CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la défense nationale

NDDN • NUMÉRO 077 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mardi 30 janvier 2018

Président

M. Stephen Fuhr

Comité permanent de la défense nationale

Le mardi 30 janvier 2018

● (0845)

[*Traduction*]

Le président (M. Stephen Fuhr (Kelowna—Lake Country, Lib.)): Nous allons commencer.

Je souhaite la bienvenue à tout le monde à la réunion du Comité ce matin.

Chers collègues, quel plaisir de vous revoir. Messieurs, soyez les bienvenus.

Nous entendrons aujourd'hui Len Bastien, dirigeant principal de l'information de la Défense et sous-ministre adjoint responsable de la gestion de l'information, ainsi que le commodore Richard Feltham, directeur général de Cyberespace, dans le cadre de nos délibérations portant sur le Canada et l'OTAN dans le domaine cybernétique. Merci beaucoup d'être venus.

Je vais céder la parole à M. Bastien. Vous aurez un maximum de 10 minutes pour faire une déclaration.

M. Len Bastien (dirigeant principal de l'information de la Défense et Sous-ministre adjoint, Gestion de l'information, ministère de la Défense nationale): Merci, monsieur le président.

[*Français*]

Cela me fait grandement plaisir d'être parmi vous ce matin.

[*Traduction*]

En tant que sous-ministre adjoint responsable de la gestion de l'information et dirigeant principal de l'information de la Défense, je dois m'assurer que la Défense dispose d'un environnement d'information fiable, sûr et intégré afin d'appuyer les activités de la Défense et les opérations militaires. Je rends des comptes au sous-ministre en ce qui a trait à l'administration, à la gestion financière et aux ressources humaines, et au chef d'état-major de la Défense pour le développement et la préparation de la force, notamment dans le cyberespace.

Le directeur général responsable du cyberespace fait partie de mon organisation; le commodore Feltham, qui m'accompagne aujourd'hui, vous en parlera tantôt.

Comme vous le savez, la nouvelle politique de défense du Canada représente une nouvelle vision: assurer la protection au pays, la sécurité en Amérique du Nord et notre engagement dans le monde. En tant que pays du G7 et membre fondateur de l'OTAN, le Canada manifeste son grand intérêt pour la stabilité mondiale. C'est donc à cette fin que nous continuerons d'assumer des rôles de premier plan et nous miserons sur l'interopérabilité dans la planification et le développement de nos capacités pour assurer une collaboration harmonieuse avec nos alliés et nos partenaires, en particulier l'OTAN.

À titre de représentant du MDN auprès du Bureau de consultation, de commandement et de contrôle de l'OTAN et auprès du Comité de surveillance de l'Agence de l'OTAN, je suis venu aujourd'hui pour discuter de la participation du Canada au sein de l'OTAN en ce qui concerne la gestion de l'information et la technologie de l'information. Je bénéficie de l'appui d'experts qui proviennent de tous les secteurs du MDN et qui participent à plusieurs groupes multinationaux sur les capacités. Le Canada contribue de façon importante aux programmes qui soutiennent les activités d'élaboration de politique et de développement technique en matière de gestion de l'information et de technologie de l'information sous la tutelle du bureau.

L'interopérabilité dans toute l'Alliance dépend largement de l'application uniforme et du respect des politiques de l'OTAN en matière de gestion de l'information et de la technologie de l'information. Il existe trois organisations principales chargées de faire respecter les politiques.

Premièrement, il y a le Conseil de l'Atlantique Nord, au sein duquel le Canada est représenté par son ambassadeur auprès de l'OTAN. Le conseil approuve le cadre de conformité avec les politiques de consultation, de commandement et de contrôle, et demande aux organismes de l'OTAN de mettre en oeuvre ces politiques et de l'informer des exemptions, des changements aux politiques et des nouvelles politiques.

Deuxièmement, il y a le Bureau de consultation, de commandement et de contrôle de l'OTAN, qui est l'organe multinational supérieur chargé d'établir les politiques. Il relève du Conseil de l'Atlantique Nord et du Comité des plans de défense en ce qui concerne les questions de politique, notamment l'interopérabilité des réseaux de l'OTAN et des systèmes nationaux. Ses priorités sont l'échange d'information et l'interopérabilité, ce qui comprend la cyberdéfense, l'assurance de l'information, le renseignement interarmées et la surveillance et la reconnaissance. La stratégie du Bureau de consultation, de commandement et de contrôle indique que l'OTAN s'engage à mettre en oeuvre ces capacités. Elle met l'accent sur la nécessité de moderniser et de rendre interopérables les forces mises à contribution par les États membres et les partenaires de l'OTAN.

Troisièmement, il y a le Comité de surveillance de l'Agence, qui est l'organe de gouvernance organisationnel de l'Agence d'information et de communication de l'OTAN et qui relève du Conseil de l'Atlantique Nord. Son rôle consiste à s'assurer que l'Agence d'information et de communication peut atteindre ses objectifs en gérant ses ressources et son rendement. Le Canada présidera cette agence pendant les deux prochaines années.

L'Agence d'information et de communication de l'OTAN a été créée en 2012 pour assurer les services, l'approvisionnement et le soutien en matière de gestion de l'information et de technologie de l'information dans l'ensemble de l'OTAN dans des domaines tels que les systèmes de commandement et contrôle, les communications tactiques et stratégiques et les systèmes de cyberdéfense.

En avril 2017, mon groupe a accueilli à Ottawa une conférence de trois jours de l'OTAN destinée à l'industrie, au cours de laquelle 750 experts de l'OTAN, de différents pays, de l'industrie et du milieu universitaire ont examiné de près des occasions d'affaires de l'OTAN et sont entrés en contact avec ces spécialistes de l'approvisionnement. L'événement, qui avait lieu pour la première fois en Amérique du Nord, a atteint un niveau de participation record. Il avait pour but de permettre à l'industrie canadienne de se faire une meilleure idée des occasions d'affaires de l'OTAN.

En décembre 2017, l'Agence d'information et de communication a octroyé à MDA, une filiale de Maxar Technologies établie au Canada, un contrat de 14,9 millions de dollars pour réaliser le projet Triton de l'OTAN, un projet de systèmes d'information de commandement et de contrôle maritimes.

Si j'avais à résumer les priorités du Canada en ce qui concerne son rôle dans l'OTAN dans le domaine de la gestion de l'information et de la technologie de l'information, je dirais que c'est l'échange d'information et l'interopérabilité. La nouvelle politique de défense du Canada présente 111 initiatives, dont un grand nombre propose des mesures positives visant à renforcer les capacités de renseignement de défense au pays et à l'étranger. L'une des initiatives, l'initiative 65, constitue notre engagement envers l'amélioration des capacités cryptographiques, des capacités d'opérations d'information et des cybercapacités. Nous nous concentrerons sur la cybersécurité, la connaissance de la situation dans ce domaine, la détection des cybermenaces et la réaction à celles-ci, ainsi que sur l'amélioration des cyberopérations et des opérations d'information propres au domaine militaire.

Sans plus tarder, je cède la parole au commodore Richard Feltham, qui vous parlera de la cybersécurité et de notre contribution aux efforts de l'OTAN dans ce domaine.

● (0850)

Commodore Richard Feltham (directeur général, Cyberspace, ministère de la Défense nationale): Bonjour. Je vous remercie pour cette occasion de m'adresser au Comité aujourd'hui. Je suis le commodore Richard Feltham, et je suis le directeur général de Cyberespace. À ce titre, je suis chargé du développement des forces en ce qui concerne les cybercapacités militaires permettant de mener des cyberopérations ainsi que le commandement, le contrôle, les communications, l'informatique et le renseignement stratégiques et opérationnels.

Le développement des forces consiste à recenser les changements nécessaires aux capacités existantes et à énoncer les nouveaux besoins en matière de capacité pour les Forces armées canadiennes. Par exemple, nos efforts actuels de développement d'une cyberforce consistent à déterminer les exigences devant être satisfaites pour mener avec succès des cyberopérations, à concevoir les solutions éventuelles pour répondre à ces exigences et à appuyer le développement et la validation de la capacité une fois que la solution a été choisie et mise en oeuvre respectivement.

À ce jour, l'engagement du Canada en matière de cyberdéfense internationale a principalement visé nos partenaires du Groupe des cinq et les activités de cyberdéfense de l'OTAN. Les fondements pour un concept général futur de cyberdéfense pour l'OTAN sont en cours de préparation en ce moment même chez les alliés. En 2016, les alliés, y compris le Canada, ont pris un engagement en faveur de la cyberdéfense afin d'établir comme priorité l'amélioration de leur cyberdéfense nationale. La participation du Canada dans cet engagement reflète notre engagement international, précise les priorités dans le développement d'une cyberdéfense individuelle solide au moyen d'une coopération facilitée dans les domaines de l'éducation, de l'entraînement, des exercices et de l'échange d'information.

D'ailleurs, nous jouons un rôle actif dans de nombreux projets et organes politiques de l'OTAN en matière de cyberespace. Bien que l'architecture complète de la cyberdéfense de l'OTAN ne soit pas encore en place, le Canada s'implique activement dans sa conception pour assurer non seulement son efficacité, mais aussi notre propre capacité à y contribuer et à travailler efficacement au sein de cette nouvelle architecture.

Or, même si l'engagement du Canada est de taille modeste, nous avons choisi des domaines d'activités qui conviennent à nos forces et qui mènent à des avantages mutuels, tant pour l'OTAN que pour nos propres intérêts. Le Canada contribue entre autres à la mise en oeuvre d'une capacité de cyberdéfense multinationale, MNCD2, un projet de défense intelligente de l'OTAN dans lequel les alliés coopèrent pour élaborer, acquérir et maintenir des capacités militaires afin de répondre aux problèmes de sécurité actuels conformément au concept stratégique de l'OTAN.

Le Canada participe à ce projet depuis 2013, au moyen de représentants et d'un soutien financier. En plus de notre apport à l'OTAN, notre participation soutient directement nos propres objectifs, et nous aide à continuer dans la direction et obtenir des résultats que nous cherchons à avoir dans le cadre de l'initiative 65, « Sécurité, Protection, Engagement », que M. Bastien a mentionnée.

Le Système de coordination des incidents et de la cyberinformation et la Plateforme d'échange d'information sur les logiciels malveillants, qui ont tous les deux été élaborés pour la cyberdéfense de l'OTAN, se sont avérés utiles au Canada et sont des exemples de projets offrant des avantages mutuels.

Les autres domaines dans lesquels le Canada contribue à la cyberdéfense de l'OTAN incluent les exercices de cyberguerre de l'OTAN, dans lesquels le Canada a surtout servi d'observateur jusqu'à maintenant. Or, grâce au développement de notre personnel spécialisé en cyberdéfense, nous allons pouvoir envoyer des équipes pour y participer pleinement cette année.

Dans l'exercice Locked Shields, nous avons travaillé avec des équipes de plus de 24 pays pour mettre à l'essai des habiletés à détecter les cyberattaques, à s'en défendre et à mener des enquêtes, tout en exerçant les procédures de prise de décision, de commandement et de contrôle. Dans l'exercice Cyber Coalition, nos équipes devront non seulement affronter des cyberattaques qui seront menées au moyen de logiciels malveillants, mais aussi par des médias sociaux et d'autres moyens hybrides. Ces attaques mettront à l'épreuve nos procédures opérationnelles et juridiques, l'échange d'information et notre travail avec nos partenaires de l'industrie de la défense.

Nous avons combiné l'expérimentation en cyberdéfense et le développement de cibles à l'aide de l'expérience et des installations qui sont offertes par le Centre d'excellence de cyberdéfense coopérative de l'OTAN en Estonie. L'exercice à venir de l'OTAN intitulé Coalition Warrior Interoperability Exercise, soit CWIX, profitera directement à notre capacité de commandement et de contrôle ainsi qu'à notre interopérabilité avec l'OTAN.

Enfin, le Canada participe activement à l'équipe des capacités en matière de cryptographie de l'OTAN et au groupe opérationnel allié sur la cryptographie depuis 2005. Nous avons été en mesure de fournir du leadership et de l'expertise à ces comités, qui nous ont aussi permis d'obtenir de l'information utile pour guider nos propres efforts de développement en matière de cryptographie. Nous avons réussi à élaborer, en respectant des contraintes de temps et d'argent, des systèmes de communication et des réseaux qui répondent à nos besoins et qui sont alignés sur des systèmes de communication sécurisés et fiables de nos alliés de l'OTAN.

Je terminerai en vous disant que la politique de défense du Canada décrit un nouveau cadre pour la manière dont nous allons mettre en oeuvre la vision consistant à « assurer la protection au pays, la sécurité en Amérique du Nord et notre engagement dans le monde ». Nous continuerons d'être un partenaire de confiance pour nos alliés pendant que nous élaborons nos propres cybercapacités pour anticiper, nous adapter et agir.

● (0855)

Le président: Merci, messieurs, pour vos déclarations.

Nous allons maintenant passer à la première série de questions de sept minutes. Ce sera Mark Gerretsen qui commencera.

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

Je vous remercie, messieurs, d'être venus témoigner aujourd'hui.

Ma question s'adresse à celui qui voudra bien y répondre. Vous avez indiqué que le Canada est un acteur important dans les programmes qui alimentent la politique en matière de gestion de l'information et de technologie de l'information et des activités de développement technique à l'OTAN. Pouvez-vous nous en parler davantage de l'importance de la contribution du Canada, en donnant peut-être des exemples concrets de la façon dont les contributions du Canada aident à la réalisation des objectifs de l'OTAN?

M. Len Bastien: Je vous remercie de la question, monsieur le président.

Nous participons activement aux activités de l'OTAN. Permettez-moi de vous expliquer les structures qui encadrent cette participation.

Je vais maintenant définir nos contributions dans le cadre des « structures de l'OTAN », une expression que vous connaissez peut-être. Il y a également des entités qui contribuent aux activités de l'OTAN qui ne font pourtant pas partie de ces structures otaniennes. Par exemple, l'Agence d'information et de communication à laquelle j'ai fait référence se trouve en fait à extérieur des structures de l'OTAN. Elle a été créée en 2012 et on l'a placée sciemment à l'extérieur des structures de l'OTAN afin que l'agence puisse avoir plus de marge de manoeuvre et se comporter davantage comme un fournisseur indépendant. Il y a donc eu des transferts et des échanges dans la façon dont notre contribution est calculée, puisque l'agence se trouve à l'extérieur des structures de l'OTAN pour ce qui est des crédits comme les militaires affectés aux postes et notre capacité d'oeuvrer au sein des structures de l'OTAN.

Permettez-moi de fournir quelques chiffres. À l'intérieur des structures otaniennes, la Défense nationale doit actuellement combler plus de 200 postes, et le taux de dotation est d'environ 96,6 %. Nous sommes très présents et très engagés en ce qui concerne notre devoir de combler des postes au sein des structures de l'OTAN.

À l'extérieur de ces structures, par exemple, nos contributions visent environ 120 à 130 postes qui participent aux activités servant à appuyer directement les opérations ou les services de soutien otaniens.

Sur le plan financier, les contributions sont encore une fois réparties parmi les diverses structures de l'OTAN. Je vais tenter de vous fournir quelques exemples plus détaillés.

Ainsi, en 2016, le Canada a assumé environ 6,6 % des frais totaux de l'OTAN. En ce qui concerne les crédits versés aux projets comme l'agence, le Canada y a consenti environ 20 millions de dollars, et 20 millions de dollars supplémentaires pour le budget militaire. C'étaient deux contributions budgétaires, mais l'une s'est fait à l'intérieur des structures de l'OTAN, alors que l'autre était à l'extérieur.

En ce qui concerne le soutien des systèmes d'information et de communication de l'agence en 2018, le budget prévu était d'environ 48 millions de dollars. Le Canada devra y verser environ 3 millions de dollars en 2018. Le budget de l'agence proviendra des pays partenaires, et la contribution du Canada se chiffrera à 3,1 millions de dollars.

M. Mark Gerretsen: Puisque mon temps est limité, j'aimerais maintenant parler de l'interopérabilité entre les alliés de l'OTAN. Je sais qu'en grande partie, cela dépend du respect et de la mise en oeuvre uniforme des politiques de l'OTAN. Pouvez-vous nous décrire un peu comment les alliés de l'OTAN, dont le Canada notamment, respectent les politiques?

● (0900)

M. Len Bastien: Monsieur le président, je vous remercie encore une fois de la question.

Le respect des politiques de l'OTAN est gouverné par le Bureau de consultation, de commandement et de contrôle NC3, l'un des conseils que j'ai décrits. Je crois que le meilleur exemple de respect serait l'engagement envers la cyberdéfense auquel a fait référence mon collègue. C'est un engagement de la part des pays partenaires selon lequel ils doivent respecter certaines consignes en matière de cybersécurité qui nous permettront d'avoir une interopérabilité dans le climat de confiance nécessaire pour travailler et...

M. Mark Gerretsen: Nous nous sommes engagés. Quel est notre progrès? Réussissons-nous?

M. Len Bastien: Richard, je vous demanderai de répondre à la question.

Cmdre Richard Feltham: Merci, monsieur le président.

Je vais vous fournir un exemple concret de la façon dont le Canada participe aux politiques et aux structures de l'OTAN.

Le réseau de mission fédéré ne se trouve pas forcément à l'intérieur des structures de l'OTAN, mais il bénéficie d'un soutien otanien dans sa structure généralisée. Nous avons déployé un réseau en Lettonie récemment qui est conforme aux normes et aux protocoles. Je crois que le Canada fait figure de proue dans ce domaine en montrant qu'il est en mesure de déployer un réseau conformément aux normes otaniennes. Voilà un bon exemple positif.

M. Mark Gerretsen: C'est ce que je recherchais. Merci.

Et qu'en est-il de nos alliés?

Cmdre Richard Feltham: Je ne peux me prononcer sur le progrès de nos alliés dans ce domaine. Je regrette.

M. Mark Gerretsen: Combien de temps me reste-t-il?

Le président: Environ une minute.

M. Mark Gerretsen: Toujours sur le même thème, pouvez-vous nous parler des avantages du maintien de l'interopérabilité? Dans quelle mesure est-ce important?

Cmdre Richard Feltham: Peu importe les opérations, qu'elles soient de nature militaire ou non, la clé de la réussite, c'est la communication. De plus en plus, la communication se fait au moyen de réseaux et de données. Si nous n'arrivons pas à assurer une interopérabilité avec nos alliés, il devient de plus en plus difficile de communiquer avec nos forces militaires et de les contrôler. Notre capacité d'opérer avec nos alliés, à la fois au sein du Groupe des cinq et de la communauté otanienne, est ce qu'il y a de plus important pour nous. Nous avons consacré énormément d'effort et de temps afin de réussir. C'est l'un des grands objectifs dans tous les groupes de travail auxquels M. Bastien a fait référence: assurer l'interopérabilité. C'est primordial.

M. Mark Gerretsen: C'est donc d'une importance critique.

Cmdre Richard Feltham: Tout à fait. Critique.

Le président: Monsieur Paul-Hus, soyez le bienvenu. À vous la parole.

[*Français*]

M. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, PCC): Bonjour, messieurs.

Ma question concerne non seulement le Canada, mais l'OTAN et tous ses pays membres. Quels types d'attaques cybernétiques sont faites présentement? Est-ce que des pays font des attaques? Quels moyens de cyberdéfense devons-nous utiliser?

M. Len Bastien: Merci de votre question.

[*Traduction*]

Si j'ai bien compris, vous voulez en savoir davantage sur les types d'attaques ou de cybermenaces que nous gérons, à la fois ici au pays et dans le cadre de notre alliance avec l'OTAN.

[*Français*]

M. Pierre Paul-Hus: Dans le cadre global de l'OTAN, j'aimerais savoir d'où proviennent les grandes menaces.

L'OTAN compte actuellement 29 pays membres, mais ils n'ont pas tous les mêmes capacités. Certains pays membres sont probablement plus régulièrement victimes de cyberattaques.

Avez-vous des informations générales à ce sujet?

M. Len Bastien: Je comprends votre question.

[*Traduction*]

Permettez-moi de commencer en expliquant certaines conditions précisées dans l'engagement. L'une des conditions, c'est que les pays sont responsables de leur propre cyberdéfense. Lorsqu'une coalition est constituée en vertu de l'autorité de l'OTAN, les capacités de cyberdéfense sont gérées par l'agence. C'est la raison pour laquelle je ne peux me prononcer sur l'intégrité ou les vulnérabilités qui pourraient exister au sein de ce cyberenvironnement.

Je peux, par contre, vous parler de notre cyberenvironnement à la Défense nationale. Je peux vous assurer que nous prenons les choses au sérieux et que nous surveillons et gérons nos réseaux avec un maximum d'intégrité lorsqu'il s'agit de cybermenaces.

[*Français*]

M. Pierre Paul-Hus: Il n'y a pas de frontières dans le cyberespace. Internet, c'est planétaire. Si on fonctionne en vase clos, il n'y a pas de cohésion.

L'étude sur l'OTAN que nous effectuons cherche à savoir s'il y a une cohésion au sein de l'OTAN et si les efforts sont regroupés. Si le Canada fait des investissements en cyberdéfense ou établit des plans en matière de cyberattaques, mais que les autres pays ne s'alignent pas sur ceux-ci, nous avons un problème. Nous voulons savoir si nous jouons seuls dans l'équipe ou non.

● (0905)

M. Len Bastien: Merci de la question.

[*Traduction*]

C'est vrai que le cyberespace n'a pas de frontière. Les plus grandes menaces que nous surveillons et suivons viennent d'Internet, un réseau dans lequel nous opérons tous, parce que nous y sommes bien obligés.

Lorsque nous créons des milieux d'interopérabilité avec nos alliés, nous préconisons la même approche prudente, en nous dotant de pare-feux et de portes qui nous permettent de réguler le trafic de façon à assurer une surveillance et une gestion. Ce n'est pas un réseau libre sans contrainte. Il serait faux de vous donner l'impression que nous sommes tous interconnectés d'une façon quelconque avec nos alliés sans nous doter de protections. Nous mettons en oeuvre énormément de mesures de sécurité au sein du ministère de la Défense nationale.

[*Français*]

M. Pierre Paul-Hus: Des troupes canadiennes ont été déployées en Lettonie. Le but de ce déploiement est d'avoir une présence physique sur le terrain eu égard à la Russie. En même temps, on sait qu'il y a des opérations de cyberattaques et de cyberdéfense.

Y a-t-il beaucoup de ressources canadiennes engagées dans la défense en Lettonie?

[*Traduction*]

M. Len Bastien: Je souscris à cette affirmation, monsieur le président. Nous avons beaucoup investi dans cette partie du monde avec nos alliés.

Je crois que votre question portait sur les risques ou les menaces qui nous préoccupent. Permettez-moi de vous expliquer comment nous fonctionnons au ministère de la Défense nationale.

Même s'il est relativement nouveau, le cyberespace est une composante établie des opérations militaires, comme les composantes terrestre, aérienne et maritime, et, comme il le fait pour ces trois aspects, le ministère de la Défense nationale développe ses capacités à cet égard. Mon mandat consiste à aider à la préparation des cybercapacités en vue de leur utilisation dans le cadre d'opérations de déploiement.

Cela dit, concrètement, c'est le commandant du Commandement des opérations interarmées qui utilise ces capacités pour le déploiement et le contrôle de sa mission. Je ne peux faire de commentaires sur la façon dont il utilise ces capacités. Je peux toutefois vous dire que mon mandat, ma responsabilité, est de les préparer, de les créer et de veiller à leur employabilité. Nous travaillons avec acharnement pour offrir aux femmes et aux hommes des Forces armées canadiennes les meilleures chances de succès lors de leur déploiement. Nous déployons les meilleures cybercapacités que nous puissions produire pour eux.

[*Français*]

M. Pierre Paul-Hus: Je ne sais pas si vous pouvez répondre à cette question, mais j'aimerais savoir si le Canada mène actuellement des opérations offensives.

[*Traduction*]

M. Len Bastien: Je vous remercie de la question, monsieur le président.

Je peux vous dire que les opérations de cyberdéfense font partie de notre réalité depuis de nombreuses années; nous le faisons depuis longtemps, sans réel problème. Il s'agit d'un domaine d'expertise que nous avons développé et amélioré au fil du temps. Récemment, lors de l'annonce de notre politique « Protection, Sécurité, Engagement », le gouvernement nous a explicitement donné la directive d'accroître nos investissements liés au cyberespace, dans les cyberopérations actives. Cela nous permettra d'avoir recours à des cybercapacités offensives pour accroître le succès de nos missions.

Je vais céder la parole au commodore Feltham, car il pourra vous fournir des renseignements plus concrets sur la nature de ces activités.

Cmdre Richard Feltham: Merci, monsieur le président.

Je ne peux me prononcer sur les activités à cet égard dans l'ensemble du Canada, mais du point de vue du MDN, comme M. Bastien l'a mentionné, la politique récemment annoncée nous autorise à mener des cyberopérations actives. C'est donc tout nouveau. Nous apprenons à mener de telles activités. Nous travaillons avec nos partenaires du gouvernement et avec nos alliés de partout dans le monde pour acquérir des connaissances sur la façon dont cela fonctionne. Je n'ai pas encore eu l'occasion de participer à des cyberopérations offensives.

[*Français*]

M. Pierre Paul-Hus: D'accord, merci.

[*Traduction*]

Le président: Monsieur Garrison.

M. Randall Garrison (Esquimalt—Saanich—Sooke, NPD): Merci beaucoup, monsieur le président. Je remercie les témoins d'être venus aujourd'hui.

J'aimerais commencer par poser des questions sur l'approvisionnement. Le Comité a discuté de nombreux aspects de l'approvisionnement, mais j'aimerais m'attarder sur deux préoccupations.

Étant donné nos préoccupations en matière de cybersécurité, a-t-on mis en place des restrictions sur les entreprises autorisées à participer à des appels d'offres pour l'obtention de contrats dans le domaine de la gestion de l'information? Je sais que diverses préoccupations ont été soulevées. Il s'agit notamment de la possibilité que des sociétés d'État d'autres pays puissent présenter des soumissions, des dangers que cela représente et de la capacité de certains d'implanter des chevaux de Troie, disons, entre autres choses, dans les systèmes informatiques. Y a-t-il des restrictions actuellement? Comptez-vous mettre en place des restrictions applicables aux participants des appels d'offres liés aux systèmes de gestion de l'information, étant donné les enjeux de cybersécurité?

● (0910)

M. Len Bastien: Merci de la question, monsieur le président.

Au gouvernement, la fonction d'approvisionnement est centralisée et relève d'un autre ministère, Services publics et Approvisionnement Canada. Dans notre ministère, cela relève du sous-ministre adjoint (Matériels). Je peux vous dire, d'après mon expérience, que nous avons invoqué l'exemption au titre de la sécurité nationale dans les cas où nous avions affaire à des questions de nature délicate en matière de sécurité nationale ou encore des préoccupations liées à l'approvisionnement de capacités en matière de GI/TI. En ce qui concerne l'intégrité de notre processus ou de notre chaîne d'approvisionnement, je vous invite à poser la question à mes collègues, qui sont les spécialistes et la véritable autorité en la matière.

M. Randall Garrison: Les responsables de l'approvisionnement vous consultent sans doute quant aux critères pour l'attribution des contrats. Donc, je vous demande encore une fois si vous incluez ces préoccupations dans les critères des contrats, car je pense qu'elles seront de plus en plus présentes à l'avenir.

M. Len Bastien: Je peux vous assurer, en ce qui concerne la portée des contrats, que nous établissons des exigences de haut niveau quant aux capacités que nous recherchons. Je peux vous dire que le gouvernement en général consacre d'importants efforts à la consolidation de l'intégrité des chaînes d'approvisionnement. Je suis conscient de cet aspect, mais cela ne relève pas de moi. Il va sans dire que lorsque j'établis ces exigences de haut niveau, cela se fait manifestement dans l'optique d'obtenir les capacités les plus efficaces et les plus sécuritaires pour obtenir les résultats souhaités.

M. Randall Garrison: Je suppose, dans ce cas, que ma question est d'ordre plus général. Lorsque vous parlez de « haut niveau », cela donne l'impression qu'il s'agit de circonstances exceptionnelles. Ma question porte sur des circonstances plus habituelles où le processus d'approvisionnement peut donner accès à nos informations.

M. Len Bastien: Je peux comprendre pourquoi les termes employés peuvent vous avoir donné cette impression. Je peux vous assurer que même si j'ai parlé d'exigences de haut niveau, on ne tient pas pour acquis que...

Nous en sommes extrêmement conscients et nous nous assurons activement que les capacités que nous acquérons sont conformes. Divers contrôles sont en place, non seulement pendant le processus d'approvisionnement, mais aussi aux étapes de la conception et la mise en œuvre, pour veiller à l'intégrité de la capacité dont nous faisons l'acquisition afin qu'elle ne représente pas un risque ou une menace sur le plan de la défense nationale.

M. Randall Garrison: Merci beaucoup.

Je tiens à poser une deuxième question sur l'approvisionnement; elle est liée à un enjeu quelque peu étrange survenu dans ma circonscription. J'ai rencontré un électeur, un propriétaire d'une petite entreprise qui éprouve des difficultés par rapport au droit de la propriété intellectuelle et à la capacité des entreprises de conserver la propriété et le contrôle des technologies de l'information, dans ce cas précis.

Je me demande si ce problème se pose dans le cas de nos activités dans le domaine de la cybersécurité. Certaines grandes entreprises tentent de conserver le contrôle et la propriété, ce qui restreint l'utilisation des technologies après leur acquisition.

M. Len Bastien: Je suis au fait de la situation que vous décrivez. En tant qu'autorité, j'ai reçu des demandes en ce sens et j'ai participé à la décision d'autoriser la diffusion de la propriété intellectuelle pour son utilisation par l'industrie et lors de soumissions subséquentes. Le contrat remporté par MDA avec l'OTAN est un exemple. L'entreprise, avec laquelle nous avions travaillé dans le passé, a demandé l'autorisation d'utiliser la propriété intellectuelle qui avait été créée dans sa soumission avec l'OTAN, ce qui lui a permis d'obtenir le contrat.

Je peux vous dire que j'ai constaté les résultats positifs associés à cette situation. Je vous invite à consulter mon collègue, le sous-ministre adjoint (Matériels) du ministère de la Défense nationale, pour toute autre question liée à l'approvisionnement et à la propriété intellectuelle, car il s'agit de son domaine de compétence.

M. Randall Garrison: Je vous remercie d'avoir donné un exemple positif. Nous avons vu, dans d'autres secteurs de la défense, des tentatives d'interdire l'utilisation de certaines technologies. L'exemple le plus connu est celui des technologies de missiles mettant en cause la Grande-Bretagne et la France. Le gouvernement français a tenté d'invoquer ses lois nationales pour interdire l'utilisation de la propriété intellectuelle, comme la Grande-Bretagne l'avait fait.

De telles situations se sont-elles produites jusqu'à maintenant?

M. Len Bastien: La meilleure réponse que je puisse donner, monsieur le président, c'est qu'il n'y a pas eu de cas de ce genre dans mon domaine, à ma connaissance.

● (0915)

M. Randall Garrison: Au début, vous avez parlé de la collaboration avec l'OTAN et le Groupe des cinq, mais tout au long de la discussion, vous avez traité des protocoles avec l'OTAN.

Avons-nous des protocoles semblables avec nos partenaires, le Groupe des cinq, comme on les appelle?

M. Len Bastien: La discussion à laquelle nous avons été invités à participer aujourd'hui était axée sur l'OTAN. Cependant, dans nos exposés, nous avons élargi la discussion sur l'importance de nos partenaires, dont il est explicitement question dans notre nouvelle politique de défense. Nous considérons que le NORAD, nos relations bilatérales avec les États-Unis, le Groupe des cinq et l'OTAN sont tous des partenariats et des alliances extrêmement précieux.

Nous avons fait d'importants investissements dans le Groupe des cinq. Nous jouons un rôle actif au sein de divers organes directeurs, y compris des forums sur le renseignement et la défense, auxquels je participe personnellement. Nous accordons une grande importance à ces relations. Nos rencontres avec nos collègues des autres pays nous sont avantageuses, et nous y contribuons de manière significative. Cela ne nous donne pas seulement l'occasion d'établir l'interopérabilité par défaut, comme pour tous nos principes directeurs, mais aussi de tirer parti des investissements de chacun dans certains domaines, y compris les cyberopérations.

Il s'agit d'une tribune qui nous est extrêmement avantageuse. Je peux vous assurer que nous participons à divers échelons, tant sur les plans militaires que civil, pour veiller au maintien de saines relations.

Le président: Merci.

Monsieur Darren Fisher.

M. Darren Fisher (Dartmouth—Cole Harbour, Lib.): Merci beaucoup, monsieur le président.

Messieurs, merci beaucoup d'être ici aujourd'hui. Vous nous avez fourni énormément de détails dans vos exposés. Je vous remercie également de nous en avoir fourni le texte au préalable.

Nous savons que les Canadiens ne sont pas à l'abri d'atteintes à la protection des données. Nous venons d'apprendre que Bell a été piraté. Quelle mesure l'OTAN prend-elle pour veiller à ce que ses infrastructures soient protégées contre les atteintes à la sécurité des données?

Je pars du principe que le cyberespace évolue probablement au quotidien. Je cherche également à savoir si nous avons la souplesse nécessaire. L'OTAN a-t-elle la capacité de s'adapter et de réagir rapidement aux cybermenaces?

M. Len Bastien: Monsieur le président, permettez-moi de répéter que selon la politique établie parmi les pays membres de l'OTAN, chaque pays est responsable des enjeux de cybersécurité qui le touche; c'est donc à nous qu'il revient d'intervenir.

Je ne suis pas en mesure de répondre à votre question sur la santé cybernétique ou l'état de préparation de l'OTAN, simplement parce que l'OTAN est responsable de ses propres activités de cybersécurité. Certes, nous faisons partie du conseil de supervision de l'organisation — le conseil d'administration, essentiellement — qui veille à ce que l'OTAN ait les ressources et les politiques nécessaires pour assurer sa réussite. Toutefois, sur le plan opérationnel, l'OTAN rend des comptes au Conseil de l'Atlantique Nord. Donc, ces questions ne concernent que l'OTAN, et nous ne pouvons nous prononcer sur les menaces et les risques de l'OTAN en matière de cybersécurité.

Je pourrais demander à Rich de vous faire part des connaissances que nous avons sur les mécanismes d'intervention mis en place par l'organisation en cas d'incident, mais je ne suis pas en mesure de me prononcer sur la santé cybernétique de l'OTAN, à ce moment-ci.

Cmdre Richard Feltham: Monsieur le président, je vous remercie encore une fois de la question.

J'aimerais répéter deux ou trois points soulevés précédemment par M. Bastien: la responsabilité des activités de cyberdéfense est clairement énoncée dans l'engagement pris à l'égard de l'OTAN, soit que chaque pays a la responsabilité de ses propres mécanismes.

En ce qui concerne le fonctionnement d'une coalition, j'ai décrit plus tôt le réseau de mission fédéré, les réseaux que nous avons déployés qui sont conformes à des protocoles acceptés par tous. J'aimerais toutefois faire un commentaire sur un point lié à la collaboration et au progrès visant l'amélioration des cybercapacités de chacun des pays membres de l'OTAN. Dans mon exposé, j'ai donné l'exemple d'un projet de défense intelligente. Cela signifie simplement que nous échangeons des données dans le cadre de la mise en oeuvre d'une capacité de cyberdéfense multinationale...

M. Darren Fisher: Le MN CD2.

Cmdre Richard Feltham: C'est un exemple positif qui démontre comment nous parvenons à travailler ensemble pour veiller à la prise en compte des intérêts cybernétiques de chaque pays. Cela dit, encore une fois, c'est la responsabilité de chacun.

Permettez-moi d'ajouter un exemple positif. Dans un cas précis, les résultats du projet de défense intelligente, du groupe de cyberdéfense multinationale, ont pu être appliqués au pays et utilisés dans nos propres réseaux. C'est donnant-donnant. Essentiellement, monsieur, nous partageons des ressources et échangeons des idées afin que tous s'améliorent.

M. Darren Fisher: Très bien.

J'essaie de comprendre comment tout cela fonctionne; je sais que le NCSM *St John's* a quitté Halifax il y a deux ou trois semaines pour participer à l'opération Reassurance. Supposons que nos troupes font l'objet d'une cyberattaque. Comment réagirions-nous? Que faisons-nous pour nous préparer à ce type de menaces?

M. Len Bastien: Merci de la question, monsieur le président. Je vais commencer, puis j'inviterai mon collègue à présenter ses observations sur la forme que cela pourrait prendre, étant donné son expérience dans la Marine.

Comme je l'ai indiqué plus tôt, nous préparerons les cybercapacités qui seront déployées avec notre marine, notre armée et notre force aérienne. C'est notre mandat. Notre rôle est de veiller à ce qu'ils aient les meilleures chances possibles de réussite en acquérant les meilleures technologies, selon nos moyens, et en leur fournissant. Toutefois, lors d'un déploiement, lorsque les forces quittent les côtes du Canada, elles relèvent du contrôle opérationnel du Commandement des opérations interarmées.

Rich pourrait vous expliquer comment cela fonctionne lorsqu'on est à bord d'un navire, vous décrire les mesures de protection de la force qui pourraient être mises en place, et peut-être faire des commentaires sur l'état de préparation cybernétique lors d'un déploiement.

● (0920)

Cmdre Richard Feltham: Merci, monsieur le président.

Permettez-moi, pour être un peu plus précis, de revenir légèrement en arrière. Lorsque nous déployons nos troupes lors de missions opérationnelles, les menaces font l'objet d'une analyse exhaustive. Il en a toujours été ainsi, et les menaces émergentes des 20 dernières années, ce sont les cybermenaces.

Lorsque le chef d'état-major de la Défense déploie des militaires en mission, le Commandement des opérations interarmées a notamment pour mandat de veiller à l'état de préparation des troupes à l'égard des menaces auxquelles elles pourraient être confrontées, notamment les cybermenaces. Il s'agit donc d'un processus d'information, entre autres choses, qui est fondé sur l'analyse des menaces.

Quant à la question générale d'un navire en déploiement, cela nous ramène au point soulevé précédemment par M. Bastien: à l'instar de nombreuses autres unités, les navires communiquent nécessairement par l'intermédiaire de réseaux. Nous devons donc mettre en place des protocoles et des réseaux sécurisés pour assurer la communication entre les divers navires qui participent à une opération.

Votre question appelle donc une réponse à deux volets: sur le plan de la sécurité du personnel, nous préparons nos troupes au déploiement en fonction de l'analyse des menaces, tandis que sur le plan de la capacité, les réseaux sont des réseaux sécurisés qui permettent la communication des navires et l'échange de renseignements entre les unités d'un groupe donné.

M. Darren Fisher: Me reste-t-il du temps, monsieur le président?

Le président: Oui, environ 40 secondes.

M. Darren Fisher: Bien.

Vous avez parlé de la capacité multinationale de cyberdéfense, ou MN CD2. Sans vouloir vous prêter des propos que vous n'avez pas tenus, je pense que vous avez dit, lorsque vous avez mentionné notre contribution importante, que celle-ci n'était pas très grande. Je crois que ce sont vos mots.

J'aimerais donc savoir comment notre apport est jugé dans le contexte de l'OTAN. Investissons-nous suffisamment? Avons-nous assez de capacité? À votre avis, devrions-nous en faire encore plus dans le domaine dont nous parlons aujourd'hui?

Cmdre Richard Feltham: Je ne peux vous parler que de ce que nous faisons. Du point de vue de la politique, le Canada a un agent de cybernétique à temps plein au quartier général de l'OTAN qui contribue à orienter les politiques de l'Organisation. C'est ce que nous faisons. Comme M. Bastien l'a dit tout à l'heure, nous participons à des projets de défense intelligente au sein de groupes à gouvernance multiple. Je dirais que notre contribution n'est pas modeste; je me suis peut-être mal exprimé tout à l'heure. J'aimerais clarifier brièvement ma pensée. Si nous prenons l'exemple de la structure de la MN CD2, nous avons versé plus de 900 000 euros à cet effort de défense commun depuis 2013 environ. Je ne dirais pas que c'est peu. Il s'agit d'une contribution substantielle, sur le plan non seulement de l'argent, mais aussi des ressources intellectuelles. En effet, nous envoyons des experts compétents dans un domaine du Canada pour qu'ils participent à une tribune multinationale et aident tous les intervenants à trouver une meilleure solution dans l'intérêt de tous. Je me suis peut-être mal exprimé en laissant entendre que notre contribution était modeste.

J'aimerais revenir sur un autre point, si j'ai le temps. L'une des contraintes de tout domaine d'opération cybernétique est les ressources humaines, qu'il s'agisse du gouvernement, de l'industrie ou de quoi que ce soit d'autre. Nous sommes à la recherche de personnes qualifiées qui sont prêtes à venir travailler pour nous. Lorsque nous affectons des membres de l'effectif, nous le faisons très judicieusement, et une personne à la fois; nous choisissons les endroits où nous aurons le maximum d'effet, dans l'intérêt du plus grand bien commun.

Le président: Nous allons maintenant passer aux interventions de cinq minutes.

Monsieur Spengemann, la parole est à vous.

M. Sven Spengemann (Mississauga—Lakeshore, Lib.): Merci beaucoup.

Messieurs, je vous remercie tous les deux d'être avec nous. Je vous remercie de votre service et de votre expertise.

En m'appuyant sur la question que mon collègue, M. Fisher, vient de poser, j'aimerais vous donner un exemple. La situation est trop intéressante pour l'ignorer, et je voudrais savoir ce que vous en pensez.

Nathan Russer est un étudiant de niveau collégial de 20 ans qui s'intéresse à la sécurité internationale et au Moyen-Orient. Il s'est rendu sur la carte mondiale des utilisateurs de Strava pour voir ce qui se passe en Syrie. Il y a trouvé une foule de données détaillées sur les militaires américains en service et sur leurs activités récréatives et sportives, qui étaient à la portée de n'importe qui.

Dans l'optique de la protection de la force, quelle est l'ampleur du travail à réaliser au sein des Forces canadiennes et chez nos alliés, y compris l'OTAN? Il faut vraiment s'assurer de concilier harmonieusement nos activités civiles et notre vie militaire, en ce qui a trait à la connectivité et à la possibilité qu'une personne souhaitant nous nuire puisse trouver très facilement ce genre de données.

M. Len Bastien: C'est un exemple fascinant dont nous avons tous entendu parler récemment, et auquel les Américains sont en train de réagir.

J'aimerais revenir sur notre position actuelle en matière de sécurité et de défense au sein de notre institution. Nous avons une politique claire et explicite qui vise tout appareil électronique ou numérique dans certaines régions où nous sommes en activité. Par exemple, il y a des salles et des étages de nos édifices où aucun dispositif numérique n'est permis, y compris les appareils de localisation à des fins sportives dont vous avez parlé. Nous fournissons des boîtes scellées pour les conserver, et les appareils peuvent être récupérés après l'activité. Nous nous assurons que ces politiques sont respectées tous les jours. Notre seuil de tolérance est limité quand vient le temps de prendre quelque risque que ce soit à cet égard.

Je ne peux vraiment pas parler au nom d'autres nations ou de l'OTAN sur leur respect de politiques semblables, mais je peux vous assurer que nous prenons la question très au sérieux au sein de la Défense nationale et de nos établissements. Je dirais que le commandant du Commandement des opérations interarmées vous donnerait la même réponse à propos des déploiements.

● (0925)

M. Sven Spengemann: C'est utile. Merci beaucoup.

Ma deuxième question porte sur la main-d'oeuvre civile et militaire qui est nécessaire ou qui le sera pour accomplir le travail relatif à la cybersécurité et à la cyberguerre. Quelle est la situation actuelle des Forces canadiennes? Arrivent-elles à embaucher au moyen de contrats externes ou à miser sur leurs compétences pour faire ce travail? Comment les tâches sont-elles réparties? Quelle part du travail est réalisée à l'interne et à l'externe?

Voilà qui soulève la question des contrats et des exemptions relatives à la sécurité qui doivent être obtenues. Dans l'intérêt du Comité et de la population canadienne, pourriez-vous nous brosser un tableau du statu quo et des besoins attendus pour la prochaine décennie?

M. Len Bastien: Nous traversons une période très exaltante. Nous prenons très au sérieux l'annonce de notre politique et l'instruction précise d'investir dans les opérations cybernétiques. Il suffit d'analyser le paysage actuel pour constater que nous ne sommes pas les seuls à investir dans la cybersécurité. À vrai dire, tout le gouvernement fédéral, de même que l'industrie — et l'ensemble du milieu — cherchent à investir, à recruter et à conserver les spécialistes dans le domaine. Les Forces canadiennes ont reçu l'ordre de mettre sur pied une cyberforce. Je vais demander au commodore Feltham d'expliquer à quoi cette force ressemblera, où nous en sommes aujourd'hui, exactement, et ce que nous avons réalisé en quelques mois seulement, depuis l'annonce de la politique.

Nous faisons preuve d'une grande originalité dans nos stratégies de ressources humaines en ce qui a trait au recrutement et au maintien en poste des spécialistes de la cybersécurité. Nous voulons nous associer aux universités et collaborer avec l'industrie. Nous sommes prêts à mettre en commun l'information avec nos alliés de l'OTAN et du Groupe des cinq, afin de trouver des solutions au défi qui nous frappe puisque nous ciblons tous le même objectif, à savoir acquérir une capacité suffisante pour évoluer en toute sécurité dans le cyberespace.

Pour ce faire, je pense qu'il est très important de savoir ce que font les Forces canadiennes, puisque notre mandat explicite de défendre la Défense nationale, en particulier sur le plan cybernétique, relèvera de ce régime. Je vais demander à Richard d'expliquer ce volet.

Cmdre Richard Feltham: J'aimerais revenir au point précédent de M. Bastien, à propos de la voie à suivre pour la main-d'oeuvre en cybersécurité, du point de vue des Forces armées canadiennes. La politique disait très clairement que nous devons créer un métier de cyberopérateur. Comme M. Bastien l'a mentionné lui aussi, c'est très emballant. La position a été créée cet été, et nous avons nos tout premiers militaires qui occupent cette fonction. Les efforts subséquents viseront à intégrer ce métier à la Force de réserve. Un métier a aussi été créé dans la Réserve pour veiller à attirer le plus de talents possible dans ce domaine. Le dossier progresse.

Le prochain défi sera toujours de savoir où trouver les gens et comment les garder en poste. Comment pouvons-nous les attirer, les recruter et les garder dans ce domaine? C'est un défi constant auquel nous consacrons beaucoup d'énergie. En toute franchise, nous utilisons des niveaux de réflexion différents de nos méthodes habituelles de recrutement au sein des Forces armées canadiennes, car il s'agit vraiment d'un groupe spécialisé auquel nous accordons une attention particulière.

Je reviendrai à votre question précise. Comme le bassin de main-d'oeuvre qualifiée est petit, lorsque des employés contractuels travaillent pour nous, ils font l'objet d'une enquête de sécurité et obtiennent une cote de sécurité du niveau approprié pour effectuer le travail dont nous avons besoin. Cela ne me préoccupe pas du point de vue de la sécurité. J'ai besoin d'une main-d'oeuvre qualifiée et désireuse de travailler dans ce domaine. Les employés contractuels sont une source, tout comme les réservistes et les membres de la Force régulière. Je travaille sur le contexte général avec les universités et l'industrie.

Le président: Votre temps est écoulé.

Le prochain intervenant est M. Yurdiga.

M. David Yurdiga (Fort McMurray—Cold Lake, PCC): Merci, monsieur le président.

J'aimerais remercier les témoins d'être avec nous ce matin.

Monsieur Bastien, ma première question s'adresse à vous. Je crois savoir que vous avez beaucoup d'expérience en matière de technologies de l'information et de cybersécurité. Quels seront les avantages de la décentralisation du programme en matière de gestion de l'information et de la technologie de l'information au sein de la Défense nationale? La décentralisation protège-t-elle davantage notre système contre les cyberattaques?

M. Len Bastien: Il est vrai que la gestion de l'information et de la technologie de l'information au sein de la Défense nationale est réalisée par des fournisseurs de services de gouvernance fédérée. Permettez-moi de vous expliquer ce que cela signifie essentiellement.

À titre de dirigeant principal de l'information, je détiens l'autorité fonctionnelle de toute gestion de l'information et de la technologie de l'information au sein du ministère. Je n'ai pas nécessairement à en être propriétaire pour contrôler ce volet avec autorité. L'Armée, la Marine, l'Aviation et le chef du personnel militaire fournissent des services de TI dans les escadres, les bases et les garnisons d'un bout à l'autre du pays. Ils le font toutefois suivant une politique que mon groupe contrôle péremptoirement.

Même si la propriété n'est pas centralisée, les opérations le sont pour ainsi dire. La gouvernance est centralisée, et la prestation est régionale. Nous faisons beaucoup de gouvernance centralisée pour nous assurer que nos investissements sont prudents et utiles aux Canadiens.

Le concept de cybersécurité reflète une réalité avec laquelle nous devons tous travailler en collaboration. Le chef d'état-major de la Défense a ordonné à mes intervenants, partenaires et fournisseurs de services de l'ensemble du ministère de se ranger derrière le commodore Feltham et son équipe pour veiller à ce que les services cybernétiques aient l'assurance dont ils ont besoin pour s'occuper de la Défense. En réalité, nos opérations de défense sont déjà très bonnes. Pour le moment, rien ne m'incite à centraliser les effectifs ou à prendre en charge toutes les activités de gestion de l'information et de la technologie de l'information au sein du ministère. À vrai dire, nous trouvons qu'une bonne gouvernance et un contrôle autoritaire donnent les résultats dont nous avons besoin.

● (0930)

M. David Yurdiga: Bien des gens se préoccupent de la cyberintégration et de l'échange d'information avec nos alliés. Ils ne croient pas que cet échange est néfaste, mais plutôt qu'il existe un risque que la sécurité d'un allié soit compromise. Quels protocoles sont en place pour nous assurer de pouvoir réagir très vite si un de nos alliés est ciblé?

M. Len Bastien: Permettez-moi d'expliquer notre environnement technique dans des termes un peu plus simples que le jargon d'ingénierie que mon équipe essaie de me faire utiliser.

Essentiellement, comme le commodore Feltham l'a dit, nous voulons communiquer avec nos alliés. C'est un volet essentiel du travail au sein d'une coalition. Que nous communiquions à un niveau très secret, secret ou protégé B, nos réseaux sont configurés de façon à pouvoir interopérer. Cependant, comme je l'ai dit plus tôt, les barrières et les pare-feux sont laissés en place afin de segmenter, en cas d'incident, les différents alliés de ces réseaux. Même si nous n'avons eu aucun incident majeur comme celui que vous décrivez, notre capacité à protéger nos avoirs à l'échelle nationale est toujours intégrée dans la conception et l'ingénierie de ces réseaux.

Nous rencontrons souvent nos alliés, le Groupe des cinq ou l'OTAN pour discuter de l'interopérabilité, de l'ingénierie et de la conception dans cette optique.

M. David Yurdiga: Je vous remercie de votre réponse.

Comme vous le savez, nous parlons d'information, d'échange et de tout le reste, mais nous devons aussi examiner les problèmes d'infrastructure. Si l'un des systèmes est piraté, qu'il s'agisse d'un service public, d'un pipeline ou de quoi que ce soit d'autre, cela pourrait entraîner une situation malheureuse et même causer la mort. Privilégions-nous une vision holistique visant à protéger toutes les infrastructures, qu'elles soient privées ou publiques? En outre, y a-t-il des échanges constants entre les infrastructures publiques et privées?

M. Len Bastien: Encore une fois, je vous remercie de la question, monsieur le président.

Comme on l'a déjà mentionné, il n'y a pas de frontières dans le cyberenvironnement. Il n'est pas aussi facile de déterminer où se trouvent les limites. Je dirais que ce que vous avez décrit constitue une préoccupation du gouvernement. Le ministère de la Défense nationale fait partie de la « cyberéquipe Canada », si l'on veut, et il n'est qu'un seul membre. La démarche de l'équipe Canada en matière de cybersécurité est menée par Sécurité publique. Bien que nous collaborions avec ce ministère, en comité, à l'élaboration d'une meilleure politique sur la cybersécurité pour le gouvernement et les Canadiens, le ministère responsable serait mieux en mesure de répondre à vos questions concernant les pratiques exemplaires en cybersécurité du Canada.

Je peux vous dire que le travail sur l'élaboration d'une politique en matière de cybersécurité est en cours. Puisque nous faisons partie du comité qui essaie de faire avancer les choses à cet égard, je suis au courant dans une certaine mesure. Toutefois, je n'ai pas de rôle clé quant aux objectifs et aux résultats de cette politique.

● (0935)

Le président: Votre temps est écoulé.

Allez-y, madame Alleslev.

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

Rich, je suis heureuse de vous revoir après 36 ans, bien entendu.

J'aimerais continuer dans la même veine, car je crois qu'à une certaine époque, le rôle d'une force militaire consistait surtout à préserver la souveraineté du pays en le protégeant contre des invasions à des frontières bien définies. Maintenant, compte tenu de la nature changeante de la guerre, nul doute qu'il y a des zones grises. La cyberguerre coûte presque moins cher et est presque plus rapide et elle est très efficace.

De plus, les réseaux militaires ne sont pas les cibles de ces attaques, car les gens du domaine militaire font du très bon travail. Par conséquent, il ne s'agit certainement pas de discuter ici aujourd'hui de la mesure dans laquelle l'OTAN gère bien ses infrastructures ou de la mesure dans laquelle le Canada gère bien ses propres infrastructures de commandement et contrôle, car nous le faisons depuis de nombreuses années et nous nous débrouillons particulièrement bien.

Je crois que nous sommes vulnérables sur le plan du vol de renseignements essentiels — comme ceux du Conseil national de recherches du Canada, qui a été victime de piratage — et des données financières, comme à Equifax, une entreprise américaine. Il s'agit de notre iCloud, de Our Cloud, de Google Docs, où toutes les informations que nous avons en tant que nation ne sont pas canadiennes. Prenez notre infrastructure de courriel, par exemple: notre capacité d'avoir des communications souveraines avec notre population passe par d'autres pays que le Canada, en fait.

Je comprends que l'OTAN considère que cette capacité nationale relève du pays; toutefois, je dirais que nos vulnérabilités, au pays, chez nous, portent atteinte non seulement à notre souveraineté et à notre sécurité, mais également à celles de nos alliés. Comment communiquons-nous pour ce qui est de notre sécurité et de nos infrastructures nationales en ce qui concerne les forces de l'alliance? Toute alliance n'est pas plus forte que le plus faible de ses maillons, et en ce moment, je dirais que nos infrastructures civiles concernant la guerre de l'information sont bien plus faibles que nos infrastructures militaires et peuvent ainsi avoir des répercussions sur l'alliance.

Pourriez-vous nous dire comment nous évaluons cela et ce que nous faisons pour corriger cette faiblesse, non seulement pour notre pays, mais pour l'alliance?

M. Len Bastien: Il faut que je parle de plusieurs aspects de ce que vous avez dit simplement pour, je l'espère, fournir quelques éclaircissements et mettre les choses en contexte concernant le concept dont je demanderai à Rich de parler, soit l'idée d'évaluer notre force et d'en faire rapport à l'alliance.

Lorsqu'il s'agit du gouvernement du Canada et de notre structure de GI-TI et de la cybersécurité à cet égard, dans le cadre de la Loi sur la défense nationale, le ministère de la Défense nationale a un mandat clair, soit celui de défendre la Défense, et nous pouvons le faire avec nos capacités et nos structures actuelles.

Pour ce qui est des opérations de déploiement, nous recevons des directives du gouvernement. Le gouvernement doit nous le demander, qu'il s'agisse d'opérations terrestres, aériennes ou en mer ou du cyberespace ou de l'espace. Nous répondons à une demande du gouvernement, que ce soit au pays ou à l'étranger, et cela devient une mission. Cela devient une opération, et c'est dirigé par le commandant du Commandement des opérations interarmées, comme je l'ai déjà dit. Je dirais que le mandat de protéger le gouvernement et les données du gouvernement est, en fait, donné au Centre de la sécurité des télécommunications, et il collabore étroitement avec Services partagés à cet égard. Il nous aide à gérer les parties de notre réseau qui sont liées à l'arrière-boutique du gouvernement, pour ainsi dire, avec Services partagés, mais nous avons toujours la responsabilité de défendre la Défense.

Je voulais seulement que vous compreniez que le ministère de la Défense nationale n'a pas du tout de mandat visant à protéger ou à défendre le gouvernement, à moins que ce dernier lui en fasse la demande, ce qui s'est déjà produit. Pour des problèmes comme le piratage au Conseil national de recherches du Canada ou d'autres événements auxquels le gouvernement a fait face, il est arrivé qu'on demande au ministère de la Défense nationale d'agir dans le cadre d'une opération nationale et de fournir des services au gouvernement à cet égard. Je voulais seulement expliquer...

● (0940)

Mme Leona Alleslev: En fait-on rapport à nos alliés par la suite? En définitive, c'est un élément important. Jadis, il convenait de ne pas aller au-delà des frontières, mais ce n'est plus le cas, car les faiblesses de notre cyberenvironnement ne touchent pas que notre pays.

M. Len Bastien: C'est bien vrai. Merci.

Monsieur le président, comme je l'ai déjà mentionné, nous participons à plusieurs tribunes. Il y a l'environnement très secret dans le cadre duquel les dirigeants principaux de l'information des organismes du renseignement du Groupe des cinq se rencontrent deux fois par année. Nous avons une feuille de route technique concernant l'interopérabilité. Nous avons tous le mandat de faire rapport sur la cybersanté à nos conseillers en sécurité nationale. Il y a des mécanismes en place nous permettant d'informer nos alliés sur notre cybersanté à presque tous les niveaux. Je pourrais ramener cela au niveau secret; le conseil de commandement, de contrôle, de communications et d'informatique se réunit régulièrement et parle de la cybersanté de notre réseau secret. Nous communiquons constamment avec nos alliés et vice versa.

Mme Leona Alleslev: Cela inclut-il nos infrastructures civiles également?

M. Len Bastien: Nous donnons de l'information à jour à nos alliés dans le cadre de ces réunions. Au début de chacune de ces réunions, on demande aux nations de parler de ce qui se passe dans leur gouvernement ou leur capitale ou de donner une perspective plus large liée au mandat ou...

Mme Leona Alleslev: Je ne parle pas seulement de l'infrastructure gouvernementale. Je parle de nos infrastructures nationales, comme nos centrales hydroélectriques et notre Facebook — ou le Facebook des États-Unis que nous utilisons — qui ont pu mener à des soulèvements.

Le président: Je vais devoir vous interrompre. Je vous ai laissé plus de temps que prévu. Je serai ravi d'accorder un peu plus de temps aux autres partis. Je crois qu'il nous faudrait discuter du volet des médias sociaux de la question de l'information, et j'espère que nous le ferons, mais je vais céder la parole à M. Bezan.

Je vais vous donner une minute supplémentaire.

M. James Bezan (Selkirk—Interlake—Eastman, PCC): Merci, monsieur le président. Je remercie nos témoins de leur présence et de leurs témoignages.

Je veux revenir sur la question que Leona vient de soulever. Je crois que notre conception de la cyberdéfense ne correspond peut-être pas tout à fait à la façon dont c'est mis en oeuvre. Quand je pense au ministère de la Défense nationale, aux Forces armées canadiennes, si un chasseur à réaction d'une nation étrangère passe près de notre espace aérien, nous ferons décoller nos chasseurs pour l'intercepter et l'escorter à l'extérieur de la zone. Si un sous-marin faisait son apparition dans le golfe du Saint-Laurent, nos forces navales iraient immédiatement défendre notre souveraineté. Si de petits hommes verts atterrissaient sur l'île de Vancouver, je sais que le ministère de la Défense nationale veillerait à ce que nos troupes aillent sur le terrain. Or, vous dites que si une entité étrangère attaquait notre cyberinfrastructure, s'il s'agit d'une infrastructure civile — qu'il s'agisse de nos réseaux bancaires, de nos réseaux de métro ou d'électricité —, nous resterions les bras croisés et laisserions le ministère de la Sécurité publique intervenir et celui de la Défense nationale n'irait pas défendre notre souveraineté.

S'agit-il d'une politique ou d'une disposition législative?

M. Len Bastien: Permettez-moi d'apporter des précisions. Je crois avoir dit qu'à la demande du gouvernement, les ressources de Défense nationale peuvent être mises à contribution dans n'importe quel environnement, dont le cyberenvironnement, pour régler un problème national, pour l'intérêt national ou pour assurer la sécurité nationale. Je n'ai pas dit qu'une politique ou une disposition nous interdisaient de le faire; j'ai dit que nous ne prendrions pas la décision de façon unilatérale. C'est le gouvernement qui prendrait la décision et ce sont les Forces armées canadiennes qui agiraient.

M. James Bezan: Si l'attaque était menée par une entité étrangère, cela ne deviendrait-il pas automatiquement une question de sécurité nationale relevant du ministère de la Défense nationale?

M. Len Bastien: Rich, voulez-vous en dire davantage?

Cmdre Richard Feltham: Je crois qu'il est important de savoir quel est notre mandat et ce que le gouvernement souhaite que notre ministère et les Forces armées canadiennes fassent. À l'heure actuelle, notre mandat consiste à protéger les réseaux des Forces armées canadiennes et à fournir de l'aide lorsqu'on nous le demande.

Pour revenir à un point dont il a déjà été question, monsieur le président, concernant l'infrastructure nationale, faisons-nous rapport à l'OTAN de l'état de notre cyberinfrastructure et de notre infrastructure nationale essentielles? À ma connaissance, ce n'est pas ce que font le ministère de la Défense nationale et les Forces armées canadiennes. À moins qu'on nous donne un mandat visant à soutenir l'infrastructure civile, ce n'est pas inclus dans notre mandat actuel.

M. James Bezan: Parlons alors de l'OTAN.

Vous avez des groupes de travail et des commandements opérationnels interarmées. Les membres de l'OTAN ont appris de dures leçons. Nous avons des troupes en Lettonie dans le cadre d'une présence avancée renforcée et nous avons des troupes en Ukraine. L'opération Unifier n'est pas nécessairement une opération de l'OTAN, mais l'Ukraine, la Lettonie, l'Estonie et d'autres partenaires ont subi des attaques. Des réseaux d'électricité ont été mis hors services et des services de métro et de transports ont été interrompus à cause de cyberattaques. Parmi les leçons apprises qui ont été communiquées à l'OTAN, lesquelles ont pu être enseignées aux fournisseurs civils de tels services ici au Canada?

● (0945)

M. Len Bastien: Ce sont d'excellents exemples.

À ce stade-ci de l'évolution de notre cyberinteropérabilité, comme l'a mentionné Rich un peu plus tôt, à notre connaissance, dans la structure actuelle, il n'y a pas de séance de rétroaction immédiate, pour ainsi dire, pour les nations, les alliés, par laquelle ces leçons apprises seraient communiquées.

Nous communiquons de l'information aux plus hauts niveaux, dans les environnements classifiés du renseignement — très secret, par exemple. On parle d'une communication plus ouverte et facile. C'est simplement un plus petit environnement à gérer. Honnêtement, nous ne gérons ou ne surveillons pas nécessairement les environnements élargis des membres de l'OTAN et les exploitations qui s'y produisent.

M. James Bezan: Or, je croyais que l'OTAN avait mis sur pied un centre d'excellence en cyberdéfense en Estonie. N'en profitons-nous pas pour utiliser les leçons apprises? C'est seulement que j'en conclus qu'ils se servent des attaques commises contre les infrastructures civiles comme des leçons apprises à communiquer à d'autres nations en veillant à ce que nous ayons les pare-feux et les mécanismes de cyberdéfense qui conviennent.

M. Len Bastien: Nous participons à ce centre d'excellence. Il est assez récent et évoluera rapidement. Je suis sûr que nous en profiterons davantage au fil du temps.

Nous tirons des enseignements des exploitations qui se produisent partout dans le monde. Si une vulnérabilité est exploitée, l'ensemble de la communauté réagit en la corrigeant et en tire des leçons. Nous ne sommes pas complaisants lorsque ces événements se produisent. Nous sommes très au courant. Ce n'est peut-être même pas nécessairement dans le cadre de nos alliances avec l'OTAN ou le Groupe des cinq que nous trouvons le moyen de redémarrer un service ou de remettre quelque chose en état de conformité en réagissant à ces exploitations. C'est fait par l'exploitation et l'entretien de notre cyberenvironnement.

M. James Bezan: L'article 5 de l'OTAN peut se résumer comme suit: une attaque contre une seule partie est une attaque contre l'ensemble des parties. On n'y a eu recours qu'une fois, soit pour les attentats du 11 septembre et bien entendu, ce sont des infrastructures civiles qui avaient été la cible d'attaques. Le projet de loi C-59 ferait en sorte qu'une position de cyberdéfense serait fournie au ministère de la Défense nationale et au Centre canadien de la sécurité des télécommunications. Qu'est-ce qui mènerait au recours à l'article 5 dans le monde virtuel?

M. Len Bastien: C'est une très bonne question.

M. James Bezan: Je sais qu'elle est hypothétique.

M. Len Bastien: Concernant les effets d'un incident, c'est du cas par cas. Ils sont évalués de la même façon que les effets produits dans tout autre environnement.

Pour tenter de répondre à votre question, je dirais que du point de vue militaire, un cyberévénement serait maintenant évalué de la même façon que tout autre type d'événement cinétique, et l'article 5 pourrait s'appliquer si l'on juge que les répercussions sur la nation sont suffisantes pour invoquer la politique. Il ne m'appartient vraiment pas de dire ce qui mènerait à le faire.

Je ne suis pas en désaccord avec vous lorsque vous dites que ce sont les industries de nos pays qui sont vulnérables à ce type d'attaques. Je veux simplement vous expliquer notre mandat, qui consiste à aider les Canadiens et à leur fournir des services par l'institution de défense nationale, de sorte que vous sachiez bien à quoi il faut s'attendre de nous si une telle chose se produit.

Le président: Merci.

Allez-y, monsieur Robillard.

M. Yves Robillard (Marc-Aurèle-Fortin, Lib.): Merci, monsieur le président. Je vais céder une partie de mon temps à mon collègue, le député Fisher.

Monsieur, pourriez-vous nous parler des aspects qui ont fait en sorte que l'entreprise canadienne MDA s'est vu octroyer le contrat de 15 millions de dollars pour la réalisation du projet Triton de l'OTAN?

M. Len Bastien: Merci de poser la question, monsieur le président.

Je n'ai pas en main aujourd'hui les détails de cette entente d'échange avec l'OTAN. Cela devait être un exemple de la valeur du rendement du capital investi en exposant l'industrie canadienne à l'agence de l'OTAN qui dépense plus de 450 millions d'euros par année. Une grande partie du travail et des contrats ne se retrouvait pas en Amérique du Nord. Cela restait en Europe, et nous étions motivés de voir l'industrie canadienne obtenir une meilleure part du marché. Cela devait être un exemple de réussite, si vous voulez, de notre placement dans le travail de l'agence. Si vous voulez, nous pouvons vous revenir avec de plus amples détails sur la portée de ce que signifiera ce contrat pour MDA, mais ce sera plus tard. Je n'ai pas les détails en main aujourd'hui.

● (0950)

M. Yves Robillard: Pour donner suite à la question, pouvez-vous en dire davantage sur le projet Triton et sur la façon dont il contribue au projet de systèmes d'information de commandement et de contrôle maritimes?

M. Len Bastien: Merci, monsieur, monsieur le président.

Comme je l'ai mentionné, les détails de ce contrat... Le contrat n'était pas avec la Défense nationale, mais avec l'agence à l'OTAN. Ce que j'en sais se limite à ce que je vous ai dit aujourd'hui, c'est-à-dire à sa réussite pour l'industrie canadienne et à sa valeur. Pourvu que nous y ayons accès, nous serons contents de vous fournir les détails sur la portée et les exigences de ce contrat. Je ne les ai pas apportés aujourd'hui.

M. Yves Robillard: Merci, monsieur.

M. Darren Fisher: Merci, monsieur le président.

Messieurs, vous avez tous les deux mentionné l'initiative 65 et l'amélioration des capacités cryptographiques. J'espère que vous pouvez en dire un peu plus long à ce sujet et me donner des exemples d'amélioration.

M. Len Bastien: Je vous remercie encore une fois pour la question, monsieur le président.

La cryptographie est à la base de notre capacité à communiquer et à transmettre l'information de manière sécuritaire. Pour pouvoir le faire entre alliés, il faut une architecture de cryptographie qui est non seulement vaste et complexe, mais aussi adaptée à nos besoins.

Le ministère de la Défense nationale a beaucoup investi dans l'interopérabilité de la cryptographie entre les pays alliés. L'évolution de la cryptographie fait suite au vecteur de menace qui devient de plus en plus problématique. L'évolution de la cryptologie est donc très sérieuse. Nous avons le mandat de demeurer conformes dans le cadre des alliances, et c'est un important secteur d'investissement. Il est énoncé dans notre politique que nous allons non seulement maintenir la cryptographie, mais aussi la faire progresser jusqu'au niveau de conformité afin de pouvoir continuer de mener des opérations et des interopérations avec nos alliés et de communiquer de manière sécuritaire.

M. Darren Fisher: Tout cela est bien, et cela me dit ce que vous voulez accomplir, mais comment la faites-vous progresser? Quel est le genre de choses que vous pouvez faire pour l'améliorer?

M. Len Bastien: Je ne suis pas techniquement outillé pour parler de façon très détaillée de notre ingénierie cryptographique, mais laissez-moi vous expliquer.

Le concept de la cryptographie est un concept d'échange de clés. Autrement dit, il faut les deux moitiés de la clé pour ouvrir le compartiment ou le document, ou la « crypte ». La capacité des vecteurs de menace à déformer ou à casser les clés est en constante évolution, et nous devons donc fabriquer de meilleures clés, mais nous ne pouvons pas le faire unilatéralement, car nous ne pourrions pas parler à nos alliés. En collaborant, nous établissons les critères pour avoir des clés évoluées. Nous parcourons ensuite le réseau mondial — la structure, si vous voulez — et nous mettons à niveau et à jour tout le matériel et tous les logiciels qui génèrent les clés. C'est un environnement très délicat et complexe, mais un environnement dans lequel nous nous débrouillons très bien, et je dirais que nous sommes en bonne posture sur le plan de la conformité entre nos pays.

Le président: Il ne vous reste pratiquement plus de temps, monsieur Fisher.

Je vais donner la dernière intervention officielle à M. Garrison, afin que ce soit juste pour tout le monde.

M. Randall Garrison: Merci, monsieur le président.

Je veux changer un peu le sujet. Je pense que nous nous heurtons à un phénomène de cyberguerre qui ne cadre pas vraiment avec les protocoles normaux et les règles de la guerre. Cela se trouve à la limite de ces protocoles et de ces règles. Les protocoles internationaux interdisent de s'en prendre à des cibles civiles. Nous avons l'habitude de ce genre de principes. Je sais qu'aucun de vous ne représente le CST, mais la mesure législative, le projet de loi C-59, dont le Parlement est saisi propose d'autoriser l'utilisation active de cyberattaques dans les actes de sabotage. Cela me préoccupe que nous, en tant que Canadiens, intervenions dans un domaine de conflit international qui n'est pas bien réglementé à l'échelle internationale.

Je suppose que ma question s'adresse largement à M. Feltham. Quelle est votre relation avec le CST pour ce qui est de ses, je dirais, demandes en faveur d'un recours aux cyberattaques actives?

Pour le deuxième volet de ma question, estimez-vous être déjà autorisés au ministère de la Défense nationale à recourir à des cyberattaques actives contre d'autres États et des étrangers dans l'intérêt du CST? Êtes-vous déjà autorisés à agir ainsi? Quelle est votre relation avec le CST à cet égard?

● (0955)

M. Len Bastien: Je vais commencer et demander ensuite à mon collègue de poursuivre.

À vrai dire, la relation avec le CST n'est pas si complexe. Il faisait partie de notre ministère il n'y a pas très longtemps. Quand la loi sur le CST a été créée, il a reçu le mandat de soutenir d'autres organismes gouvernementaux de sécurité grâce à ses capacités, si je puis dire. Je peux parler de ses capacités, ce qui nous écarte un peu du sujet. Je peux vous dire qu'elles seraient très utiles pour nous sur le plan de la cybersécurité. Je ne crois pas que le gouvernement veut que le ministère de la Défense nationale crée des capacités équivalentes, et on nous a donc demandé de travailler avec le CST pour former une équipe. Nous allons faire des déploiements et mener des opérations en tant qu'équipe, car le CST a les capacités nécessaires.

Cependant, quand la loi sur le CST a été créée, le ministère de la Défense nationale ne figurait pas parmi les organismes qu'il pouvait soutenir, ce qui est paradoxal. Nous ne faisions qu'un, et il n'était donc pas nécessaire de mentionner le ministère dans la loi. Je pense que certaines modifications du projet de loi seront utiles pour remédier à cet aspect de la politique législative, pour nous permettre de collaborer encore plus activement. Cela répond à une partie de votre question. Je tenais vraiment à expliquer que nous irons de l'avant en tant qu'équipe aussitôt que nous le pourrons.

Pour ce qui est de l'autre partie de votre question, à l'heure actuelle, en ce qui a trait au jour zéro des capacités en cybersécurité, nous avons des capacités limitées dans le cyberespace actif que nous pourrions mettre à profit pour appuyer les missions si nous n'avions pas le CST. Je ne veux pas vous donner l'impression que nous pourrions avoir de vastes capacités en matière de cybersécurité, ce qui serait préoccupant pour les Canadiens, mais la capacité de bloquer une radio, un téléphone, un site Web ou un fournisseur de services est une chose que nous mettons rapidement au point pour soutenir les missions.

M. Randall Garrison: Êtes-vous autorisés à le faire en ce moment?

M. Len Bastien: En vertu de la Loi sur la défense nationale, nous sommes autorisés à mettre ces actifs à contribution. Nous collaborons avec nos collègues du CST afin de faire preuve de transparence auprès du gouvernement par rapport à ce que nous mettons au point et utilisons dans le cadre gouvernemental.

C'est un nouveau territoire. La décision du gouvernement de nous confier le mandat de mener des cyberopérations actives — des cyberoffensives, comme vous le décrivez — n'a pas été prise à la légère, et nous ne réagissons pas à la légère au sein de notre organisation.

Nous allons tenir des séances d'information et nous aurons des comptes à rendre par rapport aux structures que nous mettons en place pour mener ce genre de cyberopérations actives.

Comme je l'ai dit plus tôt, nous ne pouvons pas mener unilatéralement ce genre d'activités comme nous le faisons pour les autres activités militaires sans surveillance ni demande du gouvernement. Au bout du compte, il y a une structure de commandement et de contrôle qui est liée à l'administration du gouvernement avant que nous puissions nous adonner activement à ce genre d'activité. J'espère que cela répond à votre question.

M. Randall Garrison: Si vous estimez être déjà autorisés, quelles sont les restrictions avec lesquelles vous devez composer? Quelles sont les restrictions qui ont été mises en place pour s'assurer qu'une éventuelle cyberorganisation offensive n'entre pas en conflit avec le droit international et adhère à certains des principes de base concernant la distinction entre les cibles militaires et civiles, ce genre de principes?

M. Len Bastien: Merci, monsieur.

Monsieur le président, je vais demander à mon collègue, le commodore Feltham, de répondre, car il est mieux placé pour en parler en tant qu'officier militaire et opérateur d'expérience.

Cmdre Richard Feltham: Merci, monsieur le président, de me donner l'occasion de répondre à la question.

Comme il a été dit plus tôt, la politique sur les cyberopérations actives pour les Forces armées canadiennes provient de la récente politique de défense. Nous travaillons avec nos partenaires internationaux et gouvernementaux pour créer cette capacité.

Vous avez demandé, monsieur le président, comment nous nous assurons que les cyberopérations actives offensives, en tant qu'élément de cybersécurité active, adhèrent au droit des conflits armés. Je peux vous dire que, comme pour toutes les opérations militaires, en cinétique ou dans le cyberespace, les Forces armées canadiennes ne mènent que des opérations conformément au mandat du gouvernement et au droit des conflits armés. C'est ce qui nous guide jour après jour, et il n'y a pas d'exception à cela.

Pour ce qui est des opérations en cours dans le domaine de la cybernétique, ce n'est pas mon domaine, et je ne peux pas en parler de façon très détaillée, mais je peux vous assurer que de notre point de vue — et j'ai mis au point cette capacité avec nos partenaires —, nous nous en tenons aux mandats. Nous faisons des missions gouvernementales et nous respectons le droit des conflits armés.

M. Randall Garrison: Existe-t-il des mécanismes spéciaux de reddition de comptes au gouvernement qui ont été mis en place compte tenu de la nature secrète des cyberopérations?

● (1000)

M. Len Bastien: Dans notre structure hiérarchique, lorsque nous recourons aux services des Forces armées canadiennes, nous passons par le chef d'état-major de la Défense. Il présente au gouvernement un rapport sur les opérations des Forces canadiennes. Je crois qu'il serait préférable que ce soit son bureau qui explique avec exactitude à quoi les modalités ressemblent d'un point de vue gouvernemental, mais je peux vous assurer que nous lui rendons des comptes. Je vais m'en tenir à cela.

M. Randall Garrison: Merci, monsieur le président.

Le président: Bien. Voilà qui termine les questions officielles. Nous avons encore du temps, et je vais donc, comme on pouvait s'y attendre, faire un autre tour. Les interventions seront de cinq minutes. Les libéraux interviendront en premier. Ce sera ensuite au tour des conservateurs et ensuite de retour à M. Garrison.

Je vais devoir garder un peu de temps à la fin. Il y a quelques motions que je dois régler, mais nous allons nous en occuper le moment venu.

Je donne la parole à M. Rioux. Vous avez jusqu'à cinq minutes. Partagez votre temps si vous le souhaitez.

[*Français*]

M. Jean Rioux (Saint-Jean, Lib.): Merci, monsieur le président.

Monsieur Bastien, j'ai une question de base à vous poser. Quelles sont les principales menaces cybernétiques qui pèsent sur le Canada? Sont-elles sensiblement les mêmes que celles auxquelles fait face l'OTAN?

M. Len Bastien: Merci de la question.

[*Traduction*]

Les vulnérabilités relatives aux vecteurs de menace que nous surveillons changent tous les jours. L'industrie ou d'autres gouvernements nous en indiquent de nouvelles tous les jours, et nous les évaluons.

Une vulnérabilité n'est pas une menace avant d'être exploitée, et nous réagissons donc constamment à ce que j'appellerais des « vulnérabilités ». Cela dit, ce serait la même chose pour l'industrie, pour les Canadiens et pour l'OTAN lorsque nous nous rendons compte de ces vulnérabilités. Nous travaillons habituellement en tant que gouvernement, qu'ensemble d'organismes gouvernementaux, pour parvenir au bon plan de rétablissement et pour remédier à ces vulnérabilités à l'aide de correctifs et de l'évolution de la technologie visant à prévenir leur exploitation.

Selon la façon dont cela fonctionne, les bons essaient de découvrir les vulnérabilités et de se protéger contre leur exploitation. Les méchants essaient de comprendre comment les exploiter. C'est donc une course. Notre capacité à garder les devants repose sur notre posture en matière de sécurité et sur la conformité à nos normes, que ce soit au sein du gouvernement ou du ministère de la Défense nationale. Je dirais que l'agence de l'OTAN qui est responsable de sa cybersécurité a le même point de vue, alors qu'elle tente constamment de réagir face à des vulnérabilités potentielles portées à notre attention et pour lesquelles nous devons prendre des mesures.

J'espère que cela explique un peu le milieu pour savoir qu'il n'est pas question d'un seul incident qui se produit. Aux nouvelles, on parle habituellement d'une série de vulnérabilités qui ont été exploitées. Notre capacité à devancer ces vulnérabilités et à demeurer protégés revient à notre capacité à interopérer avec nos alliés, à travailler étroitement avec l'industrie, même le milieu universitaire, ainsi qu'avec nos collègues du gouvernement. Nous réagissons constamment à de nouvelles vulnérabilités.

[*Français*]

M. Jean Rioux: Je vais reprendre le fil des questions de M. Garrison et parler du SCRS.

On sait que le ministère de la Défense nationale et le SCRS sont deux entités distinctes. J'ai cru comprendre de votre réponse tout à l'heure que vous n'aviez pas le mandat de travailler avec le SCRS et que, selon la loi, vous n'étiez pas tenus de travailler ensemble. Est-ce une fausse impression?

M. Len Bastien: J'aimerais clarifier la nature des relations entre les deux entités dont il est question.

[*Traduction*]

Le mandat du Centre de la sécurité des télécommunications diffère grandement de celui du SCRS. Nous travaillons avec les deux organismes. Ce que j'ai décrit, c'est une relation avec le CST qui porte précisément sur la cybersécurité et les opérations actives dans ce domaine. Cela ne va pas à l'encontre du travail que nous faisons avec ces deux organismes dans de nombreux autres domaines du renseignement. Pour ce qui est du cyberrôle, du cybermandat que j'ai décrit, la relation était avec le CST. Nous avons également une très forte relation d'interopérabilité avec le SCRS, mais pour des raisons différentes.

Le président: Il nous reste un peu de temps, et je vais donc donner la parole à M. Spengemann.

Allez-y.

M. Sven Spengemann: Merci, monsieur le président.

J'ai une question d'ordre générale qui revient à votre échange avec ma collègue, Mme Alleslev. Vous lui avez parlé de plusieurs catégories d'information qui ont été communiquées en fonction d'une autorisation de sécurité de niveau très secret et de niveau secret. Déterminer si le niveau d'habilitation de sécurité du comité doit être élevé pour qu'il puisse consulter toute la documentation dont il est saisi est une décision stratégique.

Je me demande si vous pouvez dire au comité, selon votre point de vue et plus particulièrement sur le plan de la cybersécurité et de sa dynamique qui évolue rapidement, ce que verrait le comité si sa cote de sécurité était plus élevée. Autrement dit, combien d'autres discussions détaillées pourrions-nous avoir?

Je suis conscient que c'est une séance publique, mais dans le cadre d'une réunion pour laquelle notre habilitation de sécurité serait plus élevée, dans quelle mesure pourrions-nous mieux comprendre?

● (1005)

M. Len Bastien: Une partie de la réponse à cette question reviendra à mon opinion personnelle, et je vais donc éviter cela. Toutefois, je vous dirais en toute sincérité que je suis très à l'aise avec les renseignements que je vous ai communiqués aujourd'hui, car un changement de classification n'aurait pas modifié mon témoignage de façon importante. Je crois que l'entrevue d'aujourd'hui vous permet de vous faire une bonne idée de la situation. En tout cas, je l'espère.

Habituellement, la classification concerne plus le moment de la divulgation que le contenu de l'information divulguée. Nous avons recours à la classification pour protéger des intérêts nationaux liés à la sécurité nationale et nous le faisons parce qu'à tout moment, des renseignements auront une importance considérable ou présenteront un risque énorme s'ils se retrouvent entre de mauvaises mains. Toutefois, en ce moment, ces mêmes renseignements ne représentent plus une menace et c'est pourquoi ils ne devraient plus être classifiés.

Je crois qu'une discussion non classifiée peut offrir une énorme quantité de renseignements sur les leçons apprises et sur nos réactions dans certaines situations, et que ces renseignements vous donneront une très bonne idée de la façon dont nous menons nos activités quotidiennes. Lorsque nous commençons à parler d'opérations actives et de nos plans pour le lendemain, ce niveau de classification existe pour une raison. En effet, il vise à protéger des intérêts importants pour les Canadiens, et c'est à ce moment-là qu'un défi peut se poser.

Dans la discussion d'aujourd'hui, nous ne sommes pas allés aussi loin, et j'espère donc que vous avez obtenu suffisamment de renseignements pour éclairer vos décisions futures.

Le président: Merci.

Allez-y, monsieur Bezan.

M. James Bezan: Merci. Je partagerai mon temps avec M. Paul-Hus.

Dans le premier témoignage, nous avons parlé un peu de défense intelligente au sein de l'OTAN et de son utilisation dans l'environnement cybernétique. L'Union européenne a récemment mis sur pied la coopération structurée en permanence pour la sécurité et la défense, qu'on appelle aussi PESCO. Quelles répercussions cela aura-t-il sur la défense intelligente, surtout dans un contexte cybernétique? Sera-t-elle renforcée ou améliorée par ce mécanisme ou s'agit-il d'un facteur concurrent?

M. Len Bastien: J'aimerais tout d'abord préciser que je ne connais pas tous les détails de PESCO, et que je ne serai donc peut-être pas en mesure de fournir une réponse complète à votre question. J'aimerais demander au commodore Feltham s'il a quelque chose à ajouter. Il se peut que nous devions vous communiquer plus tard les répercussions de PESCO sur les intérêts cybernétiques de l'OTAN. Je n'ai tout simplement pas ces renseignements avec moi aujourd'hui.

Cmdre Richard Feltham: Je suis malheureusement dans la même situation en ce qui concerne ces répercussions. C'est habituellement plus facile dans une discussion plus générale, lorsqu'un plus grand nombre de personnes discutent de la cybermenace et échangent des renseignements à ce sujet. Si des intérêts partagés passent de l'un à l'autre, cela pourrait entraîner des complications, mais à ce jour, je n'ai rien entendu de tel, monsieur le président.

M. James Bezan: Merci.

[*Français*]

M. Pierre Paul-Hus: Merci, monsieur le président.

Je trouve les propos d'aujourd'hui très éclairants, mais aussi un peu inquiétants. En matière de défense et de cybersécurité, votre rôle est de protéger les Forces canadiennes et l'infrastructure de défense. Lorsqu'il s'agit des opérations, on s'adresse au CST.

Ma question concerne l'OTAN. Certaines de nos troupes sont déployées présentement; les Forces canadiennes assurent notre protection. Si nous décidons d'attaquer Kaliningrad, par exemple, et de fermer sa centrale électrique, qui va mener cette attaque: les Forces canadiennes ou le CST?

M. Len Bastien: Je vous remercie de la question.

[*Traduction*]

Je répondrai en anglais, car cette industrie est vraiment beaucoup plus facile à décrire.

Permettez-moi de préciser certaines choses. Toutes les opérations militaires sont dirigées par les Forces armées canadiennes. La participation du CST dans un environnement opérationnel se fait sous l'autorité des Forces armées canadiennes. En ce moment, la capacité de l'organisme de nous prêter main-forte est en quelque sorte entravée par la loi, car nous ne sommes pas un organisme avec lequel le centre est autorisé à mener ses activités. Nous tentons de remédier à cette situation par l'entremise de ces modifications législatives.

Le scénario que vous avez décrit comporte une approche fondée sur une équipe intégrée et dirigée par l'armée qui utiliserait nos compétences et celles du CST en collaboration. Cela se fera plus tard, lorsque les modifications législatives...

● (1010)

[*Français*]

M. Pierre Paul-Hus: Après cette réunion-ci, je vais me rendre à la séance du Comité permanent de la sécurité publique et nationale, où il sera question du projet de loi C-59. Nous allons justement rencontrer le commissaire du CST.

Dans ce projet de loi, il est question de transférer au ministre de la Sécurité publique et de la Protection civile les pouvoirs du CST qui étaient reliées à la défense nationale. Le projet de loi contient aussi des dispositions selon lesquelles on doit obtenir une autorisation du ministre des Affaires étrangères pour mener une opération.

Comment voyez-vous cela?

[*Traduction*]

M. Len Bastien: En général, les répercussions du projet de loi sur le CST concernent davantage les activités du CST que les nôtres. Le CST doit pouvoir mener des activités cybernétiques et travailler avec nous d'une façon plus intégrée que nous le pouvons aujourd'hui.

Je tiens à vous faire savoir que nous avons fait le travail et les exercices nécessaires et que nous avons mené des opérations simulées avec les intervenants du CST. Nous avons déployé de grands efforts pour être en mesure de collaborer avec cet organisme dans le cadre d'opérations cybernétiques futures, mais les paramètres seront établis par le gouvernement, et je ne peux donc pas parler des autres volets.

[*Français*]

M. Pierre Paul-Hus: Est-ce que la plupart des pays de l'OTAN ont des concepts similaires? Autrement dit, la défense comprend-elle des éléments de cybersécurité, en plus des questions touchant la protection civile? Travaillent-ils tous de façon intégrée?

[*Traduction*]

M. Len Bastien: Comme je l'ai dit, nous avons d'excellentes relations avec nos alliés. Je peux vous dire que les entités avec qui je travaille régulièrement n'ont pas toutes la même structure de gouvernance lorsqu'il s'agit de l'emplacement des capacités cybernétiques au sein du gouvernement. Je peux vous parler de la participation du Canada, et j'espère le faire, mais je ne peux pas parler...

[*Français*]

M. Pierre Paul-Hus: Par comparaison avec les modèles des autres pays, celui du Canada est-il efficace? Y en a-t-il de meilleurs, par exemple au Royaume-Uni ou aux États-Unis?

[*Traduction*]

M. Len Bastien: La notion de savoir si nous sommes bons ou meilleurs que nos alliés ou si nous sommes les meilleurs représente une opinion. C'est ce que nous avons établi au Canada. Nous jugeons que nos compétences, notre structure et nos portefeuilles en matière de cyberdéfense sont très efficaces. Ces éléments ont bien fonctionné dans le domaine des renseignements d'origine électromagnétique et dans d'autres domaines et capacités que nous avons intégrés aux Forces armées canadiennes. C'est la structure que nous avons choisi de proposer au gouvernement en ce qui concerne les cyberopérations.

Le commodore Feltham a peut-être une idée plus précise des autres armées. Pour parler simplement, il a été déployé et il est opérateur; un membre civil de l'équipe de défense n'a pas cette perspective.

Avez-vous quelque chose à ajouter, commodore Feltham?

Le président: Je dois vous arrêter ici. Vous serez peut-être en mesure de revenir sur le sujet, mais je dois donner la parole à M. Garrison.

Vous avez la parole.

M. Randall Garrison: Merci beaucoup, monsieur le président.

J'apprécie beaucoup les témoignages sur la cyberdéfense que nous avons entendus aujourd'hui. Je suis également heureux d'apprendre que nous faisons de notre mieux en matière de cyberdéfense, mais dans votre témoignage d'aujourd'hui, vous avez mentionné que le projet de loi C-59 accordera au CST le pouvoir nécessaire de mener des opérations cybernétiques actives, un pouvoir que le MDN juge déjà posséder.

Dans le projet de loi, l'article 31 énonce essentiellement que les opérations cybernétiques actives, après avoir été autorisées, peuvent être menées en dépit de toute loi adoptée par le Parlement ou par un État étranger. C'est un pouvoir à très large portée.

J'aimerais savoir si vous pensez que le MDN est déjà autorisé à mener des opérations cybernétiques actives sans devoir se préoccuper des lois adoptées par le Parlement ou par un autre État.

M. Len Bastien: Permettez-moi de préciser la perception de nos relations avec le Centre canadien de la sécurité des télécommunications que j'aimerais vous transmettre aujourd'hui.

Nous avons des capacités technologiques dont nous avons eu besoin pour mener des opérations précédentes. Ces capacités nous sont très utiles, mais elles sont en quelque sorte limitées. Avant d'investir dans l'accroissement de cet arsenal d'armes cybernétiques, si l'on peut dire, nous reconnaissons qu'une grande partie de cette capacité existe déjà au sein du CST. La difficulté consiste à obtenir l'accès à cette capacité et à donner au CST le mandat législatif d'opérer à nos côtés et d'utiliser ses capacités dans le cadre d'une structure militaire. C'est la lacune que nous tentons de combler, et c'est une très petite partie du projet de loi.

Le reste du projet de loi et les modifications proposées visent surtout le Centre canadien de la sécurité des télécommunications et, à mon avis, je n'ai pas les compétences nécessaires pour formuler des commentaires à cet égard.

Richard, aimeriez-vous répondre à un élément de cette question...?

● (1015)

Cmdre Richard Feltham: Oui. Monsieur le président, j'aimerais ajouter une chose.

Comme de nombreux autres partenaires gouvernementaux, nous collaborerons avec le Centre canadien de la sécurité des télécommunications afin d'accroître les capacités des Forces armées canadiennes, mais je tiens à préciser certaines choses. En effet, toutes les opérations auxquelles participent les Forces armées canadiennes, que ce soit dans les structures militaires traditionnelles de la marine, des forces aériennes, de l'armée ou du domaine cybernétique, sont des opérations militaires mandatées par le gouvernement et menées conformément au droit des conflits armés et aux règles d'engagement expressément autorisées par le chef d'état-major de la défense par l'entremise du gouvernement du Canada.

La réponse à votre question, c'est que nos opérations cybernétiques ne seraient pas menées différemment de celles menées dans toute autre structure militaire cinétique non mandatée par le gouvernement. Je ne suis pas en position de me prononcer sur ce que ferait le CST dans le cadre de son mandat, monsieur.

M. Randall Garrison: Il me semble que certaines des pratiques courantes qu'on qualifie d'opérations cybernétiques « actives » sont la version moderne de tactiques comme le port de l'uniforme ennemi, c'est-à-dire le type de choses que nous avons tenté d'interdire expressément dans les conventions internationales. Par exemple, l'usage trompeur des uniformes a été interdit dans la Convention de La Haye de 1907.

Savez-vous si certains de nos partenaires de l'OTAN — et je sais que cela ne fait pas nécessairement partie de votre mandat — ont mené des activités qui visent à tenter de préciser les limites acceptables dans le cadre d'opérations cybernétiques actives?

M. Len Bastien: Permettez-moi de répondre en premier, et je demanderai ensuite au commodore Feltham de formuler des commentaires sur les lacunes possibles dans les politiques internationales liées à la mobilisation cybernétique ou aux règles d'engagement dans les opérations cybernétiques.

Selon mon expérience, nous nous sommes rendu compte qu'en réalité, chaque nation avait adopté des lois et des politiques différentes relativement à la participation de son armée à des opérations cybernétiques. En effet, certaines nations appuient pleinement les opérations cybernétiques offensives, alors que d'autres les interdisent. Il existe des différences importantes entre les pays et leurs structures respectives à cet égard. Je crois que le Canada examine ses options. Notre politique « Protection, Sécurité, Engagement » a proposé une portée raisonnable, en quelque sorte, pour les activités cybernétiques, et on nous a donné des directives précises pour mettre cela en oeuvre.

Commodore Feltham, si des membres de l'OTAN ou d'autres organisations mènent des activités liées à l'élaboration de politiques sur les règles d'engagement dans les opérations cybernétiques, j'aimerais que vous nous en parliez.

Cmdre Richard Feltham: Si j'ai le temps, monsieur le président, j'aimerais continuer.

Le président: Oui, mais soyez bref.

Cmdre Richard Feltham: Aux fins d'éclaircissements, monsieur le président, les « opérations cybernétiques actives » sont une combinaison de ce que nous considérerions comme étant un mode de défense actif et un mode de défense offensif. C'est la différence entre attendre que l'ennemi franchisse le mur de votre château pour l'attaquer ou l'attaquer dès qu'il atteint votre mur. C'est une défense active. L'autre méthode consiste à avancer jusqu'à l'ennemi pour mener une attaque active.

Quelle est l'intention? Si mon intention est de me défendre moi-même, je peux adopter un mode actif, mais c'est pour défendre mes propres biens. Si mon intention est d'attaquer les réseaux d'une autre personne, il s'agit d'une activité offensive. L'élément « actif » est présent dans les deux méthodes. La communauté de l'OTAN et les autres communautés s'efforcent de déterminer où se trouvent les limites. Si vous lisez un extrait du *Tallinn Manual*, par exemple, vous constaterez que la communauté juridique et les forces militaires de notre alliance s'efforcent constamment de mieux comprendre tout cela.

Existe-il des règles sur lesquelles s'entendent tous les membres de l'alliance et toutes les nations alliées? Je ne crois pas, mais c'est une conversation émergente et substantielle qui devient de plus en plus importante.

Le président: Merci.

Je sais qu'une personne souhaite obtenir quelques minutes pour poser une question, mais étant donné le temps qu'il reste et les quelques points dont nous devons nous occuper, je ne peux pas lui accorder ces minutes, à moins que tout le monde soit d'accord. Je n'ai pas le temps de donner quelques minutes à tous les intervenants.

Aviez-vous quelque chose à ajouter, monsieur Garrison?

Monsieur Bezan? Non?

J'aimerais donner quelques minutes à Mme Alleslev pour terminer la conversation, et nous aborderons ensuite nos motions.

Allez-y, madame Alleslev. Vous avez environ deux minutes.

Mme Leona Alleslev: Merci beaucoup à toute l'équipe et merci, monsieur le président.

J'aimerais terminer la conversation en revenant sur la question de savoir si vous êtes à l'aise de participer à une conversation non classifiée. Un grand nombre de personnes assises à cette table ont eu ou ont des cotes de sécurité, et c'est la raison pour laquelle ces personnes n'ont pas posé de questions auxquelles vous n'auriez pas été en mesure de répondre. Vous avez mentionné que vous étiez à l'aise avec les réponses que vous avez fournies. Je crois donc que le niveau de conversation s'est fondé sur les questions que nous avons posées et qu'il existe peut-être des niveaux de conversation classifiés auxquels nous n'avons manifestement pas eu accès aujourd'hui.

C'est particulièrement dans ce contexte que nous examinons le chevauchement entre nos infrastructures civiles et militaires relativement à notre santé et notre bien-être à l'échelle nationale et celles de nos alliés lorsqu'il s'agit des renseignements que nous échangeons entre ces deux entités. J'aimerais savoir si vous avez des commentaires à formuler à cet égard.

● (1020)

M. Len Bastien: J'espère que je n'ai pas laissé croire que dans un contexte classifié, dans lequel toutes les conditions auraient été satisfaites, une conversation classifiée dans certains domaines clés ne produirait pas un dialogue plus riche entre les membres d'un comité et nous dans notre rôle de témoins. J'aimerais tout simplement ajouter qu'aujourd'hui, nous avons entendu d'excellentes questions qui m'ont permis de parler de nos activités, de notre situation dans le monde et de nos relations avec nos partenaires sans compromettre la sécurité nationale.

Mme Leona Alleslev: Merci.

M. Len Bastien: Vous avez raison. Les questions devraient-elles...

Mme Leona Alleslev: Merci. Nous n'avons pas posé de questions auxquelles vous n'auriez pas été en mesure de répondre.

M. Len Bastien: Non, et je devrais donc vous en remercier, monsieur le président.

Des voix: Oh, oh!

Le président: C'est un argument circulaire.

M. Len Bastien: En effet.

Nous comparaissons devant votre comité pour participer à un dialogue productif et vous aider dans les travaux très importants que vous effectuez pour aider le ministère à trouver sa place au sein du gouvernement. Je vous suis donc reconnaissant.

Je ne voudrais pas vous donner l'impression qu'une conversation classifiée aurait produit des réponses différentes aux questions auxquelles j'ai répondu aujourd'hui. En effet, si vous aviez posé des questions différentes, vous auriez certainement obtenu des réponses différentes.

Mme Leona Alleslev: Je crois que cela nous cause des difficultés, car nous reconnaissons, surtout dans le domaine cybernétique, que les choses sont beaucoup plus complexes et non définies en raison de la nature changeante de la guerre et parce que, en ce moment, ceux qui nous refuseraient la souveraineté et qui remettraient en question notre sécurité nationale se déplacent très efficacement et ne sont pas limités comme nous le sommes. Pour comprendre le niveau de conversation suivant, nous pensons que nous devons être en mesure d'avoir une conversation sécurisée.

M. Len Bastien: Merci.

Le président: Je croyais qu'il était 10 h 30, car nous venons tout juste de recommencer les réunions du matin. En fait, il est 10 h 45. Je dois vérifier autre chose relativement à la motion. Encore une fois, je suis heureux d'accorder suffisamment de temps à chacun. Mme Romanado avait une question.

Il nous reste un peu de temps, et j'aimerais donc vous donner l'occasion d'intervenir, madame Romanado. Allez-y. Vous avez la parole.

Mme Sherry Romanado (Longueuil—Charles-LeMoyne, Lib.): Merci, monsieur le président.

Merci beaucoup pour vos témoignages. J'ai eu la chance de visiter les installations de MDA il y a deux semaines. Nous avons d'ailleurs grand hâte d'obtenir un complément d'information sur le projet Triton, une nouvelle solution de commandement et de contrôle maritimes pour les systèmes embarqués et déployables.

Nous avons traité quelque peu des actifs déployés aux fins de l'OTAN, surtout pour ce qui est du soutien. Vous avez parlé de 120 à 130 postes en soutien direct aux opérations de l'OTAN. Dans le cadre de la politique « Protection, Sécurité et Engagement », les effectifs militaires devraient s'accroître d'environ 3 500 personnes.

Ce n'est peut-être pas à vous que je devrais poser la question, mais j'aimerais savoir quels genres de programmes de formation sont offerts à nos militaires en matière de cybersécurité, en sachant qu'une partie de ces effectifs supplémentaires y seront affectés dans le contexte de nos opérations communes avec nos alliés de l'OTAN. Compte tenu de l'évolution extrêmement rapide de ces technologies, est-ce que nous collaborons avec l'OTAN pour concevoir ces programmes de formation?

M. Len Bastien: Nous allons effectivement vous communiquer autant d'information que possible au sujet de ce projet qui enthousiasme certes beaucoup les gens de MDA qui pourront vous fournir bien d'autres détails qui nous échappent à titre d'observateurs.

Quant à la formation de notre personnel aux fins de la cybersécurité ainsi que de la coopération avec l'OTAN, comme l'indiquait le commodore Feltham dans ses observations préliminaires, l'OTAN a investi considérablement dans un centre d'excellence pour la simulation cybernétique.

Dans un cadre technologique semblable, on peut notamment mettre à l'essai des armes cybernétiques et voir comment il est possible de réagir à une éventuelle attaque. En tant que partenaires de l'OTAN, les forces canadiennes pourront tirer un réel avantage de ces précieux outils. Nous nous réjouissons à la perspective de pouvoir en bénéficier.

Les engagements pris dans le cadre de la politique gouvernementale prévoient des investissements ministériels sur une période de 20 ans. On ne peut donc pas dire que nous pouvons disposer dès cette année de ces ressources humaines et financières additionnelles. Nous nous employons plutôt à déterminer la façon dont cette politique pourra être mise en oeuvre au cours des 20 prochaines années.

Il est trop tôt pour que je puisse vous indiquer dans quelle proportion ces ressources iront au soutien à l'OTAN. Je vais simplement vous rappeler que la politique prévoit expressément que nous allons continuer à investir dans le sens de nos relations avec nos alliés, y compris l'OTAN, le Groupe des cinq et NORAD.

Je n'ai malheureusement pas de réponse précise à vous fournir, si ce n'est de rappeler cet engagement explicite du gouvernement à poursuivre les investissements à ce chapitre. Nous aurons une meilleure idée de la nature exacte des investissements consentis aux fins de la mise en oeuvre de cette politique au cours des années à venir.

Comme Richard le soulignait précédemment, la demande excède toujours l'offre dans une telle relation d'échange avec n'importe quelle entité. Nous voulons déployer nos ressources le plus judicieusement possible de manière à optimiser nos investissements, ce qui bénéficiera à l'ensemble des Canadiens.

● (1025)

Mme Sherry Romanado: Dans les faits, un cyberopérateur doit actuellement réussir le programme de qualification militaire de base avant de suivre une formation de 16 semaines. Est-ce que nous faisons le nécessaire pour que ces programmes de formation suivent l'évolution projetée de la cyberguerre? Quelles mesures prenons-nous pour recruter les talents exceptionnels dont nous avons besoin? Nous savons qu'il s'agit d'un secteur émergent dans lequel il nous faut continuer à investir, mais que faisons-nous exactement en matière de formation et de recrutement pour nous assurer de toujours pouvoir disposer des ressources nécessaires?

C'est bien beau de pouvoir compter sur les militaires du rang, mais il nous faut également des officiers. Que faisons-nous pour en recruter dans ce domaine?

M. Len Bastien: C'est une excellente question, monsieur le président. Je vais demander au commodore Feltham d'y répondre.

Cmdre Richard Feltham: Merci, monsieur le président.

Comme je l'ai indiqué précédemment, la demande de ressources humaines dans ce secteur est extrêmement forte et très difficile à combler. Nous ne prenons pas la situation à la légère. Je vous dirais que je consacre la grande majorité de mon temps à la recherche de solutions novatrices.

À titre d'exemple, nous avons d'abord recruté des cyberopérateurs qui avaient fait leurs preuves. Nous avons ainsi muté des gens qui faisaient déjà ce travail au sein de notre centre d'opérations. Nous avons conçu des programmes de formation à l'interne. Nous avons établi des normes pour la formation de nos cyberopérateurs. Nous avons normalisé le tout en collaboration avec nos alliés de manière à permettre les échanges avec l'ensemble de nos partenaires.

Nous savons également que nous pouvons nous tourner vers le secteur civil où nous avons d'excellentes chances de pouvoir recruter de jeunes Canadiens dans les institutions postsecondaires du pays. Nous travaillons avec différents collèges afin d'accréditer leurs programmes de manière à avoir accès à des diplômés possédant toutes les compétences nécessaires pour travailler comme cyberopérateurs.

Je ne veux pas vous laisser l'impression que c'est un poste militaire que nous traitons exactement comme tous les autres, car ce n'est pas le cas. Il faut le voir d'une manière différente et miser sur une approche qui pourra être adaptée au fur et à mesure.

Je peux donc vous dire une chose aujourd'hui. J'espère que notre approche pourra effectivement s'adapter pour suivre l'évolution de la demande dans cette profession. Au cours des prochaines semaines, nous allons ainsi consacrer tout un atelier à la recherche de façons d'optimiser notre recours à la force de réserve aux fins de la cybersécurité. Nous explorons donc toutes les avenues possibles, et ce, pas seulement à l'intérieur de notre propre structure. Nous nous efforçons de solliciter les milieux industriels et universitaires à la recherche de nouvelles idées que nous pourrons mettre en application. Je ne crois pas que nous ayons toutes les réponses, mais nous collaborons avec nos alliés à l'échelle internationale comme au Canada pour pouvoir tabler sur les meilleures indications possibles dans ce contexte.

M. Len Bastien: Si vous le permettez, j'aimerais apporter un élément de réponse supplémentaire à la suite d'une question posée précédemment concernant la force de réserve et le degré d'enthousiasme que cela suscite pour nous.

Il ressort de mes interactions avec l'industrie — et nous profitons de toutes les occasions qui se présentent en la matière — qu'il est difficile pour tout le monde de recruter le personnel nécessaire aux fins de la cybersécurité. Il est possible pour les entreprises privées d'offrir une excellente rémunération à certains des spécialistes les plus talentueux. Il est toutefois très difficile pour le gouvernement d'amener ces gens-là à travailler comme fonctionnaires à temps plein ou membres des forces régulières. La possibilité de travailler à temps partiel comme cyberopérateur au sein des Forces armées canadiennes est toutefois fort intéressante, autant pour l'industrie que pour le personnel à son emploi.

Au fil de l'élaboration de ces nouveaux programmes de formation et de ces nouvelles normes de travail pour les cyberopérateurs, nous explorons différents concepts novateurs qui nous permettraient d'utiliser la force de réserve pour avoir accès aux talents disponibles dans l'industrie, ne serait-ce qu'à temps partiel.

● (1030)

Mme Sherry Romanado: Merci.

Le président: À vous la parole, monsieur Bezan.

M. James Bezan: Merci.

Ma question va un peu dans le sens de celle posée tout à l'heure par M. Fisher concernant le déploiement de l'une de nos frégates dans le cadre du groupe opérationnel naval de l'opération Reassurance de l'OTAN. Nous savons que des navires de guerre américains ont été ciblés par des cyberattaques russes. Nous avons souligné précédemment que nos troupes déployées dans le cadre de la présence avancée renforcée en Lettonie ont été victimes de tactiques de guerre hybride via la désinformation et les reportages diffamatoires de Sputnik et RT, des agences de presse contrôlées par le Kremlin.

Pouvez-vous m'expliquer la différence quant aux moyens à prendre pour assurer la cybersécurité de nos troupes déployées en Lettonie ou de notre frégate participant à l'opération Reassurance de l'OTAN par rapport à ce qui se fait dans le cadre de l'opération Unifier en Ukraine? Du point de vue de la cybersécurité, est-ce que le ministère de la Défense nationale et les Forces armées canadiennes offrent aux militaires déployés, par exemple, à Yavoriv, un soutien aussi étroit que celui fourni à ceux qui sont postés à l'extérieur de Riga via le Commandement des opérations interarmées de l'OTAN?

M. Len Bastien: C'est une autre excellente question qui nous amène à réfléchir à la forme que peut prendre le déploiement de personnel militaire dans un contexte cybernétique.

Comme Richard l'indiquait précédemment, avant de déployer nos troupes dans ces régions du monde, nous procédons à une évaluation de la menace et nous prenons les mesures nécessaires pour atténuer les risques. Dans le contexte numérique et cybernétique qui nous intéresse aujourd'hui, nous offrons à nos militaires tous les outils dont ils ont besoin pour s'acquitter de leur tâche. Nous leur fournissons des moyens d'agir de façon sécuritaire et conforme aux règles. Nous faisons de notre mieux pour qu'ils aient une longueur d'avance sur les plus mal intentionnés lorsqu'il s'agit de réaliser des choses et de profiter des faiblesses de l'autre. En outre, nous réajustons sans cesse notre approche.

D'une certaine façon, notre approche demeure la même lorsque vient le temps de déployer des spécialistes des questions cybernétiques et numériques, mais elle sera toujours adaptée en fonction de la menace que fait peser sur eux l'environnement dans lequel ils sont déployés.

J'aimerais d'ailleurs inviter le commodore Feltham, un spécialiste des opérations, à vous en dire plus long à ce sujet.

Cmdre Richard Feltham: Monsieur le président, je peux seulement répéter ce que je disais tout à l'heure. Comme le tout est fondé sur l'évaluation de la menace, je répondrais d'une façon générale à votre question en indiquant qu'il n'y a pas de différence dans la façon dont nous considérons la situation. Les ressources que nous allons déployer à l'appui d'une opération vont varier en fonction de cette évaluation de la menace. Je ne peux pas vous dire ce qu'il en est de toutes les opérations menées actuellement par les Forces armées canadiennes, mais nous procédons toujours de la même manière pour préparer nos troupes en vue d'une opération réussie. Nous analysons la menace et nous nous préparons en conséquence.

M. James Bezan: Commodore Feltham, vous êtes de la Marine. Nous allons maintenant offrir un réseau sans fil sur toutes nos frégates de telle sorte que nos marins puissent utiliser Facebook, Instagram et les programmes semblables pendant leurs temps libres. Quelle est l'incidence sur votre rôle en matière de cybersécurité? Est-ce que cette infrastructure civile rendue accessible via un actif des Forces armées canadiennes met en péril la cybersécurité d'une manière ou d'une autre?

Cmdre Richard Feltham: Vous voulez savoir si cela compromet la cybersécurité. Je porte bel et bien un uniforme de la Marine, mais je dois vous avouer qu'il y a longtemps déjà que je n'ai pas travaillé dans ce secteur. Il m'est donc impossible de vous parler en connaissance de cause de l'analyse qui a été faite par les gens de la Marine quant à la mise en oeuvre de cet outil visant à soutenir le moral des troupes.

La Marine a analysé l'incidence de ces réseaux sans fil sur la sécurité de ses plateformes parallèlement à leurs avantages pour le moral et le mieux-être des marins qui sont déployés pendant des mois et qui souhaitent pouvoir communiquer avec leur famille. Comme je ne travaille pas directement dans la Marine, je ne saurais vous dire quel genre de menace ou de cybermenace cela représente.

M. Len Bastien: Je veux seulement m'assurer que les membres du Comité comprennent bien que les réseaux sans fil mis en place par la Marine sur ces plateformes ne sont reliés d'aucune manière au réseau de la Marine elle-même. Il s'agit seulement de permettre aux marins d'avoir accès à Internet dans leurs temps libres pour les aider à mieux concilier travail et vie personnelle.

Mon organisation demeure responsable de la sécurité et de l'entretien des actifs de la Marine sur les navires en question, lesquels ne sont pas utilisés pour offrir accès à Internet aux membres de l'équipage. Il s'agit de systèmes indépendants, ce que la Marine considère comme un risque tolérable pour permettre une meilleure conciliation travail-vie personnelle. Si vous voulez en savoir plus long, il faudra que vous demandiez au commandant de la Marine à quel point il juge la situation préoccupante.

● (1035)

Le président: Messieurs, merci beaucoup de votre présence aujourd'hui. La cyberguerre et la désinformation peuvent causer des torts considérables comme nous avons pu le constater en Ukraine, en Europe et même aux États-Unis. Nous n'avons pas encore déterminé la forme que cela prendra, mais le Comité souhaite approfondir la question de la cybersécurité, et je présume que nous nous reverrons sous peu dans ce contexte.

Merci beaucoup. J'allais suspendre la séance pour vous permettre de partir, mais je vais plutôt vous demander un peu de patience, car il pourrait être difficile de ramener tout le monde. Nous devons traiter de deux motions de régie interne.

Je vais donner la parole à M. Spengemann.

M. Sven Spengemann: Merci beaucoup, monsieur le président. Je crois que tous les membres du Comité en ont reçu une copie, mais permettez-moi de vous les lire toutes les deux.

Voici la première:

> Que le Comité approuve les dépenses d'hospitalité encourues durant le voyage à Bruxelles, en Lettonie et en Ukraine du 18 au 26 septembre 2017.

Et la deuxième:

> Que le Comité approuve les dépenses d'hospitalité pour un souper dans la pièce 602 du Restaurant parlementaire le lundi 12 février 2018 en l'honneur d'Ainars Latkovskis, député et président de la Commission sur la défense, l'intérieur et la corruption, Saeima, Riga, Lettonie.

Le président: Quelqu'un veut débattre de ces motions? Il semblerait que l'on puisse les mettre aux voix les deux en même temps.

(Les motions sont adoptées)

Le président: Messieurs, je vous remercie encore une fois. Nous espérons bien vous revoir sous peu.

La séance est levée.