à M. Shea.

J'aimerais que vous nous disiez, à titre de secrétaire général adjoint délégué chargé des défis de sécurité émergents à l'OTAN, quel type de menaces la guerre hybride, et plus particulièrement la guerre cybernétique, fait planer sur les pays de l'OTAN.

Pourriez-vous aussi nous dire dans quelle mesure l'OTAN est prête à faire face à la menace que pose la guerre hybride?

M. Jamie Shea: Merci beaucoup de cette question.

La menace de la guerre hybride, comme je l'ai dit, c'est d'effacer la distinction traditionnelle entre la paix et la guerre, et de nous mener vers un monde où chaque domaine est contesté en permanence, vers un monde où la sécurité intérieure devient d'une ampleur stratégique aussi importante que la tâche traditionnelle de défendre nos frontières. Je parle ici de la sécurité des populations et des infrastructures critiques, de la capacité de nos sociétés de bien fonctionner et de la capacité des gens de mener leur vie normalement sans être assujettis à des menaces.

Avec la guerre hybride, le centre de gravité de la défense se déplace en quelque sorte du territoire ou des frontières vers nos populations mêmes. Cela va même jusqu'à toucher ce qui se passe à l'intérieur de la tête de nos citoyens. Comment perçoivent-ils la réalité? Quels messages leur semblent les plus crédibles? Quelle confiance ont-ils en la compétence de leurs dirigeants? Auparavant, la tâche de l'OTAN était assez simple: elle consistait simplement à défendre physiquement nos frontières. À présent, elle devient double. Il faut d'abord mener à bien cette tâche, qui reste importante, surtout avec l'essor des forces russes en Europe de l'Est. C'est pour cette raison que vous avez presque 500 soldats canadiens actuellement déployés en Lettonie. En même temps, il faut devenir de plus en plus compétents dans l'analyse des menaces qui se posent au bon fonctionnement de nos sociétés.

Que faut-il donc faire? Il y a en quelque sorte six axes de réflexion que nous sommes en train de poursuivre.

D'abord, il y a le renseignement. Comment pouvons-nous mieux anticiper et déceler ce genre de menace hybride et distinguer une attaque fortuite d'une attaque délibérément orchestrée? Comment pouvons-nous percevoir et définir plus rapidement et avec plus de précision les menaces afin de pouvoir réagir? Si nous passons des mois et des mois à discuter avant d'en arriver à la conclusion que quelque chose qui marche comme un canard et qui parle comme un canard est effectivement un canard, nous allons être dépassés par la vitesse de ces incidents. Il faut donc, en premier lieu, améliorer nos capacités de renseignement d'anticipation.

Ensuite, il y a la gestion de crise. Est-ce que nous pouvons prendre des décisions rapidement, en temps réel? Le renseignement y est pour beaucoup, mais avons-nous prévu une suite de mesures spéciales d'intervention en cas de crise? Comment pouvons-nous élargir le coffre à outils de mesures que nous pouvons prendre? Comme je le disais, il y a des mesures diplomatiques. Par exemple, vous avez appris cette semaine l'expulsion de plus de 100 diplomates russes par bon nombre de pays pour protester contre l'emploi d'armes chimiques à Salisbury, en Angleterre. Il faut donc des mesures économiques, mais aussi toute une série d'autres mesures qui nous donnent la flexibilité de répondre. À l'OTAN, si l'on s'en tient textuellement à l'article 5 du Traité, nous devons bien sûr attendre qu'une guerre véritable soit déclarée avant de répondre. Nous devons donc élargir la flexibilité de nos options de réponse.

Troisièmement, il y a la question de la communication stratégique. Pouvons-nous être plus aptes à repérer les fausses nouvelles et les opérations d'information et à y répondre?

Ensuite, il y a la résilience de nos infrastructures. Comment pouvons-nous rendre nos centrales nucléaires, nos systèmes électriques et nos systèmes de communications plus résistants? C'est aussi très important.

Enfin, comment pouvons-nous être plus efficaces dans le cyberspace et comment pouvons-nous apprendre de nos partenaires? Prenez un pays comme l'Ukraine, qui est un grand partenaire de l'OTAN. Beaucoup de tactiques hybrides sont déployées contre ce pays. Nous devons aider l'Ukraine, mais, en même temps, apprendre de ses expériences pour empêcher que la même chose ne nous arrive.

• (0930)

[Traduction]

Le président: Merci beaucoup.

Monsieur Bezan.

M. James Bezan (Selkirk—Interlake—Eastman, PCC): Monsieur le président, je tiens à remercier nos témoins d'être venus aujourd'hui et de nous avoir partagé leurs connaissances et leur expérience de ce grave enjeu et de la menace qu'il représente pour l'OTAN et pour le Canada en particulier.

Je sais que nous sommes tous captivés par le contenu cybernétique, la cyberguerre et la guerre hybride qui semble évoluer, surtout depuis l'invasion russe de l'Ukraine. Nous observons des percées technologiques, tant dans les pays de l'OTAN qu'en Russie, en Chine et ailleurs, dans les armes traditionnelles comme les chars d'assaut, les avions à réaction, les navires et les armes nucléaires. Les choses se modernisent, et tout le monde semble avancer au même rythme.

Certaines lectures que j'ai faites me font craindre que nos adversaires proches aient peut-être le dessus grâce à leurs avancées technologiques, comme dans le monde de la cybernétique, des missiles de croisière, des missiles hypersoniques, des armes à impulsion électromagnétique et des armes à énergie directe.

Pouvons-nous nous pencher de plus près sur la situation des pays de l'OTAN par rapport à celle des Russes, des Chinois, des Iraniens et même des Nord-Coréens pour ce qui est de la progression de leurs armes et de leur effet de déstabilisation de notre camp.

Je vais d'abord m'adresser à M. Rohozinski, puis à notre invité par vidéoconférence.

M. Rafal Rohozinski: Le sujet est très vaste, mais je vais vous répondre sur un petit aspect de la question, qui, selon moi, se rapporte spécifiquement au cyberenvironnement même.

Paradoxe intéressant, certaines des attaques les plus réussies fondées sur des codes — si on peut les appeler ainsi — contre les infrastructures essentielles au cours des trois dernières années ont été en fait le remballage du code d'attaque de la National Security Agency, la NSA, qui a été volé pendant l'affaire des Courtiers de l'ombre. Par exemple, il y a eu le démantèlement des systèmes des opérations maritimes de Maersk. Il s'agissait d'une utilisation efficace d'un code remballé.

L'une des choses que nous avons observées dans la façon dont la Russie et d'autres pays utilisent les opérations d'information est la suivante. Voyons de près comment la Russie s'y est prise. Nous avons vu en particulier que sa capacité de développer des techniques, des métiers et des processus liés à l'emploi d'une cyberopération a été très importante. Autrement dit, elle sait ce qu'elle veut faire.

D'un point de vue technique, sa sophistication n'a pas vraiment été bien différente — ni plus poussée ni plus restreinte — que la nôtre. Selon moi, il y a une raison qui a motivé les Russes dans ce

sens. Je dirais que c'est en partie parce qu'ils voient une certaine menace existentielle née de la fermeté croissante de l'OTAN face aux revendications de la Russie le long de ses frontières. Je pense que c'est un durcissement des positions russes en général. Cela reflète-t-il nécessairement une capacité plus sophistiquée que ce que nous avons sur le plan technologique? Ma réponse est non.

M. James Bezan: L'avantage technique et tactique des pays de l'OTAN sur la Russie, la Chine et les autres s'est refermé, n'est-ce pas?

M. Rafal Rohozinski: Non, je ne crois pas. Sur le plan technique, je dirais que les États-Unis, surtout, sont toujours la plus grande puissance cybernétique au monde. Cela me paraît incontestable.

Quant à la portée ou à l'ouverture à l'expérimentation dans le domaine opérationnel, j'estime que les Russes ont affiché une bien plus grande promiscuité, pour ainsi dire. Par conséquent, leur capacité de produire des effets est peut-être plus manifeste que la nôtre. Ce qui ne veut pas dire que les pays membres de l'OTAN n'ont très bien réussi, individuellement, à monter des cyberopérations — certaines connues du public et d'autres moins — mais les visées politiques ont été différentes de celles de la Fédération de Russie, et c'est pourquoi sans doute nous y accordons beaucoup plus d'attention.

M. James Bezan: Monsieur Shea.

M. Jamie Shea: Tout d'abord, oui, bien sûr il y a une diffusion de la technologie pour diverses raisons. La première, c'est qu'il y a 30 ans, la plupart des avancées étaient attribuables au complexe militaro-industriel, comme l'aurait appelé le président Eisenhower. Vous vous rappelez l'invention d'Internet, ou du Téflon du programme spatial.

Aujourd'hui, une bonne part du savoir-faire militaire provient du secteur civil. La cybernétique en est un exemple, tout comme l'intelligence artificielle et les médias sociaux. De même, bien sûr, la technologie civile est beaucoup plus répandue dans le monde. De plus en plus de pays y investissent, naturellement, pour leur économie. Pour ce qui est de la technologie militaire, je pense que nous devons tout simplement la constater.

Deuxièmement, de nombreux pays du monde ont consacré beaucoup d'argent au développement de leurs capacités de R-D et militaires. Le Brésil produit maintenant des sous-marins et des avions de première classe. Il y a quelques jours, j'ai vu que même l'Arabie saoudite avait l'intention de lancer sa propre industrie autonome de la défense. Il y a de plus en plus de pays en deçà du niveau des grandes puissances, si vous voulez, qui s'échangent maintenant du matériel militaire de pointe et du savoir-faire. Le Brésil vend à la Corée du Sud, la Corée du Sud vend à Israël. Il y aura une diffusion dans le monde.

L'autre chose, bien sûr, c'est que des pays comme la Chine — soyons honnêtes — investissent beaucoup plus que nous dans certains domaines. Ainsi, en intelligence artificielle, la Chine investit environ quatre fois plus que les États-Unis en ce moment. La Chine possède aujourd'hui le plus gros et le plus rapide superordinateur au monde et, à ce jour, les universités chinoises produisent environ huit fois plus de doctorats en ingénierie que les États-Unis.

Cela ne veut pas dire qu'ils ont tous 10 pieds de haut, bien sûr que non: ils ont eux aussi leurs faiblesses. Nous l'avons compris lors de la guerre froide, où nous avons systématiquement surestimé l'Union soviétique pendant des années. Cela nous dit que nous devons prendre nos propres sciences et technologies beaucoup plus au sérieux.

Vous avez vu les niveaux de R-D régresser dans de nombreux pays de l'OTAN. Vous avez même vu des gens contester ouvertement la valeur de la science, des preuves scientifiques, et des connaissances scientifiques. Il y a une idée qui est ressortie de la campagne du Brexit au Royaume-Uni, à savoir que nous ne voulons plus entendre les experts — nous en avons ras le bol. Je pense que nous devons accorder plus d'attention à notre propre base scientifique et technologique.

À l'OTAN, certes, nous devons examiner de plus près les répercussions de l'intelligence artificielle, de la bio-ingénierie et des nouveaux drones, etc. sur notre position de défense, et non pas seulement pour accroître notre sensibilisation — les ambassadeurs, par exemple, ont pris une journée la semaine dernière pour parler d'intelligence artificielle — mais aussi pour voir quel effet cela aura sur l'avenir.

Soit dit en passant, si vous voulez bien m'accorder encore un instant, n'oubliez pas non plus que les nouvelles technologies non seulement influencent le champ de bataille traditionnel, comme l'intelligence artificielle, mais qu'elles peuvent aussi se traduire par une guerre plus hybride. Elles jouent à la fois sur l'aspect externe, dont j'ai parlé, et sur l'aspect interne. Elles permettent de faire beaucoup de choses qu'on ne peut pas faire avec un char d'assaut, et c'est pourquoi nous devons nous pencher très sérieusement sur les nouvelles technologies.

J'ai le sentiment que les sociétés libres, pour peu qu'elles y prêtent attention, auront généralement la technologie supérieure à long terme.

• (0935)

Le président: À vous, monsieur Garrison.

M. Randall Garrison (Esquimalt—Saanich—Sooke, NPD): Merci beaucoup, monsieur le président.

Merci à tous les témoins de leur comparution.

Mes premières questions s'adressent à Madeleine Moon, dont j'ai eu le plaisir de faire la connaissance lors d'une Assemblée parlementaire de l'OTAN à Washington il y a quelques années. Nous avons profité des longs trajets en autocar pour échanger des points de vue.

Je vais vous poser des questions dans le contexte de votre participation au comité de la défense de l'Assemblée parlementaire de l'OTAN. Tout d'abord, je m'inquiète de l'abaissement du seuil d'utilisation des armes nucléaires que nous font craindre les propos belliqueux tenus en Corée du Nord. Nous l'avons vu dans le déploiement d'armes nucléaires tactiques. Je me demande si vous avez constaté un engagement renouvelé ou un raffermissement de l'engagement de l'OTAN de mettre en place les conditions d'un monde sans armes nucléaires, que ce soit à l'Assemblée parlementaire ou dans les travaux de l'OTAN même.

Mme Madeleine Moon: Si vous cherchez un monde sans armes nucléaires, commencez donc par le Royaume-Uni. Nous y travaillons, avec d'autres alliés au sein de l'OTAN, depuis longtemps.

Mais les négociations ne se font pas à deux. Il faut s'entendre pour dire que c'est une bonne idée.

Une partie de notre problème vient de ce que certains pays, comme la Corée du Nord, sont en voie de se développer et de développer leurs compétences. Nous avons voulu en contenir d'autres, comme l'Iran, qui travaillent au développement de leurs compétences. Nous ne savons pas très bien où la Russie veut en venir avec ses propos sur la création de nouvelles capacités.

On craint de plus en plus que nous nous dirigeons peut-être vers un nouveau risque nucléaire dans le monde d'aujourd'hui. Selon certaines indications venues de la Russie, l'engagement russe de non-recours à la première frappe est moins ferme que jadis. Par conséquent, nous devons être conscients que nous devons nous protéger et que les armes nucléaires font partie de notre arsenal. Nous disons très clairement que l'OTAN est une alliance défensive et qu'il n'y aura pas de première frappe. Mais nous devons par ailleurs tenir compte des économies émergentes et des nouvelles menaces que crée le développement de la capacité nucléaire et faire de notre mieux pour limiter cette technologie et l'empêcher de se répandre dans les régions où les tensions et les conflits risqueraient davantage de créer un problème avec l'utilisation de ces armes sans accord de non-utilisation de la première frappe.

• (0940)

M. Randall Garrison: Bien entendu, les États-Unis viennent tout juste de publier leur Nuclear Posture Review, c'est-à-dire l'examen de leur position nucléaire, qui semble écarter toute possibilité de première frappe. J'ai déjà demandé comment cela s'inscrit dans la politique de dissuasion de l'OTAN, qui semble exclure la première utilisation des armes nucléaires. Je ne sais pas trop ce qui arrive quand un des principaux alliés de l'OTAN semble avoir abandonné cette position.

Mme Madeleine Moon: La position de l'OTAN demeure la position de l'OTAN. Comme beaucoup de sénateurs américains vous l'ont dit et me l'ont dit, le président Trump dit ce que le président Trump dit, mais la voix la plus forte est celle de l'alliance.

M. Randall Garrison: Merci.

Mon temps de parole est limité.

J'aimerais maintenant parler des femmes, de la paix et de la sécurité, et du travail que vous avez fait à l'Assemblée parlementaire et au comité de la défense. Bien sûr, je pense que nous avons tous été heureux de la nomination d'une représentante de l'OTAN pour les femmes, la paix et la sécurité.

Ma crainte, que d'autres partagent, je le sais, est qu'à partir du moment où une représentante est désignée, les autres croient que c'est à elle de faire avancer ces objectifs, oubliant parfois que cela fait partie du mandat de chacun. Avez-vous des réflexions sur l'impact de la création de ce poste?

Mme Madeleine Moon: Il faut toujours des champions dans tous les domaines. Quelqu'un pour faire avancer les choses.

Chose importante, on parle déjà moins des femmes, de la paix et de la sécurité que du genre, de la paix et de la sécurité. On reconnaît maintenant que le genre est une considération non seulement dans l'activité militaire et la guerre, mais aussi dans notre politique, dans la façon de la pratiquer, ainsi que dans la composition de nos forces armées et dans notre protection et la représentation des valeurs de nos nations. Cela se situe à bien des niveaux.

J'ose espérer que l'arrivée en poste d'une personne qui se concentrera sur ce programme accélérera les choses. Il ne faut pas oublier que, dans toute alliance, on ne peut jamais aller plus vite que le membre le plus lent. Dans certains pays, la question de l'égalité n'est pas aussi avancée qu'ailleurs. Notre façon de voir les femmes dans le monde, dans les forces armées et en politique, de même que notre façon de protéger les civils — parce que la majorité des civils dans toutes les zones de guerre sont des femmes, des enfants et des aînés — est une question cruciale à débattre.

M. Randall Garrison: Hier soir, nous avons élu l'exécutif de notre Association parlementaire canadienne de l'OTAN. Nous avons réélu une des membres de notre comité, Leona Alleslev; une autre membre de notre comité, Cheryl Gallant; et une de mes collègues, Rachel Blaney.

Je me demande si vous avez observé des changements au fil du temps, parce que beaucoup soutiennent que, tant qu'il n'y aura pas environ 30 % de femmes participant à des organisations, cela ne changera rien à la culture. Avez-vous vu un changement, dans l'Assemblée parlementaire de l'OTAN, du nombre de femmes qui y participent, en particulier au comité de la défense?

Mme Madeleine Moon: Question intéressante. Ici, au Royaume-Uni, nous sommes vraiment aux prises avec le nouveau phénomène des femmes en politique, au moment même où, surtout dans les médias sociaux, se multiplient les menaces proférées contre elles. Il est aujourd'hui parfaitement acceptable de laisser un message social menaçant de viol ou d'assassinat une femme qui fait de la politique. Les menaces dont elles font l'objet sont vraiment terribles.

Chose intéressante à l'Assemblée parlementaire — et c'est l'une des raisons pour lesquelles c'est un tel plaisir d'y siéger — la discussion et la conversation se situent à un niveau différent. De fait, il est devenu urgent d'entendre les femmes politiques exprimer une perspective différente. Je pense que c'est important parce que les femmes apportent une perspective différente, une nouvelle compréhension des choses, et qu'elles apportent aussi l'occasion aux pays qu'elles représentent d'apprendre comment l'autre pays voit leurs femmes. Pour moi, c'est l'une des grandes valeurs. La possibilité d'entendre comment les femmes sont projetées dans la société de chacun des membres de l'alliance est aussi cruciale que le travail que nous faisons pour protéger les femmes dans les zones de guerre.

• (0945)

M. Randall Garrison: Merci beaucoup.

Le président: Merci.

Monsieur Gerretsen.

M. Mark Gerretsen (Kingston et les Îles, Lib.): Merci beaucoup, monsieur le président.

Madame Moon, j'aurais quelques questions à vous poser au sujet de l'OTAN, et de la compréhension générale de l'OTAN au sein de la population du Royaume-Uni.

J'apprends, à la lecture de votre parcours, que vous avez déjà été maire et conseillère municipale, et je pense que vous avez un lien bien spécial à ce niveau de la base. Vous entendez ce que beaucoup ont à dire. Pourriez-vous nous donner une idée, d'abord, de la perception générale de l'OTAN aux yeux de la population du Royaume-Uni. Sait-on ce qu'est l'OTAN, ce qu'elle fait effectivement, quel rôle elle joue dans la défense du Royaume-Uni? Tout ce-

la est-il généralement compris? Nous semblons avoir ce problème au Canada et nous ne savons pas si c'est une question d'éducation ou de géographie. J'aimerais bien savoir ce que vous en pensez.

Mme Madeleine Moon: De fait, nous venons tout juste de mettre sur pied un groupe de travail qui se penchera sur la façon de retourner dans l'ensemble de l'alliance et d'expliquer la nature de l'OTAN et de l'alliance, ce qu'elle est, ce qu'elle fait et ce qu'elle représente au juste. Je suis par ailleurs une ex-enseignante, donc passionnée par le fait de visiter les écoles et de parler aux enfants de politique, et des raisons pour lesquelles ils devraient s'y lancer. J'ai aussi une série de conférences que je donne régulièrement sur l'OTAN. Il y a de quoi paniquer lorsqu'on voit combien de nos moins de 25 ans n'ont pas la moindre idée de ce que fait notre force aérienne, de ce que fait notre marine, sans parler de ce que fait l'alliance de l'OTAN.

M. Mark Gerretsen: C'est tout à fait vrai.

Mme Madeleine Moon: C'est extrêmement inquiétant.

M. Mark Gerretsen: Existe-t-il, au Royaume-Uni, des programmes éducatifs déjà en place ou à l'étude visant à promouvoir cette culture? Vous pouvez imaginer, j'en suis certain, à quel point notre population est encore plus déconnectée de ce que fait l'OTAN, étant donné que nous sommes tellement loin du théâtre des opérations auxquelles l'OTAN participe régulièrement. Si on interrogeait des Canadiens au hasard dans la rue, je serais étonné que 5 % d'entre eux connaissent l'OTAN. Je suis curieux de savoir si vous avez mis en oeuvre des programmes dont nous pourrions nous inspirer.

Mme Madeleine Moon: Non, nous n'avons aucun programme ni rien dans notre système d'éducation qui permette aux enfants, dans le cadre de leurs études, de se familiariser avec l'OTAN et d'apprendre pourquoi elle a été créée. C'est pour cette raison que j'ai voulu commencer par là. Il est très important de savoir d'où vous venez pour comprendre où vous allez et pourquoi vous faites ce que vous faites. C'est un gros problème et l'Assemblée parlementaire a décidé de corriger cette lacune.

M. Mark Gerretsen: Pouvez-vous nous expliquer comment vous vous y prenez?

Mme Madeleine Moon: Nous cherchons à remettre dans les programmes scolaires les questions qui requièrent une attention particulière. En tant que députés, nous allons dans nos circonscriptions et nos bureaux de section pour parler de défense et de sécurité et je peux vous assurer qu'à Bridgend, tout le monde sait que je m'occupe de défense. Tous les résidents de Bridgend savent qu'ils recevront périodiquement de l'information de ma part sur les menaces qui planent sur notre pays, les risques auxquels nous sommes confrontés et les raisons qui motivent nos actions.

J'ai récemment reçu dans ma circonscription l'équipe de présentation de l'armée et ce sera bientôt au tour de celle de la RAF de venir. J'adore aller parler de défense et de sécurité aux gens de ma circonscription. Il y a un risque terrible que nos voix soient étouffées par ceux qui voudraient faire croire que la défense et la sécurité sont des enjeux dépassés, empoussiérés et disparus, et que nous sommes en parfaite sécurité, puisque la Grande-Bretagne est si isolée et encore une petite île au large des côtes de l'Europe.

Le Canada aussi peut penser qu'il est en parfaite sécurité de l'autre côté de l'Atlantique. Vous vous réveillez lorsque vos concitoyens sont la cible d'armes chimiques. Nous devons reconnaître que les risques peuvent se présenter sous n'importe quelle forme et n'importe quand.

• (0950)

M. Mark Gerretsen: J'ai une question qui fait suite à votre échange avec M. Garrison au sujet de la situation des armes nucléaires et des différents acteurs dans le monde.

Est-il réaliste, à votre avis, d'imaginer qu'un jour nous pouvons vivre dans un monde exempt d'armes nucléaires?

Mme Madeleine Moon: Nous avons toujours besoin d'aspirer vers quelque chose de plus grand que nous et de plus grand que l'humanité. Oui, je pense que c'est un objectif vers lequel nous devons tendre et que nous devons souhaiter. Quant à la façon d'y arriver, je pense que l'espèce humaine n'en est pas encore là.

M. Mark Gerretsen: D'accord. Merci pour cette réponse.

Monsieur Rohozinski, je reviens à votre allocution d'ouverture et à vos commentaires sur les médias sociaux, les changements qui bouleversent le monde et leur lien avec les armes nucléaires. Vos propos m'ont rappelé la crise des missiles cubains qui aurait probablement été gérée de manière bien différente si elle s'était produite dans le monde d'aujourd'hui.

Je suis curieux de savoir quelles menaces représentent, selon vous, les médias sociaux et le fait que nous vivons dans un monde où l'information est devenue si facilement accessible. Quelle incidence cela a-t-il sur la sécurité et sur l'utilisation d'armes nucléaires?

M. Rafal Rohozinski: Ce sont deux questions distinctes, mais je peux y répondre. Je pense que cela répond en partie à la question que vous avez posée à Mme Moon, à savoir si nous pourrions vivre dans un monde exempt d'armes nucléaires et comment cela est relié à l'OTAN.

Je pense que la déclaration des États-Unis sur le développement d'une nouvelle génération d'armes nucléaires à puissance variable — c'est-à-dire plus facilement utilisables, en ce sens que leur puissance peut être ajustée — envoie un très mauvais message au reste du monde, celui que ces armes peuvent maintenant être utilisées de manière restreinte.

Dans le même ordre d'idées, j'ai aussi dit que le fait que des armes peuvent être conçues pour maximiser la pulsion électromagnétique signifie que les petites puissances désireuses de se doter d'une capacité nucléaire très restreinte seraient soudainement incitées à le faire parce que cela leur permettrait de menacer des pays beaucoup plus grands. Le problème, ce n'est pas la destruction massive de la société, mais les répercussions massives susceptibles de découler de l'utilisation de ces armes.

De plus, si vous reliez ces deux choses, la capacité d'utiliser des armes nucléaires à puissance inférieure pour déployer des capacités nucléaires limitées signifie que l'idée et l'architecture des échanges nucléaires n'ont plus rien à voir avec cette escalade que nous avions avec la doctrine de la destruction mutuelle assurée ou MAD. Quel est le lien avec les médias sociaux? Je pense que le problème résulte en partie de la surmédiation ou la « Jerry Springerization » de la politique, ainsi que de la capacité hautement dangereuse de saisir le moment et de réussir à faire avancer des programmes politiques sur Twitter.

Si vous faites de la politique sur Twitter, vous ne disposez pas des mécanismes nécessaires pour vous engager dans une escalade et la gérer de manière raisonnable. Cela me ramène à mes remarques liminaires. Nous pouvons nous opposer à des pays pairs avec lesquels nous avons une divergence de vues, par exemple

concernant l'intégrité territoriale ou l'aventurisme international. Ce faisant, nous devons cependant disposer de mécanismes nous permettant de prendre des mesures pour renforcer notre confiance mutuelle dans des domaines d'intérêt commun en matière de sécurité, comme l'économie numérique, certaines questions existentielles et autres — toutes ces choses dont nous avons besoin. Si nous nous engageons dans une escalade, nous devons d'abord avoir un plan de match et, ensuite, entretenir un dialogue constant, même durant les combats.

Merci.

M. Mark Gerretsen: Il ne faut pas établir de contact visuel avec l'opposant parce qu'il risque de couper la communication.

Le président: Eh bien, moi je peux. J'essaie seulement de le faire avec élégance.

Nous passons maintenant à la ronde de questions de cinq minutes.

Madame Alleslev, vous avez la parole.

Mme Leona Alleslev (Aurora—Oak Ridges—Richmond Hill, Lib.): Merci beaucoup.

La discussion est d'un niveau exceptionnel aujourd'hui, et je ne saurais vous remercier assez de votre présence.

J'aimerais aborder certains secteurs d'intérêt et m'adresser en particulier à MM. Shea et Rohozinski. Vous nous avez donné un point de vue distinct sur ce qu'il ne faut pas faire et sur certaines priorités de l'OTAN. Nous voulons évidemment prodiguer des conseils au gouvernement, mais il s'agit d'un domaine hautement complexe. Il y a tellement d'éléments en mouvement. Quels devraient être nos trois priorités dans ce domaine? Que devons-nous faire pour travailler plus intelligemment, pas nécessairement plus fort?

Monsieur Rohozinski, peut-être.

• (0955)

M. Rafal Rohozinski: Rapidement, je pense que l'une des raisons pour lesquelles l'OTAN a été une alliance exceptionnellement efficace dans le passé, c'est parce qu'il a misé sur l'interopérabilité et les opérations interarmées.

En ce qui concerne le cyberspace, même si l'on a avancé qu'il s'agissait d'un domaine opérationnel, je pense qu'on a beaucoup de retard.

Concernant la défense des systèmes de l'OTAN, et je pense que M. Shea est très calé dans ce domaine, il y a indéniablement des lacunes en matière de capacité et je pense que les pays doivent faire preuve de leadership pour les combler.

Cependant, l'OTAN est bien plus qu'une alliance militaire, c'est aussi une alliance politique. À cet égard, je pense que le Canada joue un rôle de premier plan en reconnaissant la nécessité que l'OTAN se dote d'une stratégie politique pour faire face à cet environnement déstabilisant qu'est le cyberspace. C'est vraiment important.

Supprimer des points d'engagement et fermer des mécanismes n'est pas la bonne façon de procéder. Je pense que le Canada doit démontrer par son exemple que nous pouvons discuter, même lorsque nous avons des divergences, tout en reconnaissant le fait que l'absence d'escalade prévisible dans ce domaine particulier crée de la volatilité et une menace pour tous.

Je vais laisser M. Shea aborder les deux autres points.

Mme Leona Alleslev: Cela rejoint ce que vous disiez.

Allez-y.

M. Jamie Shea: Je ne suis pas du tout en désaccord avec ce que M. Rohozinski vient de dire.

Je sais que nous devons être brefs, voici donc mes trois principales priorités.

Nous devons investir à l'échelle des pays. L'OTAN n'est que la somme des capacités que ses membres lui fournissent. À part quelques avions AWACS — et nous sommes enchantés que le Canada soit de retour dans ce programme —, l'OTAN dépend justement de son habileté à générer des capacités nationales.

Je suis très heureux, évidemment, de voir que le Canada augmente de beaucoup son budget de la défense. J'ai déjà mentionné les 750 millions de dollars que le Canada consacrera, au cours des prochaines années, à la mise à niveau de sa cyberdéfense, à la création d'un futur centre canadien de cybersécurité et à la mise en place d'une unité nationale de coordination de la cybercriminalité. Ce sont de bons exemples. Bien entendu, nous avons besoin que les pays renforcent leur résilience.

L'OTAN pourrait apporter son aide pour le processus de planification. Elle pourrait conseiller les pays pour qu'ils investissent là où leurs investissements seront probablement les plus rentables. Nous pouvons apprendre les uns des autres. Nous pouvons donner aux pays des objectifs réalistes, mais nous devons atteindre progressivement la cible de 2 % du PIB d'ici quelques années, en raison de tous les conflits auxquels nous sommes confrontés, qu'ils viennent de l'est, du sud, sur du front intérieur dont nous avons parlé aujourd'hui. Ce sont les trois fronts stratégiques où l'OTAN doit s'engager. Et nous avons besoin d'atteindre la cible de 2 % afin d'arriver à générer l'ensemble des capacités dont nous aurons besoin.

La deuxième priorité est la relation entre l'OTAN et l'Union européenne. Même si le Canada n'est pas membre de l'Union européenne, 22 pays de l'OTAN en font partie. En ce qui concerne cette relation hybride, la coopération entre les deux institutions est primordiale. L'Union européenne possède des capacités — l'argent pour la recherche et le développement, le nouveau fonds pour la défense de 5,5 milliards d'euros en voie d'établissement afin de promouvoir plus de projets de recherche et de développement, et les efforts déployés pour réglementer l'environnement. Pensez à la directive générale sur la protection des données qui sera bientôt émise et aux efforts déployés pour protéger l'infrastructure essentielle. Pour être franc, l'Union européenne possède beaucoup de capacités que l'OTAN n'a pas, mais l'inverse est également vrai, surtout dans le domaine militaire. La solution consistera à amener ces deux organisations à collaborer, non seulement pour organiser des séminaires à Bruxelles, mais pour mettre leurs forces en commun.

Enfin, il est important de procéder à des exercices. Les défis actuels, comme je viens de le dire, nous posent des difficultés. Comment doit se faire l'affectation? À quel moment? Comment classer une attaque hybride? Comment réagir? Pour être franc, comme pour toute autre activité de la vie quotidienne, il faut s'entraîner sans cesse, non seulement sur le plan militaire — nous faisons beaucoup d'exercices —, mais également sur le plan politique, en menant des consultations en cas de crise et en essayant de déterminer quelle mesure est la mieux adaptée à la situation. Comme dans

la vie courante, plus nous nous entraînons, mieux nous sommes en mesure d'identifier la véritable menace et de la gérer.

Mme Leona Alleslev: Merci beaucoup.

Le président: C'est à vous, madame Gallant.

Mme Cheryl Gallant (Renfrew—Nipissing—Pembroke, PCC): Je vous remercie, monsieur le président.

Monsieur Rohozinski, il a fallu des parlementaires, des gens d'expérience comme vous qui participent à des groupes de réflexion, ainsi que des universitaires et des chercheurs du secteur commercial pour convaincre l'OTAN qu'il fallait considérer le cyberspace comme étant un nouveau domaine. Comme il a fallu une décennie pour y arriver, quel sera, d'après vous, le prochain domaine opérationnel?

• (1000)

M. Rafal Rohozinski: Pour être honnête, le cyberspace dépasse de beaucoup la définition que nous en avons faite. L'émergence de systèmes d'IA autonomes nous amène vers des domaines qu'il est très urgent de comprendre, pour la simple raison que les cycles décisionnels sur le fonctionnement futur de ces systèmes auront une incidence sur nous.

Le fait que nous ayons commencé à décloisonner la guerre biologique chimique, la guerre nucléaire, la guerre conventionnelle et la guerre hybride signifie que nous avons beaucoup de travail à accomplir, davantage sur le plan politique que pour définir ce domaine.

Nous avons parlé précédemment de la politique civile militaire. Je pense que nous avons plus ou moins oublié son incidence sur les relations entre États au cours des 15 dernières années, dans la foulée de la fin de la guerre froide, en pensant que nous avions réglé les problèmes grâce à la Convention sur l'interdiction des armes chimiques, au Traité sur la réduction des armements stratégiques ou START, et aux différents traités sur les armes nucléaires.

Je pense qu'il reste beaucoup de travail à accomplir, non pas tant pour définir les domaines qui peuvent être perturbateurs, mais en faisant l'examen de nos propres règles ou institutions — des Nations unies jusqu'à nos politiques intérieures. Les répercussions sur les domaines cyber, chimique et nucléaire commencent à s'enchevêtrer et c'est justement le défi que nous devons relever.

Mme Cheryl Gallant: Monsieur Shea, avez-vous quelque chose à ajouter?

M. Jamie Shea: Si vous m'en donnez la possibilité, j'ajouterais très brièvement que je suis d'accord avec l'idée que l'une des priorités clés est de rétablir les lignes rouges. Personnellement, je crois sincèrement que l'utilisation d'armes chimiques au Royaume-Uni s'explique par le fait que nous n'avons pas déployé assez d'efforts pour mettre fin à leur utilisation en Syrie. Nous n'avons pas respecté les lignes rouges que nous avons nous-mêmes tracées et, par conséquent, nous n'avons pas appliqué la Convention sur les armes chimiques.

Vous avez beaucoup parlé du nucléaire; nous ne pouvons pas nous permettre de négliger les normes nucléaires. Si nous ne prenons pas des mesures énergiques contre les cyberattaques, surtout en ce qui a trait à des logiciels vraiment destructifs comme Wanna-Cry et NotPetya, nous envoyons alors le signal que ces attaques sont désormais acceptables, qu'il y a beaucoup à gagner et peu de risque. Nous devons réagir différemment et réagir à ces violations des normes internationales, non seulement en cas de génocide, mais à toute utilisation de ces nouvelles armes à haut risque. Il faut envoyer le message que ces attaques seront contre-productives, qu'il y a davantage à perdre qu'à gagner, que les gains sont très faibles. Cela prendra du temps, mais je pense que c'est la solution.

Concernant la deuxième priorité — et je suis d'accord avec M. Rohozinski à cet égard —, c'est que nous devons nous investir beaucoup plus tôt et beaucoup plus rapidement dans les nouvelles technologies émergentes comme l'intelligence artificielle ou les systèmes d'armes autonomes. Cela veut dire que nous devons nous demander s'il existe des usages perfectionnés de ces technologies que nous pourrions mettre au point pour mieux nous défendre. Par exemple, l'informatique quantique peut fournir beaucoup de solutions en matière de cyberdéfense, ce serait une bonne chose.

Nous savons par expérience que ces nouvelles technologies ont leur bon côté, par exemple l'Internet, mais aussi leur côté obscur, et que nous devons agir plus rapidement pour essayer de faire obstacle à ce côté néfaste.

M. Rohozinski a, tout à fait, raison de signaler qu'avec les systèmes d'armes autonomes susceptibles d'être utilisés sans aucune intervention humaine dans le processus décisionnel, nous devons commencer à réfléchir aux normes dont nous avons besoin en matière de contrôle des armes et chercher un moyen de mobiliser des spécialistes afin que nous puissions tracer une ligne rouge pour empêcher l'utilisation illicite de ces armes.

Enfin, je ne crois pas qu'il y aura un nouveau domaine, mais nous devons cependant réfléchir à la manière dont les domaines existants et les gens qui y travaillent peuvent contribuer à la cyberdéfense, et comment les cyberspécialistes peuvent renforcer notre capacité dans les domaines existants.

M. Rohozinski a fait remarquer, à juste titre, que le problème que pose la multiplication des systèmes d'armes sur la plateforme Windows 2.0 et les vulnérabilités qui pourraient en découler.

Voilà les trois points que je voulais aborder en réponse à cette question extrêmement intéressante.

Mme Cheryl Gallant: D'accord.

Au sujet des cryptomonnaies, je sais que les gouvernements cherchent à trouver un moyen de les taxer, mais nous les considérons plutôt comme des menaces potentielles. Des terroristes ou autres belligérants pourraient s'en servir pour transférer de l'argent et financer des activités; or, quand nous cherchons à retracer ces gens-là, nous examinons toujours leurs opérations financières.

Nous observons actuellement un mouvement aux États-Unis en matière de réglementation des valeurs mobilières, mais du point de vue de la sécurité nationale, et plus globalement du point de vue de l'OTAN, que devrions-nous faire en tant que parlementaires et législateurs pour que cette capacité de surveillance financière soit sous contrôle?

M. Jamie Shea: Eh bien, je...

Le président: Je suis désolé, je vais devoir vous interrompre parce que notre temps est écoulé et que cette réponse nous retardera encore davantage.

Je donne maintenant la parole à M. Sheehan.

M. Terry Sheehan (Sault Ste. Marie, Lib.): Merci beaucoup, monsieur le président.

Je suis ravi d'avoir l'occasion de poser quelques questions à nos témoins. C'est un sujet très important et j'aimerais féliciter le Comité d'avoir entrepris cette intéressante étude. Je suis venu ici à quelques reprises, et c'est vraiment important.

Messieurs les témoins, vous nous avez livré des témoignages extraordinaires. Je vous en remercie.

Voici ma première question. J'ai beaucoup parlé de l'OTAN, et nos témoins de Londres — une tierce partie, un autre pays — pourraient donner leur avis. Comment est la relation canado-américaine avec l'OTAN? Diriez-vous qu'elle est bonne ou mauvaise?

● (1005)

Mme Madeleine Moon: Il m'est difficile de répondre à cette question. Pour nous, les Canadiens sont très différents des Américains. À nos yeux, les Canadiens sont plus britanniques, si l'on peut dire.

Des députés: Oh, oh!

Mme Madeleine Moon: Le Commonwealth nous unit beaucoup plus étroitement, je pense. Nous avons davantage en commun. Nous sommes proches des Américains sur le plan militaire, mais entre nous, le courant passe mal. Surtout quand on voit ce qui se passe avec les communications Twitter qui sortent des États-Unis, cela crée une distance.

Cela étant dit, la langue anglaise reste un lien fort et notre histoire, en particulier le soutien que nous nous sommes donné les uns aux autres pendant la Première et la Seconde Guerre mondiale, demeure un point crucial pour nous.

Eu égard aux menaces futures, est-il besoin de souligner l'importance d'une plus grande honnêteté et transparence envers nos propres populations? Je dis cela parce que le cynisme est de plus en plus répandu dans les médias sociaux. Notre population aujourd'hui n'est pas aussi résiliente qu'elle devrait l'être. Nous devons lui apporter pour notre part la décence et l'intégrité qu'elle mérite et l'aider à comprendre les menaces et les valeurs que nous défendons. Nous devons en faire davantage avant de passer à la prochaine menace liée à la capacité. La plus grande menace à notre capacité, c'est de miner les valeurs de la démocratie en n'étant pas aussi direct et honnête avec notre population concernant les menaces qui existent et ce que nous essayons de faire pour les contrer.

M. Terry Sheehan: Compris.

M. Jamie Shea: Tout d'abord, j'ai l'impression que le Canada montre encore une fois qu'il donne du muscle à l'OTAN, en réintégrant le programme AWACS et en prenant l'initiative de repositionner des troupes canadiennes en Europe maintenant — même si, après la guerre froide, nous ne savions pas que cela serait de nouveau nécessaire. Vous avez répondu à l'appel en prenant la tête du bataillon multinational — et le plus compliqué aussi — en Lettonie. Cela démontre que le Canada partage le fardeau, augmente son budget de défense. Cela signifie que vous parlez haut et fort au sein de l'OTAN aujourd'hui. Vous avez démontré qu'il ne s'agit pas seulement de paroles, mais de gestes, comme votre engagement envers l'Afghanistan ou les Balkans dans le passé. C'est essentiel.

Deuxièmement, le Canada défend les normes. J'ai mentionné dans mon exposé qu'il était essentiel non seulement de produire plus d'armes, mais aussi de produire des normes et de bonnes idées. Le Canada a toujours été parmi les premiers à proposer des normes depuis l'époque où je travaillais avec des gens comme Michael Ignatieff et Lloyd Axworthy. Il y a beaucoup de travail à faire.

Je suis tout à fait d'accord avec tout ce qui a été dit sur les femmes, la paix et la sécurité; le grand rôle de l'ambassadeur Hutchinson et la résolution 1325 du Conseil de sécurité. J'espère toutefois que le Canada ira plus loin et qu'il proposera d'autres types de normes au sein de l'OTAN, que nous devrions élaborer, en particulier dans les domaines du contrôle des armements et de la cybersécurité. Vous avez un rôle de leadership au sein du G7, qui pourrait aussi offrir une tribune appropriée.

Enfin, du point de vue de mon propre pays, vous avez signé un accord commercial avec l'Union européenne. Malheureusement, nous n'avons pas encore l'accord commercial avec les États-Unis que nous espérons. Vous avez démontré qu'un grand pays nord-américain peut en signer un. Dans mon pays, quand on parle de Brexit, on parle toujours du Canada plus, ou du Canada plus plus.

Je suis d'accord avec Madeleine: ouvrir la voie au multilatéralisme, à l'ordre international libéral fondé sur des règles. Vous avez beaucoup de pouvoir à cet égard, et c'est un message que tout le monde doit entendre.

M. Terry Sheehan: Merci.

Le président: Monsieur Yurdiga.

M. David Yurdiga (Fort McMurray—Cold Lake, PCC): Merci, monsieur le président. J'aimerais souhaiter la bienvenue à nos invités d'aujourd'hui. Leur témoignage est très important. J'ai appris beaucoup de choses aujourd'hui, et je vous en remercie beaucoup.

Nous sommes tous très préoccupés par la cybersécurité, la guerre hybride et les capacités nucléaires de certains pays voyous. C'est très préoccupant.

Ma première question portera sur la sécurité de l'OTAN, les renseignements classifiés et les renseignements généraux. Est-ce que tous les membres de l'OTAN ont le même accès à tous les renseignements? Sinon, qui détermine le niveau d'accès accordé à chaque membre?

Monsieur Rohozinski.

• (1010)

M. Rafal Rohozinski: À mon avis, il vaudrait probablement mieux poser la question à M. Shea puisqu'il représente l'OTAN.

M. David Yurdiga: Monsieur Shea.

M. Jamie Shea: D'accord. Tout d'abord, non.

Il y a beaucoup d'accords bilatéraux d'échange de renseignements. Vous connaissez le Groupe des cinq, bien sûr, parce que le Canada y joue un rôle important, traditionnellement. Avec cette division conjointe du renseignement et de la sécurité qui existe depuis un peu plus d'un an, l'OTAN peut aujourd'hui mener un effort concerté pour accroître l'échange de renseignements en son sein en formant de nombreux groupes. On établit par là pour la première fois un lien entre le renseignement civil et le renseignement militaire et on encourage les alliés à partager davantage. Nous avons maintenant un système appelé BICES — encore un terrible acronyme de l'OTAN. C'est un organisme distinct qui permet à tous les alliés et partenaires de l'Union européenne de déposer les rapports de renseignement qu'ils sont disposés à partager avec leurs alliés. Ils peuvent choisir le niveau de classification et les destinataires. C'est un système à participation volontaire, mais le fait qu'il soit volontaire encourage davantage le partage de renseignements que ne l'aurait fait un système imposé uniformément à tous.

La situation évolue progressivement, mais le pays qui émet des renseignements aura toujours, toujours, le privilège fondamental et le droit de déterminer ce qu'il veut partager et avec qui. L'OTAN pourrait servir de pivot au système, mais ne pourra pas toucher à ce droit national fondamental.

M. David Yurdiga: Merci.

M. Rafal Rohozinski: J'ajouterais que l'échange de renseignements est fondé sur le fait de savoir quels renseignements sont vraiment utiles pour le domaine. L'un des défis que nous pose la cybernétique consiste justement à savoir quels sont les renseignements significatifs et exploitables sur lesquels on peut travailler.

Les indicateurs de compromis, que partagent maintenant les pays de l'OTAN, tant au niveau commercial qu'au niveau classifié, sont une chose, mais comment partager l'information sur, par exemple, le trafic émergent sur les médias sociaux qui peut avoir un impact direct dans le cadre d'un impact hybride contre un pays membre de l'OTAN? Une stratégie conjointe de défense nationale ou de défense justifie-t-elle la surveillance du trafic des médias sociaux? Nombre de ces questions de politique restent sans réponses.

En fait, en guise de conclusion ou de déclaration à ce sujet, je pense que vous avez un problème ici en tant que parlementaires. Le cyberspace a sur notre société une incidence démesurée par rapport à l'idée que l'on s'en fait aujourd'hui. Nous avons au Canada un mécanisme connu sous le nom de commission royale qui nous permet de traiter de problématiques qui échappent à la simple responsabilité ministérielle. J'ai témoigné devant plusieurs comités de parlementaires et le Sénat. J'ai travaillé avec différents ministères. Dans chaque cas, le cloisonnement de la prise de décisions signifie qu'il n'y a pas d'approche holistique qui nous permette à nous Canadiens et à vous parlementaires d'encadrer dans une perspective d'ensemble la question qui se manifeste dans le domaine de la politique intérieure, de notre politique d'État, ou celui plus circonscrit de la défense nationale. Je vous encourage, mesdames et messieurs les parlementaires, à comprendre qu'il s'agit d'une question qui touche l'ensemble de la société et dont il faut débattre et, comme l'a dit Mme Moon, que nous ne devons pas ménager nos efforts pour tenter d'en définir précisément les contours.

Merci.

M. David Yurdiga: Merci.

Combien de temps me reste-t-il?

Le président: Il vous reste environ une minute.

M. David Yurdiga: D'accord. Excellent.

Il y a quelque chose que j'essaie de comprendre. Nous avons l'OTAN et l'Assemblée parlementaire. Quel est l'organe qui détermine ce qui est pertinent pour chaque membre de l'OTAN? Évidemment, tous les membres de l'OTAN ne sont pas impliqués dans une tâche spécifique. Y a-t-il un organe qui détermine ce qui est pertinent pour tel ou tel membre de l'OTAN et que tel autre ne l'obtiendra pas parce que ce n'est pas pertinent pour lui? Y a-t-il un organe qui prend ce genre de décision?

M. Rafal Rohozinski: Je vous répondrai de manière très indirecte. Nous avons des difficultés à cet égard, même à l'échelle nationale. Aucun mécanisme n'oblige, par exemple, les banques à partager entre elles des informations sur des menaces les concernant potentiellement toutes. Rien n'oblige les entreprises de télécommunications, par exemple, à informer les organisations en aval, qu'il s'agisse des banques ou des gouvernements, de choses qui peuvent les toucher sur le plan de l'échange de renseignements en matière de cybernétique. C'est un problème en cascade qui s'étend jusqu'à l'OTAN.

Je pense que la réponse honnête est non, il n'y a pas de mécanisme. Il y a des mécanismes qu'on essaie d'adopter, mais il n'y a pas de solution à ce problème. C'est l'un des défis.

M. David Yurdiga: Merci.

Le président: C'est à peu près tout le temps que vous aviez, à moins que vous ne puissiez caser une question et une réponse en trois secondes.

• (1015)

M. David Yurdiga: Vous pouvez renoncer à mes trois secondes.

Le président: Députée Alleslev.

Mme Leona Alleslev: Merci beaucoup.

J'aimerais pousser un peu plus loin vos commentaires, Madeleine, sur la façon dont nous pouvons nous assurer que nous communiquons avec notre société. Cette étude porte sur les raisons pour lesquelles le Canada est important pour l'OTAN et pourquoi l'OTAN est importante pour le Canada. Bien sûr, il est de notre devoir de parlementaires de poursuivre ces conversations dans nos circonscriptions. J'espère que vous aurez un jour l'occasion de parler aux Canadiens dans une circonscription. Du point de vue du Royaume-Uni et bien sûr en tant que membre fondateur de l'OTAN, comment expliqueriez-vous pourquoi cela devrait être important pour le Canada et pourquoi il est ou devrait être important pour l'OTAN que le Canada en soit membre?

Mme Madeleine Moon: On peut voir ça de bien des façons. Je le vois à la lumière d'une question antérieure. On commence par ses propres frontières. Où suis-je dans le monde? Quelles sont les frontières de mon pays? Qui sont les voisins? Ensuite, on se demande quelles sont les menaces qui existent dans le monde et comment elles pourraient se manifester à nos frontières. De quels moyens de défense disposons-nous pour nous protéger?

On peut dire ce genre de choses dans l'optique de la « petite Grande-Bretagne », comme on dit, mais on doit ensuite se demander de quels amis on a besoin. Qui sera à nos côtés? L'histoire de la Grande-Bretagne remonte à très loin et je pense que les Malouines ont été la seule fois où nous avons combattu seuls. Jamie aura peut-être un autre exemple en tête. Le reste de notre histoire est celle de

combats dans le cadre d'alliances. Dans le monde d'aujourd'hui, il est très difficile de faire cavalier seul. Il faut être solidaire non seulement des gens qui vont se battre avec vous en tant que pays, mais aussi de ceux qui partagent vos valeurs, qui ne vont pas saper votre société en affaiblissant ces valeurs par des compromis, en permettant l'utilisation d'armes chimiques, par exemple, ou la réduction en captivité des femmes et leur utilisation comme esclaves sexuelles. C'est le genre de monde avec lequel on veut être allié et avec lequel on veut travailler.

Nous devons aussi expliquer à nos populations que ce monde n'a pas disparu. Il n'a pas pris fin en 1945. Le monde est encore très dangereux. Certains dangers sont nouveaux et différents, mais la nécessité pour nous d'être résilients et constamment vigilants est toujours là et où que vous soyez dans le monde, les risques sont présents.

Le Canada a une double façade. L'une sur le Pacifique, l'autre sur l'Atlantique. Une autre s'ouvre maintenant sur ce nouveau territoire qu'est l'Arctique. Vous êtes dans des eaux bigrement dangereuses. J'espère que votre peuple comprendra alors pourquoi l'OTAN est aussi importante pour vous que pour les petites îles au large des côtes de l'Europe qui sont la Grande-Bretagne.

Mme Leona Alleslev: Merci beaucoup. Pour passer à l'étape suivante, pouvez-vous nous donner votre point de vue sur le fait que tous les points de l'histoire ne sont pas égaux. Diriez-vous que nous sommes à un point où la température monte, reste la même ou diminue?

Mme Madeleine Moon: Je dirais catégoriquement qu'elle monte, et ce depuis un certain temps. On m'attaque depuis quelque temps comme un guerrier de la guerre froide qui veut nous ramener dans le passé. Cependant, je pense que nous avons longtemps fermé les yeux sur les risques qui nous guettent. Jamie a raison, je pense, les décisions que nous avons prises au sujet de ces armes chimiques, en particulier, n'ont fait qu'empirer les problèmes. Nous devons nous réveiller et cesser d'être aussi complaisants que nous le voudrions à l'égard de notre sécurité et des alliances de défense auxquelles nous souscrivons; il nous faut aussi dire à nos populations que le monde est un endroit plus dangereux et que les dangers se rapprochent de nous...

Mme Leona Alleslev: Comme le dit votre Sir Richard Barrons, nous devons voir le monde tel qu'il est et non tel que nous souhaiterions qu'il soit.

Mme Madeleine Moon: En effet.

Mme Leona Alleslev: Monsieur Shea, j'aimerais que vous développiez un peu votre commentaire sur le droit international et les lacunes dans le domaine cybernétique peut-être. Que devons-nous faire à l'échelle nationale dans ce domaine?

• (1020)

Le président: Malheureusement, je vais devoir céder la parole à M. Garrison pour la dernière question officielle.

Mme Leona Alleslev: D'accord.

Merci beaucoup.

M. Randall Garrison: Ma question s'adresse à M. Shea. J'aurai un aparté avec lui à propos d'une remarque particulièrement contraignante qu'il a faite dans sa déclaration préliminaire; je ne veux pas m'attarder là-dessus maintenant.

Vous avez parlé du concept de ligne rouge pour des choses comme les armes chimiques et du rôle que pourrait jouer le Canada pour promouvoir certaines normes sur le contrôle des armes.

Pourriez-vous nous en dire un peu plus sur le rôle de l'OTAN dans l'établissement de lignes rouges au regard des nouvelles menaces nucléaires que représentent les armes tactiques et sur l'idée que l'OTAN poursuive d'autres activités dans le domaine du contrôle des armes?

M. Jamie Shea: Tout d'abord, pour ce qui est des remarques contrariantes, excusez-moi — il n'y avait rien là de délibérément contrariant, mais je me ferai un plaisir d'y revenir en privé, monsieur.

Deuxièmement, l'examen des nouveaux défis — et on a beaucoup parlé aujourd'hui de cybernétique, mais l'attaque de Salisbury montre également que les armes chimiques sont toujours utilisées — doit nous amener à réfléchir à ce que l'on peut faire au sein de l'alliance, en collaborant pour accroître notre résilience nationale face aux armes chimiques si jamais elles devaient être utilisées de nouveau.

Il est clair, par exemple, qu'il nous faut être en mesure de détecter le type d'arme très tôt, d'analyser exactement de quoi il s'agit et, par conséquent, de partager l'expertise entre les laboratoires de l'OTAN. Comme vous l'avez vu dans le cas du polonium 210 lorsqu'il a été utilisé à Londres en 2006, il peut se répandre partout, à différents endroits, de sorte que la méthode de suivi est particulièrement importante pour protéger nos populations civiles. Bien sûr, il serait important de former des forces d'intervention et ce genre de choses. Pour des raisons évidentes, nous avons en quelque sorte abandonné la voie de la médecine et la recherche de ce qui pourrait être efficace. Un bon exemple serait d'essayer d'utiliser l'OTAN pour revitaliser certaines compétences essentielles, tant au niveau national qu'au niveau de l'OTAN.

Dans le domaine nucléaire et cybernétique, il y a aussi beaucoup de bon travail à faire. Vous vous souviendrez de l'initiative de sécurité nucléaire que le président Obama a lancée pour surveiller ces matières. Encore une fois, la contrebande des armes chimiques a repris. C'est clair, sinon elles n'auraient pas pu être utilisées à Londres, alors comment pouvons-nous travailler ensemble pour trouver des façons efficaces de repérer ces choses lorsqu'elles tra-

versent les frontières, y compris l'échange de renseignements, et travailler avec les pays et les partenaires pour veiller à ce qu'ils gardent ces choses sous clé et verrouillées — quand ils en ont?

Dans le domaine cybernétique, il y a les MRCS. Comment aboutir à des accords internationaux qui préviennent les cyberattaques contre les infrastructures essentielles comme les hôpitaux, les réseaux électriques et les choses dont nos populations peuvent dépendre? Les États-Unis et la Chine, par exemple, ont conclu un accord qui vise à interdire ce genre d'attaques, alors comment à partir de là en arriver à une entente à l'échelle internationale?

Il y a beaucoup de bon travail à faire dans ce domaine. Je disais simplement poliment et humblement qu'un pays comme le Canada, qui a une bonne tradition intellectuelle et diplomatique, serait bien placé pour prendre l'initiative au sein de l'OTAN également.

Merci.

Le président: Je vous remercie tous les trois d'avoir participé à notre discussion d'aujourd'hui.

Comme je l'ai mentionné au début, c'est notre dernière réunion officielle sur ce sujet. Nous allons maintenant parler des instructions de rédaction et des recommandations au gouvernement du Canada sur la façon d'améliorer les choses.

Cette conversation a commencé il y a quelques mois. Évidemment, après les dernières élections présidentielles américaines, on a beaucoup parlé de l'OTAN. À la fin, on ne parlait plus que de partage du fardeau et des dépenses pratiquement, ce qui est important. La plupart des gens seraient d'accord pour le reconnaître, mais la participation, les capacités et toutes sortes d'autres choses sont aussi importantes. Il est important de tenir compte de ces facteurs et leur problématique est plus complexe que celle consistant à savoir simplement qui dépense quoi pour l'OTAN. Nous avons fort à faire.

Je tiens à vous remercier encore une fois de votre participation à cette conversation. Nous allons suspendre la séance pour nous mettre au travail.

Merci beaucoup.

[La séance se poursuit à huis clos.]

Publié en conformité de l'autorité
du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la Loi sur le droit d'auteur. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre des communes.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la Loi sur le droit d'auteur.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à l'adresse suivante :
<https://www.noscommunes.ca>

Published under the authority of the Speaker of
the House of Commons

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its committees are hereby made available to provide greater public access. The parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its committees is nonetheless reserved. All copyrights therein are also reserved.

Reproduction of the proceedings of the House of Commons and its committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the Copyright Act. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the Copyright Act.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the House of Commons website at the following address: <https://www.ourcommons.ca>