CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la défense nationale

NDDN • NUMÉRO 038 • 2e SESSION • 41e LÉGISLATURE

TÉMOIGNAGES

Le jeudi 20 novembre 2014

Président

L'honorable Peter Kent

Comité permanent de la défense nationale

Le jeudi 20 novembre 2014

● (1535)

[*Traduction*]

Le président (L'hon. Peter Kent (Thornhill, PCC)): Bonjour, chers collègues. Comme l'indique l'ordre du jour, nous poursuivons notre étude de la défense nord-américaine conformément au paragraphe 108(2) du Règlement.

Aujourd'hui, nous accueillons deux témoins, chacun pendant une heure. Durant la première heure, nous rencontrons Rafal Rohozinski, qui est directeur du SecDev Group, pour parler de la question de la cybersécurité. Merci beaucoup d'être là.

Monsieur Rohozinski, si vous voulez bien nous présenter votre déclaration préliminaire s'il vous plaît.

M. Rafal Rohozinski (directeur, SecDev Group): Merci beaucoup.

Merci aux membres du comité. C'est un véritable privilège d'aborder avec vous aujourd'hui la question de la cybersécurité.

En guise d'introduction, je dois vous dire que je ne suis pas seulement un directeur du SecDev Group, une entreprise canadienne qui oeuvre à l'intersection des domaines de la technologie et de la sécurité et qui a travaillé activement dans un rôle opérationnel dans le domaine cybernétique pour les gouvernements des États-Unis et du Royaume-Uni en particulier. Je suis aussi un membre principal de l'International Institute for Strategic Studies, dont le siège est à Londres, où, en collaboration avec des collègues du gouvernement, je me suis penché sur les répercussions stratégiques très complexes de la cybernétique et de ses liens avec d'autres formes d'insécurité, y compris les guerres hybrides et la criminalité transnationale.

Ce n'est peut-être pas habituel, mais je vais commencer ma déclaration en vous racontant une histoire. La semaine passée, alors que je me rendais au Moyen-Orient, j'ai été réveillé, un matin, par une application de mon iPhone. J'ai déjeuné en regardant une émission russe diffusée en continu sur mon iPad. En route vers l'aéroport, j'ai reçu un appel important et j'ai utilisé une application de communication vocale chiffrée, appelée Silent Circle, afin de discuter en toute sécurité avec mes collègues du Moyen-Orient. Tandis que j'approchais de l'aéroport, ma carte d'embarquement électronique s'est activée automatiquement dans une autre application afin que je puisse rapidement réaliser les procédures de sécurité.

Savez-vous ce que cette histoire a de spécial? Peut-être rien, parce que tout ce que je viens de décrire, eh bien, un d'entre vous ou vous tous en faites l'expérience au quotidien. Ce qui est inhabituel, c'est qu'aucune de ces technologies n'existait il y a cinq ans. C'est là où je voulais en venir. La vitesse à laquelle et la mesure dans laquelle le monde numérique a colonisé notre monde physique sont renversantes. Il y a 25 ans, il y avait peut-être 14 000 personnes connectées à Internet. Aujourd'hui, plus du tiers de l'humanité a un accès Internet à large bande, et il y a plus de téléphones cellulaires sur la planète qu'il n'y a d'êtres humains. Cela a un impact important et profond sur toutes nos sociétés.

Notre dépendance aux technologies et aux réseaux numériques s'est accrue plus rapidement que notre capacité de concevoir des règles et des règlements ou d'adapter les lois et pratiques actuelles à ce nouvel environnement. Nous vivons dans une nouvelle ère, ce que nous appelons chez SecDev une ère d'autonomisation ouverte, dans laquelle la capacité d'agir des gens s'est accrue plus rapidement que la capacité des institutions à s'adapter. L'aspect positif de cette autonomisation, c'est que la connaissance humaine n'a peut-être jamais fait un aussi grand bond en avant. Plus de personnes peuvent prendre des décisions en ayant accès à des renseignements et à des connaissances qu'à tout autre moment de l'histoire de l'humanité.

Cependant, cette importante autonomisation s'accompagne de grands risques, et ces risques ne se limitent pas simplement aux risques implicites de défectuosités techniques ou aux manipulations malfaisantes de l'information dans les systèmes d'information dont nous dépendons, qui font souvent les manchettes lorsqu'on apprend qu'il y a eu d'importantes violations de la vie privée ou pertes de données, d'importants vols de données ou d'autres cas de compromission de renseignements critiques et de systèmes de communication.

Alors que notre quotidien est de plus en plus médiatisé ou facilité par la cybernétique, on constate qu'il y a aussi d'importants risques implicites liés à la réécriture tacite du contrat social entre les particuliers et les États. Les risques implicites liés à ces défis normatifs sont peut-être aussi complexes, sinon plus, que le défi technique d'avoir à gérer les vulnérabilités et les insécurités de notre infrastructure numérique essentielle.

Pour illustrer ce point, prenons l'exemple, actuellement, des travailleurs canadiens qui travaillent pour des institutions ayant pignon sur rue, comme des usines de voitures ou d'autres types d'usines, et qui peuvent, en toute légalité, s'adonner à des actions syndicales, comme du piquetage dans leur milieu de travail. En d'autres mots, ils peuvent interdire l'accès à leur lieu de travail à de nouveaux travailleurs non syndiqués ou aux clients. Mais que se passe-t-il si l'employeur n'a pas pignon sur rue et qu'il s'agit plutôt d'une entreprise virtuelle, peut-être un site Web plutôt qu'un magasin traditionnel? Si les travailleurs dans cet environnement décident d'interdire l'accès à leur milieu de travail dans le cyberespace, disons, grâce à une attaque de déni de service, on considère alors qu'ils ont commis un acte criminel.

Je n'essaie pas de dire qu'une attaque informatique de déni de service équivaut à un piquet de grève. Je veux simplement souligner que nous avons des droits et qu'il y a certaines normes pour lesquels nous nous sommes battus pendant des décennies dans le monde physique qui n'ont pas d'équivalent naturel ou significatif dans le monde numérique.

La cybercriminalité pose elle aussi certains défis à la lumière de notre cadre normatif actuel. La criminalité dans le cyberespace, qu'elle vise des particuliers ou des États, tire profit de la nature internationale de l'environnement cybernétique pour compliquer le travail des organismes d'application de la loi, qui doivent chacun enquêter sur ces dossiers sur leur territoire. Pour parler franchement, les cybercriminels peuvent utiliser l'absence d'une convention mondiale sur la cybercriminalité et l'absence d'ententes entre les organismes d'application de la loi pour s'adonner efficacement à des activités qui échappent aux cadres d'application de la loi nationaux. La meilleure façon d'expliquer cette situation est peut-être d'utiliser une analogie.

À l'époque de la prohibition aux États-Unis, la plupart des services de police étaient des organisations locales. Les trafiquants d'alcool et les contrebandiers profitaient de l'absence d'une législation ou d'une convention unifiée à l'échelle des États ou à l'échelle du pays pour contourner la compétence des autorités d'application de la loi locales. Cela a mené à la création d'un service de police national aux États-Unis. Cependant, malheureusement, pour faire la même chose afin de lutter contre la cybercriminalité, il faudrait conclure un accord mondial, ce qui est très peu probable actuellement.

Le cyberenvironnement a aussi un impact important sur la sécurité nationale du Canada, et ce, pour d'autres raisons encore. Si notre pays s'est bâti le long des chemins de fer, l'économie canadienne actuelle passe maintenant par la fibre optique du Web. Pour le dire simplement, le Canada est le premier pays du cyberespace en raison de sa géographie. Le commerce, la gouvernance et le quotidien sont tous dépendants des télécommunications et d'Internet. À cet égard, le cyberespace est une ressource stratégique nationale, dont la perturbation ou la vulnérabilité à une telle perturbation constituent des risques importants pour la sécurité nationale, des risques bien plus grands que les autres menaces physiques à l'intégrité économique et territoriale du pays.

J'ajouterai que les risques et les menaces ne pèsent pas uniquement sur le cyberespace, mais sur tout ce qu'il permet, y compris les infrastructures essentielles et l'accès important aux connaissances, y compris dans les domaines scientifiques de la génétique et de la biologie, entre autres, qui, en tant que tels, constituent des risques uniques et importants dans nos sociétés de plus en plus complexes et de plus en plus dépendantes des technologies.

La défense du cyberespace n'est pas une tâche facile. D'abord et avant tout, il s'agit d'un environnement synthétique qui a été conçu pour être résilient, et non pour être sécuritaire. Contrairement à la terre, à l'air, à la mer ou à l'espace, le cyberespace doit faire l'objet d'une attention constante et continue aux niveaux des technologies, du codage et de la réglementation pour se maintenir. Les modifications apportées à n'importe lequel de ces trois aspects peuvent provoquer d'importants changements dans l'environnement synthétique, ce qui peut avoir un effet en cascade sur le commerce, la gouvernance et la vie quotidienne.

On dit parfois que le cyberespace n'a aucun centre, mais je ne suis pas d'accord. Le cyberespace se manifeste dans le monde physique, dans les commutateurs, les routeurs et les câbles utilisés par l'industrie des télécommunications. Ironiquement, les télécommunications restent parmi les industries les plus réglementées au Canada et au sein des pays du G7, et malgré tout, on n'a pas fait grand-chose pour tirer parti des dispositions de la Loi sur les télécommunications pour obliger les exploitants de ces infrastructures à prendre des mesures pour atténuer les vulnérabilités dans ce domaine ou les convaincre de le faire.

Pour le dire tout simplement, bon nombre des vulnérabilités critiques implicites du cyberespace canadien pourraient et devraient être atténuées par les exploitants des infrastructures, qui peuvent plus facilement repérer les tendances en matière de malfaisance et les éléments qui rendent la malfaisance possible et trouver des solutions à grande échelle. Après, une meilleure coordination et une meilleure coopération entre les organismes gouvernementaux et le secteur privé contribueraient énormément à accroître la résilience du cyberespace canadien et la confiance des gens et à réduire au minimum le potentiel d'événements catastrophiques ou associés à la théorie du cygne noir.

Je vais maintenant parler brièvement des aspects militaires du cyberespace et de leur importance relativement à la cybersécurité. La très grande dépendance des sociétés très industrialisées à l'égard de la cyberinfrastructure, y compris la façon dont nous avons choisi de structurer les institutions responsables de la défense nationale et de réaliser des gains en efficacité à cet égard, signifie que le cyberespace est devenu une zone active d'expérimentation et de renforcement des capacités, offensives et défensives. Que l'on veuille ou non que le cyberespace devienne un domaine d'activité militaire, la réalité, c'est que ce sera le cas, parce qu'il offre aux personnes et aux entités malveillantes — qu'il s'agisse d'États, d'organisations criminelles transnationales, d'organisations terroristes ou de personnes détenant une superpuissance — la capacité de causer et de générer des effets prolongés. En effet, le cyberespace leur permet de sauter des générations de guerre industrielle et de se mesurer à n'importe quel acteur sur la scène mondiale pour ce qui est de recourir à la force à des fins politiques.

Le milieu militaire moderne s'appuie sur les technologies. Il y a quelques années, j'ai eu l'occasion d'offrir un atelier à l'intention de membres principaux au Center for Strategic Leadership du Army War College américain. Une des questions qu'on a posées à ce groupe de personnes triées sur le volet dans les milieux de la défense et du renseignement était de savoir si nous pourrions refaire, aujourd'hui, l'invasion de la Normandie, compte tenu de la structure actuelle des forces. Eh bien non, parce que nous avons éliminé des niveaux entiers de postes et de fonctions qui ont maintenant été remplacés par des processus technologiques. En fait, nous n'avons plus suffisamment de personnes formées pour tout faire manuellement.

● (1540)

Si c'est déjà le cas aujourd'hui, dans l'environnement opérationnel futur, si l'on tient compte de l'utilisation accrue des technologies automatisées, les risques et les vulnérabilités implicites de l'environnement technologique ne feront que croître.

Ce qui est peut-être aussi digne de mention au sujet de la dimension militaire du cyberespace, c'est qu'on peut générer des effets sans avoir accès aux ressources dont disposent seulement les États. Des groupes aussi disparates que des gangs de narcotrafiquants d'Amérique latine et le soi-disant État islamique peuvent générer des répercussions importantes dans le cyberespace et par lui en vue d'atteindre leurs objectifs politiques. Permettez-moi de vous donner un exemple. L'année dernière, c'est non pas l'État islamique, mais un groupe associé au gouvernement syrien qui a réussi à pirater le compte Twitter de l'AP pour y afficher un faux message selon lequel la Maison-Blanche était attaquée et que le président Obama avait été blessé, ce qui a causé une chute de 150 points, ou 1,36 milliard de dollars, dans les marchés boursiers en trois minutes. Il s'agit d'un impact à court terme, mais il s'agit tout de même d'un impact lié à une information stratégique, et je crois qu'il s'agit là d'un avant-goût de ce qui nous attend.

Selon moi, ce qu'il faut tirer de cette analyse plus générale et plus complexe, c'est que les activités dans le cyberespace, comme le conçoivent bon nombre de nos États alliés et les acteurs non étatiques, ne se limitent pas à des activités par le truchement des domaines de réseau, mais procèdent du principe selon lequel on peut profiter du domaine de l'information pour générer des effets. Cette notion est importante compte tenu du fait que, de façon générale, notre tendance dans le monde occidental — et j'inclus là-dedans les Forces canadiennes — a été de voir les opérations liées à l'information et les opérations liées au réseau informatique comme deux choses distinctes. Selon moi, c'est une erreur.

En conclusion, j'aimerais faire remarquer que, malgré les vulnérabilités et l'insécurité associées à cette infrastructure qui s'est immiscée de façon aussi profonde et généralisée dans nos vies quotidiennes, la gouvernance et le commerce, le cyberespace est bénéfique pour les sociétés ouvertes. Par conséquent, il est bénéfique pour la sécurité nationale d'en maintenir l'ouverture. Nous n'assurerons pas une meilleure sécurité en construisant des frontières numériques, des barrières ou des enclaves. Il faut plutôt adopter une approche plus intelligente et fondée sur le renseignement pour comprendre la nature des risques, des menaces et des occasions qui émanent du cyberespace et qui passent par lui et élaborer des capacités et des mécanismes à l'intérieur et à l'extérieur du secteur public pour garantir la résilience et la capacité de prendre des mesures décisives dans ce domaine et en nous en servant, pour défendre nos intérêts nationaux.

Merci de votre attention. Je suis prêt à répondre à vos questions.

● (1545)

Le président: Merci beaucoup, monsieur Rohozinski.

Nous allons commencer la première série de questions. Vous avez sept minutes chacun.

Monsieur Norlock, allez-y, s'il vous plaît.

M. Rick Norlock (Northumberland—Quinte West, PCC): Merci beaucoup, monsieur le président.

Merci à notre témoin d'être là aujourd'hui.

Pour commencer, j'aimerais vous faire part de mon expérience relativement à ces belles choses qu'on appelle des ordinateurs, des logiciels malveillants et de toutes ces autres choses qu'on achète. On paie 150 $ pour un logiciel antivirus et on l'installe. Et si on ne le met pas à jour chaque semaine, quelqu'un trouve une façon de le contourner. Je retire de votre témoignage que, peu importe ce que nous faisons aujourd'hui, dans peut-être 10 jours, quelqu'un aura trouvé une façon de le court-circuiter ou de contourner le genre de barrière que vous aurez érigée pour vous protéger. J'aimerais que vous nous parliez de cette situation et que vous le fassiez en répondant aux questions suivantes.

Au Canada, bien sûr, nous comptons sur Sécurité publique, qui est notre organisme responsable de la cybersécurité. J'aimerais savoir dans quelle mesure vous croyez qu'il est approprié de comparer notre cadre de cybersécurité avec celui, disons, des États-Unis, qui ont récemment mis sur pied leur Cyber Command ou USCYBERCOM en tant que centre de commandement de leurs opérations cybernétiques. J'aimerais bien que vous nous parliez de ces choses.

M. Rafal Rohozinski: Bien sûr. Merci beaucoup pour ces questions.

En ce qui concerne votre première question, oui, je crois qu'il faut reconnaître qu'un des prix à payer pour l'ouverture, c'est le fait que l'environnement lui-même représentera toujours un certain niveau d'insécurité. C'est tout à fait vrai. Le problème, cependant, c'est que, de par leur nature, les menaces liées au code malveillant peuvent être réunies et constatées à plus grande échelle. En d'autres mots, ce qui nuit à votre ordinateur et qui est difficile à déceler est en fait beaucoup plus facile à détecter par quelqu'un qui vous fournit vos services et qui peut voir que la même chose se produit à de multiples reprises en même temps.

On en revient au commentaire que j'ai formulé dans mon témoignage selon lequel nous n'avons pas vraiment trouvé où se trouve un tel point focal, le point où l'on peut voir les risques et les menaces qui pèsent sur les personnes. Au Canada, 95 % de ce que nous appelons le cyberespace est en fait exploité par une seule entité, Bell Canada. L'entreprise le fait par une diversité de mécanismes, mais il reste qu'il y a là une importante concentration. Il y a des règlements sur les télécommunications actuellement qui exigent des exploitants qu'ils travaillent de certaines façons... l'échange d'information, etc. La sécurité n'est pas l'une de ces choses. En d'autres mots, nous n'avons pas utilisé le mécanisme le plus utile auquel nous avons déjà accès afin de pouvoir régler ce qu'on pourrait appeler le « problème des 95 % », le problème d'un écosystème sale qui est actuellement pollué par des cybercriminels opportunistes qui nous obligent à payer 150 $ chacun pour essayer de nous défendre, un ordinateur à la fois.

En guise de contexte, SecDev a participé à une étude en collaboration avec Bell Canada pour essayer d'évaluer l'ampleur de ce qu'on pourrait appeler les comportements malfaisants en ligne. L'étude a été réalisée il y a deux ou trois ans déjà. Nous avons constaté que, à tout moment, de 5 à 12 % de tous les appareils connectés à Internet appartenaient à un réseau de zombies. En d'autres mots, ils étaient sous le contrôle d'une forme ou d'une autre de logiciel malfaisant, ce qui n'était pas voulu par l'exploitant du système lui-même. C'est un problème assez important. Le fait que nous n'avons pas créé de réglementation ou de mesures incitatives pour pousser l'industrie des télécommunications à fournir cette première ligne de défense est, je crois, l'un de nos principaux échecs en matière de cybersécurité.

Pour ce qui est de la question — si j'ai bien compris — de savoir qui devrait être responsable du portefeuille de la cybersécurité, si je regarde ce que font nos collègues du Groupe des cinq, il s'est passé une chose qui ne s'est pas produite au Canada. Au Canada, la question de la cybersécurité n'est pas encore considérée comme une priorité en matière de sécurité nationale. En d'autres mots, ce n'est pas considéré comme un thème qu'il faut aborder de façon interinstitutionnelle ou intergouvernementale, comme ils l'appellent aux États-Unis. Aux États-Unis, il y a une entité-cadre qui assure la coordination des activités de cybersécurité à l'échelle du gouvernement. Dans un même ordre d'idées, au Royaume-Uni, les mécanismes qui constituent la version de Sécurité publique, sa version du CST, et l'industrie sont beaucoup plus forts et beaucoup plus développés qu'ils ne le sont ici en ce moment.

Je crois, pour répondre à votre question directement, qu'il faut que Sécurité publique Canada prenne les devants en matière de coordination de la cybersécurité telle qu'elle s'applique à tous les aspects de la sécurité publique et la sécurité, ce qui signifie assurer l'interface entre les secteurs public et privé. Il faut aussi une institution pour fournir ces capacités du côté militaire, ce qui, si je ne m'abuse, n'existe pas actuellement.

● (1550)

M. Rick Norlock: Dans la même veine, le réseau du ministère de la Défense nationale est adéquat, mais dans quelle mesure les capacités utilisées par le Centre de la sécurité des télécommunications ou le CSTC sont-elles suffisantes pour assurer la protection des renseignements électroniques et des structures d'information du gouvernement du Canada? Vous les avez séparées en deux entités, les secteurs public et privé et le milieu militaire, et vous dites maintenant que c'est nécessaire. Si je comprends bien, cela signifie qu'il devrait y avoir deux entités au sein du gouvernement, l'une qui s'occupe de l'aspect militaire et l'autre, des secteurs public et privé. Pourrions-nous plutôt les réunir sous un même toit?

M. Rafal Rohozinski: Je ne peux pas vous parler des capacités du CSTC, puisque je ne le représente pas. Je n'en suis pas un des employés et je n'ai pas eu le privilège d'y avoir accès à ce titre. Cependant, d'un point de vue institutionnel, je crois qu'il est évident que le CSTC assume un rôle principal en matière de cybersécurité au Canada parce que, très franchement, c'est là où le gouvernement a réuni l'expertise et le savoir-faire nécessaire. Quant à savoir s'il doit continuer d'être le centre de ces opérations, c'est une très bonne question.

Encore une fois, selon moi, le passé est garant de l'avenir. À une époque, le contrôle aérien relevait du département de la Défense américain. Actuellement, c'est une agence civile qui en est responsable. Je crois qu'il y a actuellement des capacités au sein du CSTC qui devront être transférées dans les services d'application de la loi et d'autres ministères du gouvernement qui ont une responsabilité relativement à certains aspects de la cybersécurité dans des domaines sectoriels très précis. De façon générale, cependant, j'estime que, du point de vue institutionnel, il doit y avoir une compréhension, et je dirais une reconnaissance du fait que le cyberespace doit être aussi important que l'intégrité du territoire et la sécurité économique et énergétique. Nous devrions y accorder autant d'importance, c'est-à-dire assurer un genre de coordination intergouvernementale et interagences qui nous permettrait de compter sur des politiques coordonnées.

Le président: Votre temps est écoulé. Merci beaucoup, monsieur Rohozinski.

Monsieur Chisholm, s'il vous plaît.

● (1555)

M. Robert Chisholm (Dartmouth—Cole Harbour, NPD): Merci beaucoup, monsieur le président. Si j'arrive à faire vite, je vais partager une partie de mon temps avec M. Brahmi.

J'ai trouvé votre exposé et votre mémoire très intéressants. J'aimerais revenir sur la question de la coordination et de la coopération dont M. Norlock vient de parler, mais voici comment je veux le faire. En juillet, le Conseil national de recherches a été victime d'une cyberattaque majeure, y compris l'infiltration de systèmes contenant des renseignements personnels. La réaction du gouvernement a été de blâmer la Chine.

J'ai deux questions pour vous. Pouvez-vous nous donner une idée de la mesure dans laquelle les infrastructures essentielles du Canada sont protégées contre des cyberattaques d'entités parrainées par des États? Et pourrions-nous faire mieux sur le plan de la coordination et de la coopération?

M. Rafal Rohozinski: Pour ce qui est de la vulnérabilité, selon moi, nos systèmes sont bel et bien vulnérables. Ils le sont pour deux raisons: parce que la sécurité n'a jamais été la priorité au moment de la conception de ces systèmes et parce que nous n'avons pas mis en place le genre d'exigences réglementaires nécessaires pour s'assurer que les exploitants des infrastructures essentielles font de la sécurité non seulement une responsabilité qu'ils ont, en tant qu'entreprise, à l'égard de leurs actionnaires, mais aussi une responsabilité à l'égard du Canada et, franchement, de la sécurité nationale. Selon moi, c'est là notre principal échec.

M. Robert Chisholm: En ce qui concerne la coordination des organismes du secteur public qui enquêtent sur nos vulnérabilités, en faisons-nous assez?

M. Rafal Rohozinski: Encore là, je crois qu'une partie du problème, c'est que, actuellement, la majorité des capacités que possède le gouvernement pour s'acquitter du travail d'attribution est concentrée dans une institution qui n'a jamais été conçue à cette fin — le CST — et c'est pourquoi j'ai dit plus tôt que, selon moi, il faudra réaffecter en partie les capacités qui, pour toutes les bonnes raisons, sont actuellement centralisées dans le CST. Il faut soit les transférer dans d'autres ministères du gouvernement, soit envisager la création d'une institution civile, non militaire et non liée au renseignement qui s'occuperait de tout ce qui touche la coordination de la cybersécurité.

Je souligne à nouveau que nous avons beaucoup à perdre ici. Nous ne sommes pas l'Estonie, qui se traverse en six heures, ni Israël. Le Canada est un pays qui se traverse en six ou sept heures d'avion. Le coup essuyé par la perte d'une infrastructure essentielle serait beaucoup plus catastrophique, et c'est pourquoi il faut vraiment mettre un accent stratégique sur ce dossier.

M. Robert Chisholm: D'après ce que j'en sais, les autres pays des Five Eyes n'ont pas opté pour une agence civile. Il s'agit habituellement d'une activité associée au renseignement.

M. Rafal Rohozinski: Oui et non. Je crois qu'il faut faire une distinction entre deux choses.

Oui, il y a eu, et pas seulement parmi les Five Eyes, mais, si je ne m'abuse, à l'échelle... Nous avons réalisé une étude sur l'équilibre stratégique pour l'IIES; environ 90 pays commencent à mettre sur pied l'équivalent d'un commandement cybernétique, c'est-à-dire une organisation militaire qui s'occupe directement du cyberespace, qui en fait son domaine d'opérations et qui forme du personnel, l'outille et élabore une doctrine touchant la réalisation d'opérations cybernétiques. C'est ce que font les autres pays des Five Eyes, en tout cas.

Cependant, au Royaume-Uni et aux États-Unis, on constate aussi une coordination entre les agences civiles, comme la Homeland Security et le Critical Infrastructure Protection Office au Royaume-Uni, qui ont repris des capacités du GCHQ et de la NSA pour les transférer dans des agences civiles responsables de l'infrastructure essentielle, du secteur financier, du secteur de l'énergie, etc.

M. Robert Chisholm: D'accord.

Merci beaucoup.

Le président: Il vous reste trois minutes, monsieur Brahmi.

[*Français*]

M. Tarik Brahmi (Saint-Jean, NPD): J'aimerais poser une question qui inquiète beaucoup les citoyens de Saint-Jean-sur-Richelieu, où il y a eu une attaque menée par ce qu'on appelle un loup solitaire.

J'aimerais que vous nous parliez de la cybercriminalité ou du cyberterrorisme sous l'angle des loups solitaires. Si on n'est pas capable de lier un incident particulier à une organisation terroriste, comment peut-on intervenir?

Existe-t-il des critères permettant de définir qu'un acte est assimilable à du terrorisme parce qu'il a été inspiré par des informations prises sur Internet? Si de tels critères n'existent pas, comment peut-on protéger le cyberespace pour éviter que des personnes ayant des problèmes de santé mentale posent un acte terroriste après avoir eu accès à des informations provenant d'organisations terroristes? Ces personnes peuvent n'avoir aucun lien avec une organisation terroriste ni en connaître, mais elles vont interpréter certains messages dans le cyberespace comme une incitation à poser un acte terroriste.

● (1600)

[*Traduction*]

M. Rafal Rohozinski: Excellente question, et avant de répondre, je dois dire que je témoigne lundi devant un comité sénatorial pour parler de la question du cyberterrorisme. Nous avons travaillé en partenariat avec Sécurité publique Canada dans le cadre du programme Kanishka, qui portait précisément sur les médias sociaux, Internet et la radicalisation, et les mesures que l'on peut prendre, tant dans le secteur public qu'au niveau communautaire, afin de pouvoir identifier les personnes à risque de radicalisation et réaliser une intervention précoce.

La réponse longue, je dirais, c'est que je crois que vos observations sont tout à fait justes. Plus Internet ou plus la population sur Internet reflétera la société en général, plus on y retrouvera le bon, la brute et le truand: des personnes susceptibles d'être mobilisées et les autres. Cela a très certainement été exploité par des groupes comme Daesh, l'État islamique.

Je dirais que la principale différence, entre Al-Qaïda et l'État islamique, c'est qu'Al-Qaïda était une conspiration. Les personnes finissaient toujours par être approuvées par quelqu'un d'autre qui connaissait telle autre personne. Il y avait un contact physique. Dans le cas de Daesh, le soi-disant État islamique, c'est davantage comme une marque. Le groupe transmet un message idéaliste, et ceux qui sont intéressés choisissent d'agir de leur propre chef. C'est terriblement difficile à détecter parce que, même si la technologie nous permet, à un certain niveau, d'identifier les personnes qui ont accès au contenu pouvant provoquer une radicalisation, le fait de mettre cette technologie à la disposition des organismes d'application de la loi sans motif signifie que, au bout du compte, nous créons un système de surveillance dont les conséquences négatives l'emporteraient sur les avantages liés à l'identification des personnes à risque.

Cependant...

Le président: Votre temps est écoulé, monsieur Brahmi. Nous pouvons poursuivre sur cette lancée avec le prochain intervenant.

Monsieur Daniel, s'il vous plaît.

M. Joe Daniel (Don Valley-Est, PCC): Merci, monsieur le président, et merci, monsieur Rohozinski, d'être là.

Vous avez parlé de plusieurs choses. C'est intéressant de constater qu'il y a autant d'enjeux liés aux cyberattaques, etc. Mais parlons des aspects les plus fondamentaux du dossier, les protocoles Internet. Pouvez-vous nous expliquer qui les rédige, de quelle façon on les applique, et ainsi de suite? Il s'agit des éléments fondamentaux de la communication sur les cyberréseaux, et je ne crois pas que quiconque en ait vraiment tenu compte lorsqu'on envisageait l'utilisation plus répandue d'Internet comme c'est devenu le cas. Comme vous le savez, il y a très longtemps, le protocole a été créé pour assurer la communication entre des universités, alors pouvez-vous simplement nous aider à comprendre les notions de base? Pouvez-vous aussi nous parler de l'aspect matériel si vous en avez l'occasion?

M. Rafal Rohozinski: Bien sûr. Je vais vous donner la réponse courte.

Effectivement, les normes qui définissent actuellement l'interopérabilité entre le matériel qui utilise le protocole Internet viennent d'une structure de gouvernance qui a initialement été mise en place en 1995, au moment de la mondialisation d'Internet. On avait entre autres créé une entité, l'ICANN, qui réglementait l'octroi des adresses, mais il y avait aussi des sous-comités responsables de la sécurité, et, par exemple, des aspects techniques du cyberespace lui-même.

Au départ, durant les 15 premières années d'Internet, si vous voulez, de 2000 au milieu des années 2000, une bonne partie du travail était fait par des ingénieurs, des chercheurs, qui avaient peut-être travaillé pour des sociétés, mais qui, en fait, tentaient de rédiger des protocoles visant à faciliter la communication entre différents appareils. Au cours des dernières années, des pays comme la Chine, la Russie et d'autres ont commencé à envisager le cyberespace d'un point de vue plus stratégique. Il y a eu plus d'interventions par des sociétés ainsi que des groupes d'ingénieurs parrainés par le gouvernement afin d'établir des normes qui leur sont favorables.

Comme je l'ai dit, il est important, puisque le cyberespace est un lieu très synthétique, de comprendre de quelle façon l'introduction de normes peut modifier le domaine de sorte qu'il corresponde ou qu'il ne corresponde pas à nos normes et nos valeurs. Cet aspect devrait vraiment faire partie des choses sur lesquelles se penche une institution de cybersécurité qui serait créée au niveau gouvernemental.

● (1605)

M. Joe Daniel: Votre organisation participe-t-elle à ce genre de travail, qui vise à s'assurer que les protocoles sont sécuritaires et qu'Internet devient plus sécuritaire?

M. Rafal Rohozinski: Il est évident que l'un des critères que nous avons élaborés lorsque nous travaillions avec d'autres États qui voulaient créer des stratégies nationales de cybersécurité, c'était le besoin de comprendre le rôle des normes et de participer à des organismes de normalisation afin de s'assurer que les aspects techniques du cyberespace ne vont pas à l'encontre ni des intérêts nationaux, ni de l'intérêt commun.

M. Joe Daniel: Vous avez dit qu'environ 15 % des ordinateurs sont contrôlés à distance par certaines de ces applications, etc. Y a-t-il une collusion entre les fabricants de matériel et les gens d'Internet pour que ce soit possible? Y a-t-il des gens qui travaillent dans l'ombre à cette fin? On sait bien que le chiffrement n'a pas tenu le coup. Même le chiffrement à 256 bits pour les communications a été contourné en quelques heures.

M. Rafal Rohozinski: Je crois que le problème est davantage l'écosystème lui-même.

Si l'on prend le temps d'y réfléchir, les lois sur la protection des consommateurs qui existent pour la construction d'un appareil — par exemple un véhicule — exigent des fabricants qu'ils fassent de la sûreté et de la sécurité les aspects fondamentaux de la conception de leurs produits, que ce soit des ceintures de sécurité, des coussins gonflables ou je ne sais quoi d'autre.

Ce n'est pas le cas lorsqu'on achète un logiciel. Il a été conçu pour assurer son interopérabilité et non sa sécurité. Je crois que c'est la conséquence du fait qu'il y a eu, si l'ont veut, une importante ruée vers l'or pour construire un domaine mondial au cours des 15 dernières années, et que la sécurité a vraiment été reléguée au second plan. Je crois que les choses vont changer, mais ce n'est certainement pas le cas actuellement.

M. Joe Daniel: Le gouvernement devrait-il établir des normes pour ces genres de problèmes afin de rendre le cyberespace plus sécuritaire?

M. Rafal Rohozinski: Je crois que c'est très certainement l'une des questions qu'il faudra se poser. Je dirais que le besoin de s'occuper des aspects fondamentaux de l'insécurité et de la vulnérabilité des réseaux au point de concentration le plus élevé, qui est au niveau de l'exploitation des réseaux eux-mêmes, est probablement plus important qu'au niveau des consommateurs, pour le moment, en ce qui concerne l'impact que cela pourrait avoir.

M. Joe Daniel: La fusion de l'industrie de la défense et d'Internet, qui semble très utile à de nombreux égards, s'est produite un peu sans supervision. Qu'en pensez-vous?

M. Rafal Rohozinski: Je ne suis pas sûr de comprendre la question. Pouvez-vous la poser différemment?

M. Joe Daniel: L'industrie de la défense a adopté Internet comme moyen de communication, mais on dirait bien que ça s'est fait sans que personne ne réfléchisse vraiment à la sécurité.

Ma question complémentaire est la suivante: le gouvernement devrait-il créer un ministère de la sécurité responsable de contrôler ce qui se passe sur Internet et d'y appliquer la loi?

M. Rafal Rohozinski: Je vais peut-être répondre de façon différente.

Si nous examinons le modèle qui a été adopté en matière de sécurité aux États-Unis et qui prend forme actuellement, nous constatons qu'il s'agit certainement d'une approche sectorielle qui concerne la mesure dans laquelle la sécurité doit être assurée pour veiller à la survie ou répondre aux besoins du secteur lui-même. Le secteur financier, par exemple, possède ses propres mécanismes de communication de l'information et pour assurer la sécurité entre les institutions les plus vulnérables et, en fait, il joue un rôle essentiel au sein de l'économie américaine.

Des initiatives semblables ont été réalisées au sein de l'industrie de la défense aux États-Unis, où la NSA partage des signatures classifiées qui donnent à l'industrie de la défense de meilleures chances d'atténuer les vulnérabilités dans le domaine cybernétique que d'autres secteurs.

De ce point de vue, oui, je crois qu'il faut adopter une approche plus sectorielle en matière de cybersécurité, et reconnaître qu'il y a différentes priorités en ce qui concerne la façon dont il faut procéder.

M. Joe Daniel: J'ai une dernière question qui est un peu reliée à tout ça.

Devrait-on mettre sur pied un système Internet parallèle qui est protégé et qui n'utilise pas les protocoles qui ne sont pas sécurisés, afin de pouvoir compter sur un réseau très sécurisé pour les infrastructures essentielles et l'industrie de la défense?

M. Rafal Rohozinski: Je dirais que tous les réseaux qui sont conçus de façon à être interopérables sont toujours vulnérables. Qu'ils soient conçus de façon isolée ou non, au bout du compte, ils afficheront la même vulnérabilité de base. Je crois que le ver Stuxnet l'a assez bien prouvé en Iran, où un système complètement isolé a tout de même été compromis par un vecteur.

Pour moi, et j'aborde cette question du point de vue de la sécurité, il faut changer les mentalités au sujet de la sécurité. Il ne faut pas imaginer une ligne Maginot et se demander comment écarter toute menace. La question consiste plutôt à savoir de quelle façon on peut détecter les menaces que nous connaissons et dont nous soupçonnons l'existence sur votre réseau, et ensuite à les définir et à les manipuler afin d'en réduire au minimum l'efficacité.

● (1610)

Le président: Votre temps est écoulé.

Madame Murray, allez-y, s'il vous plaît.

Mme Joyce Murray (Vancouver Quadra, Lib.): Merci pour votre exposé et votre analyse, qui sont fascinants.

J'aimerais revenir sur la question de M. Daniel au sujet de la stratégie de cybersécurité. Vous avez dit que nos autres partenaires des Five Eyes ont adopté une approche plus coordonnée en matière de cybersécurité. Est-ce grâce à une stratégie nationale de cybersécurité? Est-ce que le Canada devrait envisager de se doter d'une telle stratégie?

M. Rafal Rohozinski: La réponse est oui, et je crois que c'est vraiment quelque chose sur quoi le Canada devrait travailler.

Le problème en ce qui concerne la cybersécurité, c'est que ce n'est pas aussi facile à comprendre que les soins de santé, le chômage ou d'autres enjeux sur lesquels l'électeur moyen a une opinion ou non. La cybersécurité a tendance à être un sujet beaucoup plus abstrait, ce qui signifie qu'il faut vraiment qu'il se passe un événement majeur pour qu'elle se retrouve à l'ordre du jour national, qu'on y accorde des ressources adéquates et qu'on assure le niveau de coordination nécessaire. On parle de créer une nouvelle institution.

Mais, encore une fois, lorsqu'on se rend compte de l'importance du cyberespace pour la gouvernance, le commerce et notre sécurité nationale, je crois que nous jouons avec le feu en omettant de le faire.

Mme Joyce Murray: Selon vous, faudrait-il une stratégie nationale de cybersécurité assortie de certains aspects sectoriels ou une stratégie de cybersécurité liée au milieu militaire et à la défense et une autre pour le commerce et le monde civil?

M. Rafal Rohozinski: C'est une bonne question, et voici ce que j'en pense. Il faut y aller petit à petit.

Selon moi, pour comprendre le rôle de la cybernétique dans le milieu militaire, il faut se doter d'une doctrine sur les opérations cybernétiques qui sera conforme à la posture de défense actuelle. Cependant, puisque le cyberespace recoupe des enjeux liés à l'application de la loi, à la défense et même des enjeux nationaux — par exemple, pour contrer la radicalisation ou lutter contre la criminalité — il faut presque obligatoirement une analyse plus générale.

Je suis presque un peu surpris que nous n'ayons pas encore eu de commission royale sur le cyberespace qui se serait penchée sur la façon dont il a un impact sur tous les aspects de la gouvernance au Canada, parce que, d'une certaine façon, c'est un point de départ presque naturel avant que nous puissions commencer à définir précisément quel serait l'impact sur des domaines comme la défense nationale.

Cependant, si on ne le fait pas, je crois qu'il serait plus prudent de commencer par une approche sectorielle.

Mme Joyce Murray: Vous avez dit qu'aucune des technologies dont vous avez parlé n'existait il y a cinq ans. Les technologies s'imposent plus rapidement que nous ne pouvons créer des lois pour les encadrer. Nous savons que la loi qui a créé le cadre juridique du CST a été rédigée en 2001, et on n'y a même pas changé un point ou une virgule depuis.

J'aimerais savoir si, selon vous, la mise à jour des lois régissant le CSTC ferait partie intégrante d'une bonne stratégie de sécurité.

M. Rafal Rohozinski: Encore une fois, je crois que la réponse est oui. Au bout du compte, le CSTC est — et c'est bien ainsi — l'institution où nous avons réuni les capacités et les connaissances liées au domaine cybernétique au sein du gouvernement. Cependant, le CSTC est limité de certaines façons et n'est peut-être pas l'institution la plus appropriée pour se pencher sur la façon dont ces capacités devraient être réparties dans l'ensemble du gouvernement.

Alors je dirais, oui, mais il ne faut pas seulement mettre l'accent sur le CSTC, mais plutôt sur ce que le centre représente en tant que bien national pour le gouvernement afin qu'on puisse s'attaquer à l'ensemble des défis liés à la cybersécurité.

Mme Joyce Murray: J'ai des questions concernant deux autres domaines. Je tâcherai d'être brève.

Le directeur adjoint de l'agence de la Sécurité intérieure a déclaré qu'il est essentiel d'intégrer la protection de la vie privée et des libertés civiles aux programmes et activités de cette agence pour la renforcer et accroître son efficacité. En d'autres mots, le respect de la vie privée ne va pas directement à l'encontre d'un haut niveau de sécurité. Si on intègre adéquatement ce premier élément à l'organisation, on a en fait le meilleur des deux mondes. Seriez-vous d'accord avec cette approche ?

M. Rafal Rohozinski: J'y serais très favorable, comme en font foi — je crois — les commentaires que j'ai livrés durant mon témoignage. Nous risquons de réécrire en silence le contrat social entre les citoyens et l'État si nous ne tenons pas compte du rôle de la protection de la vie privée et des droits individuels en rééquilibrant les valeurs institutionnelles.

● (1615)

Mme Joyce Murray: En d'autres mots, si on modifiait adéquatement les lois régissant le CSTC pour améliorer la protection de la vie privée, cela, en fait, aurait pour effet de le renforcer.

M. Rafal Rohozinski: C'est exact, mais je devrais peut-être faire une petite précision qui est très importante. Il y a la surveillance à des fins d'application de la loi, mais il y a aussi la surveillance de la santé publique. Ces deux formes de surveillance utilisent essentiellement le même genre de méthode, c'est-à-dire recueillir des données pour comprendre des tendances liées à certains comportements ou incidents afin qu'il puisse y avoir une intervention.

Nous en sommes venus à comprendre le rôle de la surveillance de la santé publique et son importance pour les enjeux fondamentaux en matière de santé publique. Nous avons compris que ce rôle, dans une optique d'application de la loi, nous permet de déterminer quelles personnes sont à risque de commettre des actes criminels bien avant qu'elles soient prises en charge par le système de justice pénale. Je pense qu'il est probablement bien plus pertinent de réfléchir à ces leçons pour voir comment elles peuvent être appliquées à la surveillance policière du cyberespace que de simplement considérer le monde de l'application de la loi ou de la surveillance gouvernementale à la lumière des révélations de Snowden. Je crains que le balancier aille dans le sens inverse.

Mme Joyce Murray: D'accord. Merci.

Les organismes de nos autres partenaires Five Eyes déploient ce genre d'efforts coordonnés, mais pas les nôtres. En outre, vous venez de dire que les activités de cet ordre sont menées en vase clos. Il a été dit — et je suis d'ailleurs d'accord avec ce commentaire — que si nous avons ces cloisonnements, c'est en partie parce que nous n'avons pas de comité parlementaire chargé d'examiner tous les ministères et les organismes qui s'occupent de la sécurité et du renseignement de sécurité.

Dans les pays où il y en a un — c'est-à-dire tous nos partenaires Five Eyes —, ce comité parlementaire qui a le pouvoir de mener ce genre d'activités en vertu d'habilitations de sécurité peut, de fait, cerner les lacunes, les chevauchements et les problèmes d'interopérabilité. C'est comme si la GRC était sur la même fréquence que la sécurité de la Chambre des communes. C'est en partie pour cette raison que les autres pays ont des services coordonnés — contrairement à nous —, alors il y a beaucoup de…

Le président: Madame Murray, votre temps est malheureusement écoulé.

Nous allons passer à la deuxième série de questions, avec des interventions de cinq minutes. C'est à M. Williamson d'ouvrir le bal.

M. John Williamson (Nouveau-Brunswick-Sud-Ouest, PCC): Merci, monsieur le président.

Merci d'être avec nous aujourd'hui. C'est très intéressant.

Je vais revenir sur certains points que vous avez soulevés ou vous poser quelques questions à ce sujet afin d'avoir un peu plus de contexte.

Vous avez dit que certaines menaces pourraient créer et générer des « effets prolongés » au pays ou dans la société. Pourriez-vous expliquer ce que cela pourrait englober ou ce à quoi vous faisiez allusion?

M. Rafal Rohozinski: Ce pourrait être quelque chose d'aussi simple que la perturbation à grande échelle des réseaux de télécommunications; la manipulation des données dans des systèmes cruciaux, par exemple, ceux du Conseil du Trésor ou de la Banque du Canada; ou la manipulation à distance du système SCADA ou des systèmes de contrôle des processus relatifs aux réseaux de distribution d'électricité ou, par exemple, aux centrales nucléaires. Il peut donc s'agir d'effets quasi physiques — c'est-à-dire quand on touche aux infrastructures — ou encore de manipulation de l'information afin d'en miner la fiabilité ou de favoriser une défaillance des systèmes causée par le fait qu'ils ne pourront plus s'appuyer sur les données reçues.

M. John Williamson: Merci.

Vous avez dit que nous n'avons pas établi d'exigences réglementaires; qu'entendez-vous par là? Encore une fois, je comprends votre point de vue, mais pourriez-vous préciser ce que cela pourrait impliquer pour le gouvernement ou le Parlement? Je comprends dans une certaine mesure ce que vous dites.

M. Rafal Rohozinski: Je vais vous donner un exemple. Il sera enjolivé, mais je crois qu'il sera éloquent.

Toutes les banques canadiennes utilisent les mêmes fournisseurs d'accès Internet pour la plupart de leurs services de réseau. Elles peuvent voir tout ce qui se produit dans leur infrastructure, mais pas ce qui se produit à l'échelle des diverses infrastructures; c'est seulement au niveau de l'exploitant que cela devient visible. À l'heure actuelle, si cet exploitant allait dire aux banques qu'il a détecté une vulnérabilité touchant chacune d'entre elles, il y a fort à parier qu'elles lui demanderaient pourquoi il ne les a pas averties 30 secondes plus tôt, quand il l'a su, et qu'elles le tiendraient responsable de leurs pertes.

Cela a un effet pervers, car les exploitants d'infrastructures n'ont pas avantage à fournir ces renseignements. À mon avis, si on modifiait les instruments actuels de la Loi sur les télécommunications pour obliger les exploitants à les fournir, cela — premièrement — leur permettrait d'éviter d'être tenus responsables et — deuxièmement — augmenterait les renseignements utilisables sur le plan de la cybersécurité qui seraient à la disposition des clients en aval.

● (1620)

M. John Williamson: Voilà qui est intéressant. Je pense que vous soulevez un bon point, mais ne risquons-nous pas de… Je vais aborder l'aspect vers lequel se dirige M. Daniel, je crois, avec l'approche sectorielle; j'en viens même à me demander s'il est préférable d'adopter une approche à grande échelle ou à petite échelle. Je vais vous donner un bref exemple: celui que vous avez fourni au sujet de l'AP, si je ne m'abuse, quand vous avez parlé de la fausse nouvelle qui a été propagée.

Au bout du compte, je pense que nous voulons espérer qu'AP a la responsabilité de se protéger contre ce genre d'attaques. C'est cette organisation qui a le plus à perdre quand une telle attaque survient, car c'est elle qui communique des renseignements erronés. Les gens remettent alors en question ses données; ils se tournent vers d'autres sources d'information. De même, je crains que, si nous imputons la responsabilité des données des banques à une autre entité, personne n'en soit vraiment responsable. Je n'en suis pas arrivé à une conclusion sur la question, mais les banques ne devraient-elles pas être responsables de leur propre sécurité? Si nous continuons à déléguer les responsabilités vers le haut, peut-être qu'en fin de compte, personne ne sera responsable de leur contrôle. Si je dis cela, c'est parce qu'à mon sens, les joueurs de ce milieu doivent être agiles et savoir s'adapter, reconnaître les menaces et évaluer la situation, et je suis frappé de voir que, finalement, c'est au sein du gouvernement qu'on voit le moins ce genre de réflexion et d'approche. Comprenez-moi bien: il y a certaines choses que les gouvernements font très bien.

Le président: Monsieur Williamson…

M. John Williamson: Il me reste probablement une trentaine de secondes à peine, mais cette question d'une approche à grande échelle ou à petite échelle…

M. Rafal Rohozinski: Je ne crois pas que le gouvernement devrait assumer la responsabilité, mais je pense qu'il a comme rôle d'établir des règles à des fins soit régulatrices, soit incitatives. Dans certains cas, il est probablement fort préférable de créer des incitatifs pour la communication de renseignements au moyen d'une réglementation très légère plutôt que de créer une institution chargée de la surveillance à cet égard. Selon moi, il est important de prendre des mesures tant à grande échelle qu'à petite échelle.

Le président: Merci. Le temps est écoulé.

Monsieur Chisholm, s'il vous plaît.

M. Robert Chisholm: Merci beaucoup, monsieur le président.

Encore une fois, je vais partager mon temps avec M. Rafferty.

Nous avons effleuré le sujet de l'État islamiste et de son rôle dans le cyberespace. Apparemment, une conférence s'est déroulée récemment au Koweït. Certains des partenaires Five Eyes étaient là, mais pas le Canada. Que fait-on ou que devrait-on faire pour lutter contre les actes de l'État islamiste dans le cyberespace?

M. Rafal Rohozinski: Je vais vous fournir une réponse à deux volets qui répondra en partie à une question posée tout à l'heure.

Cette méthode de surveillance de la santé publique comme moyen d'identifier les personnes à risque a bel et bien — je crois — une applicabilité dans le cyberespace et pourrait être appliquée à l'échelle communautaire sans porter atteinte aux droits des Canadiens. Il y a certainement quelque chose que nous devrions faire, car l'État islamiste est seulement la pointe de l'iceberg en ce qui concerne la menace d'autoradicalisation à laquelle nous sommes confrontés.

Je crois que ce serait une grave erreur d'empêcher l'État islamiste d'utiliser Internet. En effet, c'est un canal qui nous permet de comprendre les actes et les motivations de ses membres, et il est bien plus utile pour nous de recueillir ainsi des renseignements de sécurité sur cette organisation que de simplement l'empêcher d'accéder à Internet. Si je dis cela, c'est en partie parce que notre entreprise a été engagée pour réaliser précisément ce genre de travail, c'est-à-dire comprendre les motivations et les actes d'organisations comme l'État islamiste dans des pays tels que la Syrie et l'Irak.

M. Robert Chisholm: Alors, vous dites que cela permet de faire le travail d'évaluation et de détection ici, ou en ligne.

M. Rafal Rohozinski: Tout à fait. C'est un autre sujet, mais il est peut-être important.

Étant donné qu'Internet dans sa totalité est le reflet de la majeure partie de l'humanité à l'heure actuelle, c'est probablement l'outil de renseignement le plus précieux dont nous disposons. Par « renseignement », je n'entends pas les renseignements d'États; je parle plutôt de renseignements ouverts. Internet nous permet vraiment d'avoir un aperçu de conversations qui, par le passé, seraient restées locales et connues de quelques personnes seulement. Qui plus est, nous pouvons acquérir ces renseignements en maintenant une distance: pas en utilisant la capacité du CSTC d'écouter des conversations très ciblées entre deux personnes, mais, vraiment en étant capable de les écouter dans un contexte de foule.

Je pense que cet aspect n'est vraiment pas apprécié à sa juste valeur. Mes collègues dans le milieu du renseignement de sécurité aux États-Unis diront ouvertement que de 80 à 90 % des renseignements utiles sont des renseignements de sources ouvertes. Ce n'est pas le genre de renseignements que nous obtenons en payant les institutions; c'est plutôt de l'information qui est bel et bien accessible et qui doit simplement être traitée après avoir été obtenue à l'état brut.

● (1625)

M. Robert Chisholm: Intéressant, très intéressant.

Le président: Monsieur Rafferty, vous avez 90 secondes.

M. John Rafferty (Thunder Bay—Rainy River, NPD): Je vous remercie, monsieur le président.

Merci de votre présence, monsieur Rohozinski. Je veux juste revenir sur certains commentaires de Mme Murray au sujet de l'accès légal et de la protection de la vie privée.

Vous avez de l'expérience de travail pour d'autres gouvernements nationaux. Devrait-on élaborer des lois et des normes internationales pour régir le cyberespace? Très brièvement, pourriez-vous nous expliquer ce qui a été fait et nous faire part de vos réflexions personnelles à l'égard du respect de la vie privée?

M. Rafal Rohozinski: Je pense qu'à l'heure actuelle, les changements dans le secteur commercial et le regroupement des données à grande échelle représentent un risque bien plus grand que ce qui se passe dans les institutions gouvernementales. C'est un domaine extrêmement problématique, car non seulement nous avons créé une industrie à partir de cela, mais nous en bénéficions aussi de façon disproportionnée. Par exemple, il y a une fonction utilitaire — pour laquelle nous renonçons tous quand nous décidons de divulguer des renseignements personnels à Google — qui nous permet d'organiser notre quotidien de façon plus efficace et efficiente.

Comme je l'ai dit, je pense que le risque de réécrire secrètement le contrat social… Et je ne parle pas seulement de celui qui lie les institutions gouvernementales et les citoyens. À cet égard, la responsabilité du troisième secteur — le secteur privé — doit vraiment être explorée en profondeur, ce qui n'a pas été fait à ce jour. Je crois que les révélations de Snowden ont au moins levé le voile sur le fait qu'il s'agit d'une question de contrat social, mais le fait qu'on a beaucoup considéré cela comme la responsabilité des institutions gouvernementales a partiellement occulté — à mon avis — la nécessité de mener un examen bien plus approfondi de la situation.

Le président: Merci.

Notre dernier intervenant est M. Bezan. Vous avez cinq minutes.

M. James Bezan (Selkirk—Interlake, PCC): Merci, monsieur le président.

Monsieur Rohozinski, c'est bon de vous revoir. La dernière fois que nous avons discuté, il était question de la situation en Iran, de ses cybercapacités et d'attaques que ce pays a orchestrées en sol nord-américain. Je veux savoir ceci: qui représente une menace?

Par ailleurs, vous avez peut-être entendu parler d'une histoire divulguée la semaine dernière, selon laquelle un destroyer américain — l'U.S.S. *Donald Cook* — a été rendu non opérationnel par un bombardier russe non armé en avril dernier pendant qu'il patrouillait la mer Noire. Le réseau Voltaire a signalé qu'un Su-24 russe a frôlé le navire et a « neutralisé tous les radars, circuits de contrôle, systèmes de transmission d'information, etc. embarqués à bord du destroyer US. Autrement dit, le tout-puissant système Aegis, aujourd'hui incorporé [aux] navires les plus modernes de la OTAN [*sic*], a été tout simplement déconnecté. »

Quelle est la crédibilité de cette histoire? À quelles autres capacités faisons-nous face sur le plan militaire?

M. Rafal Rohozinski: Encore une fois, je reviendrais sur ce que j'ai dit tout à l'heure. Dans le cadre du travail que j'ai réalisé cette année — c'est la première année — avec l'Institut international d'études stratégiques, la notion d'équilibre stratégique — qui sert vraiment d'étalon au moment d'examiner les capacités des États-nations et d'autres joueurs dans des domaines militaires traditionnels — a commencé à englober le cyberespace comme un de ces domaines. Peut-être que l'aspect le plus intéressant des travaux de recherches menés, c'est le grand nombre de pays en train de développer des cybercapacités actives, offensives.

Pourquoi est-ce ainsi? Comme je l'ai dit tout à l'heure, c'est parce que ça leur permet de sauter tout un stade de développement dans la guerre industrielle. Cela abaisse le seuil à partir duquel ils peuvent rivaliser sur les plans politique et militaire, en ce sens qu'il n'est plus nécessaire d'investir dans des techniques impliquant du matériel à utilisation humaine qui étaient en fait seulement accessibles aux pays les plus développés. Au fond, la question consiste non pas à déterminer qui est une menace, mais plutôt qui n'en est pas une, puisque le seuil est si bas. À mon avis, si nous ne voulons pas être comme des Zoulous devant une mitrailleuse Gatling, nous devons nous réveiller et reconnaître qu'il est essentiel d'investir dans les cybercapacités en tant que composante de la sécurité et de la défense nationales et qu'il faut consacrer le temps et les ressources nécessaires au développement de ces capacités.

Concernant la question du système Aegis dont était muni le destroyer, je ne peux pas vraiment faire de commentaires à ce sujet. J'ai entendu parler de cette histoire, mais il pourrait tout aussi bien s'agir d'une fausse nouvelle faisant partie de la stratégie opérationnelle d'information des Russes dans le contexte du conflit ukrainien.

M. James Bezan: Qu'il se soit vraiment produit ou non, est-ce qu'un tel incident serait considéré comme un acte de guerre?

M. Rafal Rohozinski: La question mérite d'être posée, et il y a eu beaucoup de travail réalisé au cours des trois dernières années afin de déterminer comment les actuelles lois sur les conflits armés pourraient être modifiées afin d'inclure la question du cyberespace. Je pense que l'on comprend mieux maintenant — surtout depuis les événements survenus en Ukraine et en Crimée — qu'il est impératif d'intégrer cette composante à la liste des éléments susceptibles de déclencher une réaction des alliés.

Toutefois, comme nous l'avons vu — et je suis certain que votre comité se penchera également sur cette question — le cyberespace a assurément un rôle très grand et très important à jouer dans les guerres hybrides, c'est-à-dire celles qui ne sont pas régies par les lois sur les conflits armés et qui ne sont pas considérées comme une guerre entre deux États. Étant donné la confluence de ces deux éléments, je pense qu'il sera extrêmement difficile de créer des normes régissant l'utilisation des cybercapacités dans le contexte de guerres n'impliquant pas deux États.

● (1630)

M. James Bezan: Les États-Unis ont établi un cybercommandement. Nous menons certaines activités dans le NORAD — et il est question de la défense de l'Amérique du Nord — mais nous avons aussi une excellente relation avec l'OTAN; et vous avez déjà mentionné l'Estonie. C'est là-bas que se trouve le centre d'excellence de l'OTAN pour la coopération en matière de cyberdéfense. Pouvez-vous dire dans quelle mesure il est important que le Canada joue un rôle accru en matière de cybersécurité au sein de ces organisations multinationales?

M. Rafal Rohozinski: Ce centre n'est pas une structure opérationnelle de l'OTAN. C'est un centre de recherche, alors il n'a en fait aucune capacité, outre la fonction de recherche qui lui est confiée. Me demandez-vous si le Canada devrait se doter d'un cybercommandement ou, du moins, se demander comment intégrer une cyberforce dans son actuelle structure de forces? Si oui, je vous réponds sans équivoque par l'affirmative. Évidemment, le défi, c'est que nous avons trois services solides et nos propres traditions en matière d'institutions et qu'il sera difficile de les réorganiser pour créer une cyberforce sur les plans institutionnel et budgétaire et aussi en raison — tout simplement — du leadership visionnaire nécessaire pour arriver à ce résultat.

Le président: Sur cet appel à l'action, monsieur Rohozinski, nous allons mettre fin à cette heure de travaux et à votre témoignage. Toutefois, au nom de tous les membres du comité, je vous invite à nous faire part de toute réflexion qui pourrait vous venir à la suite de votre comparution, de tout sommaire ou de tout conseil que vous souhaiteriez encore nous communiquer. Quoi qu'il en soit, nous vous remercions assurément de votre présence ici aujourd'hui.

Mme Joyce Murray: Il y avait d'autres questions, mais le temps est maintenant écoulé.

Merci.

Le président: Nous allons maintenant suspendre la séance pendant que nos prochains témoins prennent place. Si possible, nous aimerions que la transition se fasse de façon fluide et rapide.

● (1630)

(Pause)

● (1635)

Le président: Bon, chers collègues, poursuivons notre étude de la défense nord-américaine.

Deux représentants du ministère des Pêches et Océans sont avec nous aujourd'hui. Ils sont tous deux rattachés à la Garde côtière canadienne. Il s'agit de Nadia Bouffard, sous-commissaire, Opérations, et de Gregory Lick, directeur, Soutien des opérations.

Madame Bouffard, veuillez nous livrer votre déclaration préliminaire.

Mme Nadia Bouffard (sous-commissaire, Opérations, Garde côtière canadienne, ministère des Pêches et des Océans): Merci, monsieur le président.

[*Français*]

Bonjour à tous.

[*Traduction*]

Je m'appelle Nadia Bouffard. Je suis sous-commissaire intérimaire aux opérations de la Garde côtière canadienne. Je suis accompagnée de Greg Lick, directeur général des opérations.

Merci de nous donner l'occasion de parler de la Garde côtière canadienne et de son rôle au chapitre de la sécurité maritime. La Garde côtière canadienne appuie ses partenaires et alliés et sert la population canadienne avec fierté, et cela ne date pas d'hier. Depuis plus de 50 ans, elle est reconnue à l'échelle du pays comme un symbole de sécurité et de service maritimes. Notre personnel travaille dans des circonstances difficiles, dans le plus rude des climats et dans bon nombre des régions les plus reculées du Canada. Les navires de la Garde côtière canadienne, facilement reconnaissables à leur coque rouge et blanche, symbolisent la sécurité, la souveraineté et la sûreté.

Notre mandat consiste surtout à assurer la sécurité des marins en mer, et nous mettons en oeuvre des programmes cruciaux pour veiller à ce que les déplacements des navires dans les eaux canadiennes soient sécuritaires, économiques et efficients. À cette fin, notre service direct inclut l'aide à la navigation et à la gestion des voies navigables, les interventions environnementales, le déglaçage et les services de communications et de trafic maritimes ainsi que, bien sûr, les activités de recherche et de sauvetage. Ces services sont dispensés le long de la plus longue bande littorale au monde et dans de grandes voies navigables telles que les Grands Lacs, la voie maritime du Saint-Laurent, le fleuve Mackenzie et le lac Winnipeg, pour n'en nommer que quelques-unes.

Bien que nous n'ayons pas explicitement de mandat législatif en matière de sécurité et d'application de la loi, j'expliquerai aujourd'hui comment nous appuyons directement nos partenaires qui ont de tels mandats.

Notre flotte représente le pilier de notre organisation. Le gouvernement a récemment injecté 6,8 milliards de dollars dans le renouvellement de nos navires et de nos hélicoptères, et je suis ravie de déclarer que nous avons réalisé d'importants progrès sur ce plan.

Le comité sera peut-être très intéressé d'apprendre que nous avons récemment intégré à notre flotte en service les derniers patrouilleurs semi-hauturiers. Ces neuf nouveaux patrouilleurs fournissent de nouveaux outils pour réaliser notre programme de sécurité maritime sur les Grands Lacs et la voie maritime du Saint-Laurent, et pour assurer la protection et la conservation des ressources halieutiques le long des côtes Atlantique et Pacifique. Nous renouvelons notre flotte en vue de maintenir nos importantes capacités en matière de navires et d'hélicoptères dans l'avenir.

En ajoutant à cela nos divers systèmes de suivi des navires, on peut dire que la Garde côtière canadienne est bien en mesure d'appuyer les priorités de sécurité du Canada. Aucun ministère ni organisme n'est responsable à lui seul de la sûreté maritime au pays. Il importe de reconnaître que c'est toujours le ministère qui dirige les efforts en ce sens, étant donné son mandat explicite en ce qui a trait à la sûreté, au renseignement de sécurité et à l'application de la loi. Les autres organisations qui participent à ces efforts incluent notamment la GRC, Transports Canada, l'Agence des services frontaliers du Canada, Pêches et Océans Canada — pour nos agents de conservation et de protection — et le ministère de la Défense nationale.

La Garde côtière joue deux rôles au chapitre de la sûreté maritime. Nous fournissons des renseignements maritimes cruciaux à nos partenaires de sécurité et nous contribuons à la mise en œuvre d'activités de sûreté sur l'eau. L'information que nous fournissons est essentielle pour améliorer la connaissance du domaine maritime, qui est à la base de la sécurité maritime au pays.

Pour ce faire, le Canada utilise une approche multidimensionnelle qui est le fruit d'un effort coordonné — entre les ministères fédéraux, les pays alliés et d'autres ordres de gouvernement — qui vise à recueillir, à regrouper et à analyser l'information et les renseignements de sécurité pour soutenir la surveillance maritime. Les organisations fédérales utilisent ces renseignements à diverses fins, comme la sécurité et la sûreté maritimes, la défense nationale et la protection environnementale. Par exemple, le rapport sur les renseignements exigés au préalable — 96 heures à l'avance — fournit à nos partenaires de sécurité de l'information sur le type de navire, la marchandise, l'équipage, le plus récent port d'escale, le port de destination et le pays d'origine.

Les systèmes de suivi et d'identification des navires de la Garde côtière valident les renseignements sur l'emplacement déclarés par les navires et surveillent leurs déplacements dans la zone économique exclusive du Canada et ses approches maritimes ainsi que dans le reste du monde. L'information recueillie provient d'un certain nombre de sources, comme les radars, le Système d'identification automatique et le Système d'identification et de suivi à distance, de même que d'autres systèmes de gestion du trafic maritime.

● (1640)

Nous recueillons aussi de l'information météorologique et géographique ainsi que des rapports en temps réel sur les navires commerciaux et les embarcations de plaisance repérés par nos propres navires.

Le Système d'identification et de suivi à distance fournit des données de position sur les navires de 300 tonnes et plus, dont les navires battant pavillon canadien, les navires internationaux qui se dirigent vers un port canadien et les navires qui transitent à l'intérieur des 1 000 miles nautiques du littoral canadien. Dans une zone de 50 milles nautiques, c'est le Système d'identification automatique de la Garde côtière canadienne qui fait le suivi des navires de 300 tonnes et plus.

Ces capacités sont essentielles dans le vaste territoire arctique canadien, où il existe peu de ressources rapidement utilisables pour faire le suivi du domaine maritime. Le rôle important joué par la Garde côtière canadienne pour ce qui est de fournir de l'information maritime se remarque de surcroît par sa présence dans les trois centres des opérations de la sûreté maritime, ou les COSM, comme on les appelle. Ces centres jouent un rôle crucial dans la collecte, l'analyse et la communication d'informations et de renseignements de sécurité dans le domaine maritime. Situés sur la côte Ouest du Canada et dans la région des Grands Lacs, on y trouve des gens de cinq ministères fédéraux: le ministère des Pêches et des Océans et la Garde côtière canadienne, le ministère de la Défense nationale, Transports Canada, l'Agence canadienne des services frontaliers et la GRC.

La Garde côtière canadienne procure beaucoup de valeur à ces centres, car elle fournit près de 80 % des renseignements sur le trafic maritime dont ses partenaires ont besoin. Dans le Nord, les centres des opérations de la sûreté maritime de la Garde côtière assurent le suivi de tous les navires qui pénètrent dans l'Arctique, y compris dans toute la zone de services de trafic maritime du Nord canadien. Depuis les salles de surveillance des centres, la Garde côtière envoie des rapports sur toutes les activités connues des navires dans l'Arctique et dans les approches, et ce, deux fois par jour.

Le personnel de nos centres des opérations de la sûreté maritime communique régulièrement avec diverses organisations fédérales, territoriales et internationales pour maintenir une bonne connaissance de toutes les activités dans l'Arctique. Sans s'y limiter, cela inclut la liaison avec le ministère des Affaires étrangères; Environnement Canada; l'Agence de la santé publique du Canada; les gouvernements du Nunavut, des Territoires du Nord-Ouest et du Yukon; le gouvernement du Groenland; et la garde côtière américaine.

[*Français*]

La Garde côtière canadienne joue un deuxième rôle important à l'appui de la sécurité canadienne en fournissant les plateformes maritimes et le soutien nécessaires à l'application de la loi ainsi qu'à la capacité d'intervention sur l'eau. Pour ce faire, la Garde côtière offre les navires, l'équipement, le personnel et son expertise aux organismes fédéraux d'application de la loi et de la sécurité, afin d'assurer une protection plus efficace dans les eaux navigables canadiennes.

Nos navires sont systématiquement présents dans les eaux canadiennes, le long de nos côtes, dans les Grands Lacs, tout au long du fleuve Saint-Laurent et dans le Haut-Arctique. Ils ont l'habitude de soutenir les activités d'application de la loi dans le cadre de leurs opérations quotidiennes et lorsque c'est nécessaire.

Un bon exemple de nos activités de routine maritime est le programme conjoint de l'Équipe des enquêtes sur la sûreté maritime de la Gendarmerie royale du Canada et de la Garde côtière. Ce programme conjoint assure la présence de ressources spécialisées en matière d'enquêtes sur la sûreté dans la voie maritime des Grands Lacs et du Saint-Laurent, la Garde côtière étant responsable de l'exploitation des navires, et la Gendarmerie royale, de toutes les activités liées à l'application de la loi.

Grâce à leur grande visibilité, aux patrouilles fréquentes et à leur capacité d'intervention rapide face aux menaces potentielles, ces équipes assurent une forte présence à l'échelle nationale et dissuadent les activités illégales.

En 2012, la Garde côtière a commencé la transition du programme de l'Équipe des enquêtes sur la sûreté maritime, passant de quatre navires intérimaires d'origine à de nouveaux patrouilleurs semi-hauturiers. Par comparaison avec les navires d'origine modifiés, ces nouveaux navires affichent une plus grande portée, une vitesse accrue et une meilleure capacité de navigation dans des conditions météorologiques difficiles, et ce, en tout temps.

De plus, ils sont en mesure de communiquer de façon sécuritaire avec d'autres navires appartenant au gouvernement du Canada, ainsi qu'avec des réseaux nationaux classifiés de commandement et de contrôle, ce qui renforce le programme considérablement. Ces nouveaux navires ont été construits à des fins précises de réalisation d'activités de sûreté maritime et ils ont amélioré la capacité globale de la Garde côtière de fournir un soutien efficace lors d'activités maritimes d'application de la loi.

● (1645)

Les navires de la Garde côtière canadienne jouent aussi un rôle essentiel de soutien des priorités en matière de sûreté maritime dans l'Arctique. Chaque année, de la fin de juin au début de novembre, la Garde côtière canadienne déploie six brise-glaces: un brise-glace léger, et une combinaison de cinq brise-glaces lourds et brise-glaces moyens dans l'Arctique.

Souvent la seule présence visible du gouvernement du Canada dans de nombreux secteurs de la région, ces navires renforcent la souveraineté du Canada par la prestation de services essentiels aux partenaires et aux collectivités nordiques.

Cela comprend l'escorte de navires commerciaux...

Le président: Excusez-moi.

[*Traduction*]

Pourriez-vous clore rapidement votre déclaration préliminaire afin que nous ayons assez de temps pour poser des questions?

Mme Nadia Bouffard: Avec plaisir.

[*Français*]

Cela comprend l'escorte des navires commerciaux et militaires à travers des eaux glacées pour livrer des fournitures essentielles aux résidents du Nord, une capacité de recherche et de sauvetage, ainsi qu'un rôle de premier répondant lors d'incidents de pollution.

Cela comprend aussi nos plateformes à l'appui des travaux scientifiques, comme la collecte de données scientifiques marines, le relèvement hydrographique, la cartographie du plateau continental du Canada, et les travaux de recherches, tels que ceux qui ont mené à la découverte de l'un des navires de l'expédition de Franklin.

Toujours dans l'Arctique, la Garde côtière canadienne s'assure que notre flotte continue de fournir un soutien efficace aux milieux de la sûreté et de l'application de la loi.

Cela comprend notre participation aux exercices dans l'Arctique, comme l'opération Nanook, à laquelle nous prenons part depuis un certain nombre d'années, aux côtés de nos partenaires du ministère de la Défense nationale.

À l'instar du programme de l'Équipe des enquêtes sur la sûreté maritime et de sa récente transition vers de nouveaux patrouilleurs semi-hauturiers, la capacité de brise-glace de la Garde côtière canadienne sera considérablement améliorée en 2022, avec l'arrivée du NGCC John G. Diefenbaker.

Il s'agira du premier brise-glace polaire et il remplacera le NGCC Louis S. St-Laurent à titre de porte-étendard de la flotte arctique du Canada.

Le NGCC John G. Diefenbaker pourra être utilisé dans l'Arctique pendant de plus longues périodes chaque année et dans des conditions de glace plus difficiles que ce n'est le cas actuellement.

[*Traduction*]

En conclusion, bien que la Garde côtière canadienne n'ait pas de mandat direct — législatif ou autre — en matière de sûreté, elle fournit un apport important à la sûreté maritime du Canada.

Merci.

Le président: Merci, madame la sous-commissaire.

Nous allons amorcer notre première série de questions. Les interventions seront de sept minutes. Monsieur Williamson, à vous de commencer.

M. John Williamson: Merci, monsieur le président.

Madame Bouffard, monsieur Lick, merci de votre présence ici aujourd'hui.

Malheureusement, j'ai baissé la tête au mauvais moment lors de votre déclaration préliminaire. Avez-vous dit — et je m'excuse si je fais erreur — que la Garde côtière n'a pas le mandat d'appliquer la loi? Ai-je bien compris? Peut-être que non.

Mme Nadia Bouffard: C'est exact.

M. John Williamson: Ah bon. C'est intéressant. Je ne le savais pas.

Je viens du sud du Nouveau-Brunswick, et, dans mon patelin, quand nous regardons au loin d'autres coins du pays, nous voyons des îles américaines situées entre l'endroit où on se trouve et ces endroits-là. Ce n'est donc pas seulement dans le Nord que la Garde côtière défend notre souveraineté et surveille la frontière. C'est même tout près de chez nous et, bien souvent, près de ports américains aussi.

J'ai une question brève. Bien que la Garde côtière n'ait pas le mandat d'appliquer la loi, il arrive de temps à autre qu'on débatte de la possibilité d'armer ses agents. Avez-vous une opinion sur ce sujet?

● (1650)

Mme Nadia Bouffard: Vous avez tout à fait raison de dire que nos navires et notre équipage ne sont pas armés, à l'exception de deux navires stationnés à St. John's, sur la côte Est, qui sont munis — je crois — d'une arme d'un calibre de 50 mm…

M. Gregory Lick (directeur, Soutien des opérations, Garde côtière canadienne, ministère des Pêches et des Océans): D'une mitrailleuse de calibre 50 et d'armes de poing de 9 mm.

Mme Nadia Bouffard: Merci.

Ces navires armés travaillent donc dans un contexte hautement spécialisé en vertu de la Loi sur la protection des pêches côtières, de la Loi sur les pêches et du Code criminel. Nos agents des pêches et nos agents de la protection des pêches mènent leurs activités dans ce contexte, en vertu de ces lois.

M. John Williamson: Avez-vous une opinion concernant cet aspect en général? Faudrait-il qu'on se penche là-dessus? Bon, en fait, laissez-moi revenir en arrière.

Est-ce que les gardes côtiers de nos proches alliés — les États-Unis, la Grande-Bretagne, l'Australie — ont un mandat policier, un mandat d'application de la loi?

Mme Nadia Bouffard: Le rôle des gardes côtiers dans le monde et la portée de leurs pouvoirs diffèrent selon les pays. Ceux, entre autres, qu'on est habitué de voir et qu'on connaît bien — puisqu'on les voit à la télévision — ce sont les gardes côtiers américains, qui sont armés et qui ont un mandat bien plus vaste.

Au Canada, nous avons une approche multidisciplinaire impliquant divers ministères. Nous ne sommes pas mandatés pour mener des opérations de sûreté et d'application de la loi, mais nous appuyons le programme et les organisations qui ont ce mandat. Il y a des agents de la GRC à bord de nos navires pour mener de telles opérations.

Greg, savez-vous ce qu'il en est dans les autres pays? Je connais bien la garde côtière américaine, mais pas les autres.

M. Gregory Lick: Madame Bouffard a raison à cet égard. Les gardes côtières dans le monde varient beaucoup d'un pays à l'autre, et elles ont toutes des rôles et des mandats différents. À coup sûr, comme l'a dit Mme Bouffard, nous n'avons pas de mandat en matière de sûreté, mais il y a des exemples très clairs et très éloquents d'endroits où nous fournissons un soutien à nos partenaires, comme la GRC sur les Grands Lacs, et dans la voie maritime du Saint-Laurent, au moyen de nos ESM. C'est probablement le meilleur exemple d'opérations conjointes que nous menons avec eux.

Les autres exemples sont surtout des opérations de sûreté ponctuelles où nous conduisons notre partenaire à l'endroit où une interception particulière a lieu.

M. John Williamson: Intéressant.

Avez-vous des réflexions ou des commentaires à formuler à propos de la question globale du port d'armes par tous les agents de la Garde côtière, pas seulement à bord des deux navires à St. John's que vous avez mentionnés, mais dans toute la flotte?

Mme Nadia Bouffard: Nous avons examiné la question par le passé, et nous n'avons pas reçu la directive de modifier notre approche actuelle, alors nous réalisons actuellement notre mandat conformément aux directives qui nous ont été données.

M. John Williamson: Je m'attendais à ce que vous disiez cela.

Le président: Soyez très bref, s'il vous plaît, monsieur Williamson.

M. John Williamson: Je n'ai pas le choix. Il y a tellement d'aspects à aborder.

Je sais que vous avez effleuré le sujet, mais vous n'avez pas eu l'occasion de parler de certaines ressources basées dans le Nord, dans l'Arctique.

Mme Nadia Bouffard: Tout d'abord, elles ne sont pas basées dans le Nord.

M. John Williamson: Merci pour la précision.

Mme Nadia Bouffard: Elles exercent des activités dans cette région pendant une bonne partie de l'année, soit de juin à novembre. Dans ma déclaration préliminaire, j'ai mentionné que nous avons six brise-glaces de diverses tailles qui font du déglaçage et dispensent certains services, et qu'ils sont disponibles pour divers services comme des interventions environnementales et des opérations de SAR durant cette période.

Greg, voulez-vous parler plus en détail des brise-glaces?

M. Gregory Lick: Certainement.

Comme l'a dit Mme Bouffard, nous utilisons six brise-glaces dans le Nord. En outre, nous menons des activités courantes de déglaçage et d'approvisionnement de communautés éloignées, entre autres choses. Nous avons aussi deux ou trois navires sur le fleuve Mackenzie qui ont surtout une fonction d'aide à la navigation. Les services en matière de sûreté ne sont pas — évidemment — le principal type de service que nous fournissons, mais notre rôle là-bas est surtout d'aider à la navigation, de procéder à des opérations de recherche et de sauvetage et d'assurer la surveillance.

Je pense que l'autre ressource — si ce mot est juste — qu'il importe de mentionner, c'est le Centre des opérations de la sûreté maritime qui effectue la surveillance dans l'Arctique. C'est un autre élément clé de notre soutien en matière de sûreté. Dans ce cas-ci, c'est la garde côtière du COSM de l'Est qui l'effectue pour nous et qui fournit le gros des renseignements à nos partenaires, tout particulièrement en ce qui concerne la zone maritime de l'Arctique.

● (1655)

Le président: Merci, monsieur Lick.

Monsieur Chisholm, vous avez sept minutes.

M. Robert Chisholm: Merci beaucoup, monsieur le président.

J'ai une foule de questions à poser. Si cela vous convient, je vais toutes les formuler, puis je vous donnerai l'occasion d'y répondre.

Il y a deux choses ou trois dont j'aimerais parler. La première, c'est que vous faites partie des 17 ministères et organismes responsables de veiller à la sûreté maritime — ce qui ne doit pas être un jeu d'enfant — mais il existe apparemment un groupe de travail sur la sûreté maritime. J'aimerais que vous m'indiquiez quelle est la fréquence des réunions de ce groupe et peut-être à quelle date remonte sa plus récente réunion. J'aimerais aussi connaître quelques-uns des points qui étaient à l'ordre du jour.

L'autre chose dont je veux parler, ce sont les enjeux territoriaux qui entourent le passage du Nord-Ouest et l'Arctique. Je suppose que cela doit créer des tensions intéressantes entre le Canada et les États-Unis. J'aimerais que vous parliez un peu des difficultés additionnelles causées par cette situation tant pour ce passage que pour d'autres régions du Nord.

Je suis curieux. Le SID et aussi le SISD, je crois, permettent d'effectuer le suivi des navires de 300 tonnes brutes et plus. Qu'en est-il des navires moins lourds? Ne représentent-ils pas une menace pour la sécurité? On pourrait penser qu'ils ne sont donc pas détectés. Avez-vous des commentaires à ce sujet?

De plus, concernant les ressources dans le Nord, on a récemment décidé de reporter la construction sur la côte Ouest du nouveau brise-glace lourd qui est censé remplacer le *Louis*. Je réfléchis à ce qu'il adviendra de cela dans sept ou huit ans et je me pose des questions. Quand envisageons-nous de retirer le *Louis St-Laurent* du service? Qu'est-ce que cela signifie pour la capacité de la Garde côtière de remplir sa fonction de déglaçage à des fins de sûreté dans le Nord?

Toujours à propos des ressources, le directeur parlementaire du budget a publié récemment un rapport sur les patrouilleurs hauturiers. Ils étaient — bien entendu — promis pour 2007, et je crois que le budget affecté à cette fin était de 3,1 milliards de dollars. Il a laissé entendre que nous ne serons pas en mesure de produire six à huit navires: ce sera plutôt quatre et, si nous attendons encore, ce sera trois. Étant donné les capacités de déglaçage de ces navires, cela a certaines répercussions. Je me demande si vous pourriez nous livrer vos commentaires à l'égard de vos ressources, ou plutôt des biens dans le Nord. Je sais que ce ne sont pas « vos » biens, puisqu'ils ont été affectés à la marine.

Voici ma dernière question, je crois. Toujours à ce sujet — celui des patrouilleurs hauturiers pour l'Arctique — comment cela va-t-il fonctionner? La Garde côtière dispose de l'expertise relative à la dotation en personnel de ces navires et à leurs activités de déglaçage et de surveillance dans le Nord. Comment cela va s'articuler sur le plan opérationnel, vu que la marine est responsable de ces patrouilleurs, qu'il y en ait trois, quatre ou cinq? Comment cela va-t-il fonctionner?

Si vous le voulez bien, j'aimerais entendre vos commentaires.

● (1700)

Le président: La sous-commissaire a deux minutes et demie pour répondre à ces questions.

M. Robert Chisholm: Je l'ai vue au travail. Elle est capable de le faire.

Des voix: Oh, oh!

Mme Nadia Bouffard: Bon, je vais essayer. J'espère que vous allez m'aider, Greg.

Je vais d'abord répondre très rapidement à votre dernière question. Nous ne sommes pas des experts en approvisionnement, alors nous tenterons une réponse, et si nous pouvons vous fournir plus de détails après coup, nous le ferons.

M. Robert Chisholm: Merci.

Mme Nadia Bouffard: Je vais laisser à Greg le soin de répondre à la question concernant le groupe de travail sur la sécurité maritime, et je vais parler très brièvement des relations entre le Canada et les États-Unis. Je crois que cela répondra à certaines de vos questions.

La relation que nous entretenons avec les États-Unis et la garde côtière américaine dans le cadre de notre mandat est très étroite et axée sur la collaboration — et est très productive pour cette raison —, et ce, dans le Nord comme ailleurs, et qu'il soit question de sûreté ou d'interventions environnementales. Il est possible de le constater au moyen d'un certain nombre de groupes, de réunions, de traités, d'accords et de protocoles d'entente auxquels nous prenons part avec ce pays. Je pourrais vous donner deux ou trois exemples, mais, comme nous avons peu de temps, je ne le ferai pas. Disons simplement que nous avons une relation de longue date avec la garde côtière américaine. Il nous arrive régulièrement de participer à des réunions avec ses représentants et d'avoir des conversations téléphoniques avec eux depuis Ottawa comme des régions. Sur le plan des opérations, nous travaillons en très étroite collaboration. Il n'y a aucune difficulté à cet égard. Une telle relation est essentielle pour mener nos opérations.

Vous avez demandé pourquoi le seuil est fixé à 300 tonnes et ce qu'il advient des navires plus légers. Je crois que la règle à l'origine de cette limite de 300 tonnes brutes émane de l'Organisation maritime internationale, et que son rôle et son mandat étaient vraiment axés sur la sécurité et sur les risques associés à la sécurité des marins et à la protection environnementale.

Le président: Le temps est écoulé.

Monsieur Chisholm, vous pourrez revenir sur les réponses de Mme Bouffard à votre prochain temps de parole.

M. Robert Chisholm: Elle peut simplement fournir ses autres commentaires par écrit.

Le président: Effectivement, ce peut être par écrit.

C'est maintenant le tour de M. Norlock. Allez-y.

M. Rick Norlock: Merci beaucoup, monsieur le président.

Je remercie les témoins d'être présents ici aujourd'hui.

Puisque nous étudions la défense nord-américaine, pourriez-vous nous dire dans quelle mesure et dans quels domaines la Garde côtière canadienne coopère avec les Forces armées canadiennes à ce chapitre?

Mme Nadia Bouffard: C'est un autre exemple de notre relation très étroite et fluide avec les Forces armées canadiennes. Nous avons évidemment avec elles une relation très proche — une relation de partenaires — pour les activités de recherche et de sauvetage. Je copréside d'ailleurs un comité SAR avec le major-général Coates. Nous menons des opérations avec leur soutien et leur collaboration.

Greg, vous pourriez peut-être décrire plus en détail certaines activités que nous menons avec elle.

M. Gregory Lick: Je crois que j'aimerais ajouter quelques éléments à ce que Mme Bouffard a dit. Sans aucun doute, dans le domaine de la recherche et du sauvetage, les centres conjoints de coordination des opérations de sauvetage situés à Halifax, à Trenton et à Victoria, que nous partageons avec le personnel des Forces armées canadiennes, constituent notre principal secteur de collaboration. C'est de là que nous gérons le système SAR et l'ensemble des opérations. Ils sont l'un des éléments essentiels pour la recherche et le sauvetage et pour notre capacité de réagir efficacement dans les situations de recherche et de sauvetage.

Je crois que j'ajouterais à cela les exercices que nous faisons, dans le Nord et dans l'ensemble du pays. Nous effectuons de nombreux exercices avec les Forces armées canadiennes, principalement dans le domaine de la recherche et du sauvetage, qui est notre principal mandat ou notre priorité. Nous faisons aussi des exercices de sûreté maritime, qui supposent habituellement le soutien des hélicoptères des Forces armées canadiennes, l'utilisation de nos navires et la participation de différentes équipes d'intervention d'urgence, qui proviennent principalement de la GRC. Nous travaillons tous ensemble pour réagir face à la présence de navires dont nous avons pu apprendre l'existence grâce à notre connaissance du domaine maritime ou pour leur interdire l'accès.

Ce sont les principaux secteurs où, selon moi, nous concentrons nos efforts au chapitre de la coopération.

● (1705)

M. Rick Norlock: Merci beaucoup.

Puisque nous parlons de ce domaine, le programme des équipes d'application de la loi en matière de sûreté maritime est un projet conjoint de la GRC et de la Garde côtière canadienne. Comme vous l'avez mentionné, il a été créé en 2005, et il renforce la sûreté maritime, particulièrement dans les Grands Lacs et dans le secteur du Saint-Laurent. Pouvez-vous me dire quels genres d'interdictions cette équipe d'application de la loi ciblerait? Y a-t-il des menaces pour la sûreté au Canada auxquelles les ESM seraient confrontées? Ensuite, de quels genres de ressources la Garde côtière dispose-t-elle afin de s'acquitter de cette responsabilité?

Mme Nadia Bouffard: Concernant les ressources, nous avons parlé dans notre déclaration préliminaire de la remise à neuf des navires utilisés dans la Voie maritime du Saint-Laurent et dans les Grands Lacs, qui nous permettent de mieux soutenir nos partenaires, comme la GRC.

Je ne suis pas certaine de la réponse à la première question concernant les détails du rôle des ESM au chapitre de la sûreté.

M. Rick Norlock: Je sais qu'elles effectuent un travail précis.

Mme Nadia Bouffard: Oui.

M. Rick Norlock: Vous, ainsi que la GRC, visez certaines entités ou certaines menaces dans les Grands Lacs et le Saint-Laurent. J'aimerais en savoir plus sur les types de menaces auxquelles vous avez fait face depuis 2005, sur certaines opérations auxquelles vous avez participé, et sur certaines réussites, ou certains défis, à cet égard.

Mme Nadia Bouffard: Voulez-vous essayer de répondre à cette question?

M. Gregory Lick: Oui.

Sans entrer dans les détails des interdictions qui ont vraiment été mises en place, je dirais que la plupart des interdictions relatives au personnel, aux navires sur l'eau, et ainsi de suite, étaient principalement liées à des infractions au Code criminel. Je n'ai certainement pas tous les détails des types d'interdictions, mais elles étaient surtout liées au Code criminel.

Les infractions pourraient aller de quelque chose d'aussi simple que de l'alcool sur un bateau à de la contrebande ou quelque chose de ce genre. Certains incidents qui ont eu lieu sont connus du public, comme les incidents de contrebande dans la région de Cornwall.

M. Rick Norlock: Vous parlez des cigarettes illégales et illicites, c'est exact?

M. Gregory Lick: Ça pourrait être quelque chose comme ça. La contrebande est vraiment une chose...

M. Rick Norlock: N'ayez pas peur de le dire; je crois que nous lisons tous les journaux.

L'autre élément, bien sûr — et cela nous ramène à une question antérieure — , c'est que nous savons qu'une bonne proportion des armes à feu utilisées au Canada de façon illégale sont importées des États-Unis. « Contrebande » est le bon mot. Je me demande si c'est l'une des tâches des ESM.

Mme Nadia Bouffard: Je ne sais pas, mais je dirais que la GRC serait vraiment la mieux placée pour répondre aux questions touchant les interdictions spécifiques et l'application de ces interdictions. Elle saurait vous répondre.

M. Rick Norlock: Merci.

Certains domaines dont on a précédemment... Vous avez parlé des nouvelles ressources dont vous disposez et qui vous permettent de bien mieux faire votre travail. Nous avons le plus long littoral au monde, et nous avons l'une des plus petites populations. J'imagine que nous avons le mérite de faire un fichu bon travail pour protéger les personnes qui utilisent le littoral, que ce soit pour des raisons commerciales, de plaisance ou d'autres activités.

Puisque nous parlons de la défense nord-américaine, je me demande simplement quel genre de lien d'interopérabilité vous lie aux Forces armées canadiennes, à la GRC et à d'autres entités qui ont pour objectif d'assurer notre sécurité, ainsi qu'aux entités américaines du même genre.

Mme Nadia Bouffard: Ce sont toutes de bonnes questions.

M. Gregory Lick: En ce qui a trait à l'interopérabilité... Nous pouvons les prendre une à une, mais elles ont toutes des thèmes très similaires par rapport à notre travail.

Je dirais qu'un des meilleurs exemples de l'interopérabilité avec les Forces armées canadiennes est l'un des systèmes qui fait partie d'un projet, IMIC3, que nous sommes en train d'élaborer et d'installer à bord de navires de la Garde côtière canadienne, particulièrement à bord des plus grands navires, et sur certains des navires de la Marine royale canadienne.

Il fournit une image non classifiée à ces navires et certains centres d'opérations des Forces armées canadiennes et de la Garde côtière canadienne. Il fournit une image maritime nationale dans un format non classifié afin que la flotte et le personnel côtier puissent prendre connaissance de la situation. Cela nous permet, à nous ainsi qu'à la Marine, à mesure que nous achevons le projet, d'avoir une compréhension commune, une même image des menaces potentielles.

● (1710)

Le président: C'est tout le temps que vous aviez.

Madame Murray, allez-y, vous avez sept minutes.

Mme Joyce Murray: Merci d'être ici pour nous aider à comprendre le rôle de la Garde côtière.

Lors de témoignages précédents, nous avons posé beaucoup de questions au sujet des menaces contre l'Arctique dans le cadre de notre étude de la défense nord-américaine. Je dirais que 95 % des témoins ont répondu que les menaces sont non pas militaires, mais liées à la fonte des glaces due au changement climatique, à l'augmentation du trafic maritime, à la sûreté des personnes, donc à l'aspect de la recherche et du sauvetage, à la pollution et aux déversements potentiels, à la souveraineté, etc. Donc, c'est un aspect très important de votre travail avec vos brise-glace et d'autres mesures.

Selon le Bureau du vérificateur général, soit selon le rapport de l'automne 2014 du commissaire à l'environnement et au développement durable, il n'y a pas de réelles mesures du rendement pour les services de brise-glace dans l'Arctique ni de mesures pour les cas où des utilisateurs ont demandé un service qui n'a pas été fourni. La Garde côtière prévoit-elle mettre ces mesures en place?

Mme Nadia Bouffard: Nous avons reçu le rapport du commissaire et nous procédons actuellement à son évaluation. Nous regarderons quelles améliorations peuvent être apportées aux services de la Garde côtière dans le Nord.

Vous avez raison de dire que la qualification du risque est liée non pas à la sûreté dans le Nord, mais plutôt à toutes les autres choses dont nous avons parlé, y compris l'environnement, la population, la prestation de services, la recherche et le sauvetage...

Mme Joyce Murray: Excusez-moi, j'ai environ quatre questions, et j'espère que vous n'y répondrez pas toutes en disant que vous tenez compte du rapport.

Voici une autre préoccupation: selon le commissaire, la Garde côtière croit qu'elle dispose des ressources nécessaires pour surveiller le trafic actuel, et ce, même s'il y a eu des faiblesses au chapitre de l'intervention à certains moments et ainsi de suite. Toutefois, selon le commissaire, la Garde côtière a fait remarquer qu'elle ne possède pas les ressources suffisantes pour répondre à une augmentation de la demande de services, et nous savons que cette augmentation se produit à cause de la fonte des glaces. Le manque de ressources pour répondre à ces demandes est-il lié aux fonds inutilisés? Quel est le total des fonds inutilisés de la Garde côtière depuis 2006? Je qualifierais l'écart de récupération prévue.

Mme Nadia Bouffard: Je n'ai pas ce chiffre avec moi, mais je vais commencer par dire que l'augmentation du trafic est peut-être surévaluée aujourd'hui. Il ne fait aucun doute qu'à un certain moment nous allons devoir évaluer les ressources dont nous disposons pour assurer un service et réagir au risque accru associé à l'augmentation du trafic.

Au cours des deux ou trois dernières années, le trafic dans le Nord est passé de 250 à 350 voyages, comparativement à des millions de voyages plus au sud. Ce n'est pas une immense augmentation. Il ne fait aucun doute, toutefois, que, avec l'augmentation des activités dans le Nord, le trafic pourrait augmenter à l'avenir.

Mme Joyce Murray: Merci. Donc, il s'agit d'une augmentation de 50 %, très approximativement, dans...

Mme Nadia Bouffard: C'est dans une très grande région.

Mme Joyce Murray: Oui, et une augmentation de 50 % est une augmentation importante. J'aimerais obtenir une réponse écrite à la question sur les fonds inutilisés depuis 2006, s'il vous plaît.

Mme Nadia Bouffard: Je serai heureuse de vous la fournir.

Mme Joyce Murray: Pour ce qui est des services que vous fournissez, les brise-glace sont importants. Vos deux brise-glace les plus efficaces devraient être mis hors service dans cinq à sept ans, mais ils seront remplacés par un seul brise-glace. On dirait que vous prévoyez une réduction de la capacité de fournir du soutien à l'aide des brise-glace. Y a-t-il eu une analyse du risque que vous contrez grâce aux brise-glace, et est-elle liée à une réduction du risque, ce qui serait étrange étant donné l'augmentation du trafic? Ou le fait d'en replacer deux par un seul s'agit-il aussi d'un problème de ressources?

● (1715)

Mme Nadia Bouffard: Je vais répondre de façon générale, puis je vais demander à Greg de fournir plus de détails.

À mesure qu'on remplace la flotte, il faut continuer d'exploiter la flotte actuelle jusqu'à ce que les nouveaux brise-glace soient prêts. Nous ne considérons pas que l'arrivée de nouveaux brise-glace, comme le brise-glace polaire, par exemple, réduira notre capacité, nos ressources et notre service.

J'ai mentionné dans notre déclaration préliminaire que le brise-glace polaire actuellement en construction va être plus gros et plus efficace et nous permettra de fournir des services plus longtemps dans le Nord.

Mme Joyce Murray: Merci.

Cela soulève une autre question que je voulais poser au sujet du temps de déploiement des brise-glace. Depuis 2011, la Garde côtière a écourté de 33 jours-navire la période totale pendant laquelle elle prévoyait déployer des brise-glace dans l'Arctique. De plus, au cours de deux des quatre dernières années, la Garde côtière a déployé un brise-glace de moins que prévu dans l'Arctique en raison de problèmes d'entretien — elle possédait donc des brise-glace désuets — et elle n'a pas respecté les périodes de déploiement prévues. Si nous ne respectons pas ces périodes, qu'elles sont réduites, qu'il y a des problèmes d'entretien des navires et que nous remplaçons deux brise-glace par un seul, pouvez-vous nous expliquer comment la Garde côtière répondra aux besoins en matière de sécurité et de défense dans le Nord? Ou s'agit-il d'une question de ressources inadéquates pour effectuer le travail que l'on vous demande de faire?

Mme Nadia Bouffard: Greg est responsable d'établir chaque année nos plans annuels en matière de déploiement, donc je pense qu'il est le mieux placé pour vous expliquer comment nous déterminons le degré de service approprié.

Le président: Une réponse très brève, s'il vous plaît.

Mme Joyce Murray: D'accord, j'avais une autre question à poser, mais allez-y, répondez à cette question.

M. Gregory Lick: Merci beaucoup pour cette question.

Oui, le vérificateur général, par l'entremise du commissaire à l'environnement et au développement durable, a fait remarquer les statistiques que vous venez de souligner. Je crois qu'il est très important, par contre, de dire que nous respectons actuellement notre mandat de service dans l'Arctique, du moins à quelques journées ou à quelques heures près. C'est la statistique la plus importante à connaître à ce sujet, je crois.

En ce qui a trait au nombre de navires déployés dans l'Arctique, les navires sont comme des voitures: nous devons aussi veiller à leur entretien. Ces biens ne nécessitent pas un entretien de deux heures dans un garage. Je crois que tout le monde peut comprendre ça. L'entretien dure des mois et des mois. Lorsque nous évaluons des navires qui ont l'âge des nôtres et qui sont dans leur état actuel, ce que nous devons faire, et Mme Bouffard l'a souligné dans sa déclaration préliminaire, c'est prolonger leur vie jusqu'à ce que nous soyons en mesure de renouveler leur capacité avec un plan de renouvellement de la flotte.

Le président: Merci, c'est tout le temps que nous avions.

Monsieur Bezan, s'il vous plaît.

M. James Bezan: Merci, monsieur le président. Bienvenue à vous deux et merci d'être ici. J'ai passé beaucoup de temps dans l'Arctique, et c'est un secteur de préoccupation. Tous les Canadiens aiment l'Arctique, et sa situation actuelle favorise le développement de nouvelles occasions et de nouveaux défis. J'ai eu l'occasion d'être à bord du *Amundsen* dans la baie d'Hudson il y a quelques années et j'ai pu remarquer le superbe travail qu'il effectue là-haut en matière de cartographie et de recherche environnementale ainsi que sa prestance, lorsque nous nous sommes arrêtés à Churchill et que les gens là-bas ont pu profiter de la présence de la Garde côtière dans leur cour.

Maintenant que nous avons parlé du remplacement du *Louis S. St-Laurent*, pouvez-vous nous parler du nouveau brise-glace lourd qui va le remplacer prochainement et de ses caractéristiques par rapport aux brise-glace que nous possédons actuellement, et de la façon dont ces capacités favoriseront la protection de nos voies maritimes internationales et de notre souveraineté? Aussi, pourriez-vous nous en dire plus sur la façon dont ce nouveau brise-glace se compare à ceux des autres nations arctiques?

● (1720)

Mme Nadia Bouffard: Je vais commencer de façon très générale, mais c'est Greg, l'expert, en ce qui a trait aux navires. Ce que je comprends du nouveau brise-glace polaire que nous attendons pour 2022, c'est qu'il aura la capacité de passer de plus longues périodes dans le Nord. Il est plus résistant et plus efficace pour le déglaçage. La combinaison de ces deux éléments lui permettra d'avoir une saison de déglaçage et de prestation de services dans le Nord plus longue.

M. Gregory Lick: De plus, afin de profiter de cette plus longue saison, tant au début de la saison qu'à la fin de la saison... et nous parlons d'un total de trois mois, environ un mois et demi au début et à la fin. C'est la période de déploiement que nous visons pour ce navire en particulier. Il faut une cote glace plus élevée afin que le navire puisse fonctionner dans d'autres régions et dans des régions plus éloignées que notre flotte actuelle. C'est un autre aspect important pour que le navire puisse aller plus loin dans l'Arctique.

En ce qui a trait à votre question sur la sûreté maritime, ou sur son aspect de surveillance, je peux vous dire que nous avons été très efficaces au moment de collaborer avec tous nos partenaires de la sûreté maritime. Comme nous l'avons souligné tout au long de notre témoignage, l'élément de soutien qui fait partie du mandat de la Garde côtière a fait en sorte que nous avons travaillé avec tous nos partenaires en matière de sûreté, que ce soit la GRC ou les Forces armées canadiennes, afin de cerner quelles étaient leurs exigences pour ce type de navire dans l'Arctique. Pour vous donner un exemple, il y a un centre des opérations très complexe sur le navire, et ce centre fournira la capacité de communication et de surveillance à nos partenaires, soit les capacités dont ils ont besoin et qu'ils nous ont demandées pour le navire.

C'est comme ça que nous avons intégré les capacités au navire.

M. James Bezan: Merci.

Nous sommes aussi en train de construire de nouvelles installations où les bateaux pourront accoster et se ravitailler à Nanisivik. Comment permettront-elles à la Garde côtière d'en faire plus dans l'Arctique?

Mme Nadia Bouffard: Je suis désolée, j'ai manqué la première partie de votre question.

M. James Bezan: À Nanisivik, il y a de nouvelles installations d'accostage et de ravitaillement, qui ont été construites principalement pour la Marine, mais qui seront aussi utilisées par la Garde côtière. Comment ces installations permettront-elles à la Garde côtière d'en faire plus dans l'Arctique?

M. Gregory Lick: Essentiellement, elles nous servent exactement à ce qu'on pourrait penser. Elles nous permettent de nous ravitailler dans l'Arctique. Par le passé, le ravitaillement se faisait à l'aide de barges, par un transfert de bateau à bateau. Les nouvelles installations représentent une autre possibilité ou solution de ravitaillement pour nos navires dans l'Arctique.

M. James Bezan: Une chose dont vous n'avez pas parlé dans votre réponse, monsieur Lick, est le nouveau brise-glace qui est actuellement en construction. Du point de vue de la Garde côtière, comment ses caractéristiques se comparent-elles à celles des brise-glace des autres nations ?

M. Gregory Lick: Je le comparerais à notre flotte actuelle, ce qui pourrait vous permettre de mieux comprendre la comparaison. Nous pouvons le comparer avec un certain nombre de brise-glace en activité partout dans le monde, mais, parfois, à cause de l'âge du navire et de l'époque où il a été construit, certaines classifications sont un peu difficiles à comparer.

Essentiellement, toutefois, très sommairement, notre *Louis S. St-Laurent* est un brise-glace polaire de classe 4, environ, et ce que nous visons avec le brise-glace polaire — je vais le confirmer au comité — c'est un brise-glace polaire de classe 2. Cela vous permet de comprendre la différence entre notre flotte actuelle et les autres. Bien sûr, lorsque nous le comparons avec, disons, les brise-glace actuels de la Garde côtière américaine, le *Healy*, le *Polar Star* et ainsi de suite, il sera davantage capable que ces navires d'entrer dans certaines régions, comme je l'ai dit, des régions dans lesquelles nous ne pouvons actuellement pas entrer ou dans lesquelles nous allons très rarement; ou nous pourrons y aller plus longtemps.

Le président: Merci.

Monsieur Chisholm, s'il vous plaît, vous avez cinq minutes.

M. Robert Chisholm: Merci.

Je pense que le *Louis S. St-Laurent* a été mis en service en 1969 et qu'on a récemment laissé entendre qu'il serait mis hors service dans quatre à six ans. Mais je crois comprendre que vous allez devoir l'entretenir, parce que le nouveau brise-glace, le brise-glace polaire, ne sera pas mis en service avant 2022. Quels seront les coûts du prolongement de la vie du *Louis S. St-Laurent*, et combien de temps serez-vous en mesure de le maintenir en activités?

Ensuite, je veux revenir à ma question sur les NPEA, au sujet des navires. Formerez-vous les personnes qui exploiteront ces navires dans l'Arctique? Ou les exploiterez-vous vous-mêmes?

Ma dernière question concerne les hélicoptères Bell et le moment où nous pouvons nous attendre à ce qu'ils soient disponibles.

● (1725)

Mme Nadia Bouffard: Je vais commencer de façon très générale, et je vais demander à Greg de compléter. La Garde côtière prévoit dépenser environ 360,4 millions de dollars sur 10 ans dans un programme de prolongement de vie et de modernisation de milieu de durée de vie des navires. Donc, ce n'est pas seulement pour notre brise-glace polaire, c'est pour l'ensemble de notre flotte. Le programme a été annoncé en février 2012 et consiste en une série de mesures provisoires visant à prolonger la vie des navires de la Garde côtière canadienne. Il comprend les brise-glace actuels, afin que nous puissions assurer la continuité de la prestation des services par la flotte actuelle, et l'attente de nouveaux navires. À ce jour, nous avons dépensé environ 30 millions de dollars pour les travaux effectués.

M. Robert Chisholm: Veuillez m'excuser. Désolé. Je comprends, mais vous ne répondez pas à ma question, et nous n'avons pas beaucoup de temps. Je demanderai donc à M. Lick de répondre.

Mme Nadia Bouffard: Greg pourrait vous donner les détails au sujet du brise-glace polaire, si nous les avons. Comme je l'ai dit au début, nous ne sommes pas les experts de l'approvisionnement des navires de la Garde côtière.

M. Gregory Lick: Ce que je peux vous dire, c'est que nous nous sommes engagés à nous assurer que le NGCC *Louis S. St-Laurent* et le reste de la flotte fonctionnent... et nous investissons pour prolonger leur vie jusqu'à ce qu'ils soient remplacés. Je n'ai pas les chiffres avec moi, mais je crois que nous pouvons nous engager à vous les envoyer.

M. Robert Chisholm: Et pour les NPEA; comment allez-vous...?

M. Gregory Lick: Le projet de NPEA est évidemment un projet sur lequel nous travaillons en étroite collaboration avec la Marine royale canadienne. Plus particulièrement, je dirais que nous avons eu des échanges récents dans l'Arctique, où des officiers de navigation de la Marine royale canadienne viennent à bord de nos navires et travaillent avec nos agents pour acquérir de l'expertise et des connaissances en déglaçage, observer les glaces et connaître tous les éléments dont ils ont besoin pour naviguer de façon sécuritaire dans l'Arctique.

M. Robert Chisholm: La dernière question concernait les hélicoptères Bell. Le printemps dernier, j'ai rencontré les gens des travaux publics, et certaines questions ont été soulevées au sujet de la capacité de ces hélicoptères d'effectuer le travail demandé par la Garde côtière. Je me demandais si vous pouviez me dire ce qu'il en est.

M. Gregory Lick: Certainement, en ce qui a trait au contrat actuel d'hélicoptères légers qui a été annoncé plus tôt cette année, nous avons actuellement un contrat avec Bell Helicopter à Montréal pour la production de 15 hélicoptères légers. Ils sont en production. Ils répondent entièrement à nos exigences au chapitre des capacités que nous avons demandées dans le processus d'appel d'offres, et nous sommes certains qu'ils seront livrés à temps et conformément au budget. Nous n'avons aucune préoccupation au sujet de ce contrat.

M. Robert Chisholm: Ce contrat comprend-il d'autres hélicoptères?

M. Gregory Lick: Non. Je crois que vous auriez remarqué que, à la suite de la signature du contrat, il y a eu un autre processus pour nos hélicoptères moyens. Ce processus est toujours en cours, et l'annonce n'a pas encore été faite.

M. Robert Chisholm: D'accord.

Donc, en ce qui vous concerne, vous avez toutes les ressources nécessaires pour répondre aux besoins en matière de recherche et de sauvetage dans le Nord.

Mme Nadia Bouffard: La réponse est oui, mais comme je l'ai dit plus tôt, si le trafic augmente avec le temps, à un certain moment, nous allons devoir nous pencher là-dessus. Mais oui, actuellement, nous croyons que nous avons tout ce dont nous avons besoin.

M. Robert Chisholm: Quelle importance devrait avoir cette augmentation; y a-t-il un seuil?

Mme Nadia Bouffard: C'est une bonne question.

M. Robert Chisholm: Vous avez dit à Mme Murray qu'une augmentation de 50 % n'est pas particulièrement préoccupante, soit le fait de passer de 250 à 350 voyages. Donc, quelle...

Mme Nadia Bouffard: C'est une chose sur laquelle nous allons devoir nous pencher à l'avenir, mais, actuellement, nous croyons avoir ce dont nous avons besoin.

Le président: Je vais utiliser la prérogative du président pour poser deux ou trois dernières questions. Vous avez effleuré le sujet, et, lors de notre dernière rencontre, le vice-amiral Norman a parlé des changements et des choses à prendre en compte à l'avenir concernant l'équipage à bord des navires de la Garde côtière. Vous en avez parlé à un moment aujourd'hui, mais les installations sur les brise-glace actuels et sur le nouveau brise-glace actuellement en conception, lorsqu'on parle de rénovation temporaire ou de modernisation des navires actuels et du nouveau navire, permettront-elles d'accueillir en permanence du personnel de la Marine royale canadienne?

● (1730)

M. Gregory Lick: Monsieur le président, je crois que je comprends votre question. En ce qui a trait aux exigences pour les nouveaux brise-glace lorsqu'ils seront prêts — et le gouvernement a l'intention de les financer — c'est quelque chose que nous évaluerions avec nos partenaires. Donc, dans ce cadre, lorsque nous élaborons nos exigences, comme le fait la Marine, nous consultons nos partenaires au sujet de leurs exigences. Pour ce qui est du brise-glace polaire, par exemple — et j'en ai parlé plus tôt — nous avons parlé à nos différents partenaires de la sûreté maritime et nous leur avons demandé quelles étaient leurs exigences. Pour être honnête, je n'ai pas ce genre de détails en ma possession, mais nous pouvons vous revenir au sujet des caractéristiques du brise-glace polaire, peut-être par rapport au nombre de couchettes sur le navire.

Le président: Mais, il ne fait aucun doute que le ministère de la Défense nationale, la Marine, pour être plus précis, semble considérer la Garde côtière comme le premier répondant, et ce sera de plus en plus le cas à l'avenir, et il faudra qu'il y ait, dans le cadre de votre travail actuel avec la GRC dans les eaux plus au sud, une augmentation de la présence du personnel de la Marine royale canadienne à bord de vos navires.

M. Gregory Lick: Je viens de me souvenir du chiffre, du moins pour le brise-glace polaire. Il a une capacité d'environ 100 personnes à bord. En fait, l'équipage représente environ la moitié de ce chiffre. Les couchettes supplémentaires disponibles à bord sont destinées au personnel de différentes missions, que ce soit des missions scientifiques, de sûreté ou d'interventions environnementales. Il pourrait s'agir de toutes sortes de missions. Il y a des places supplémentaires à bord qui permettront l'exécution de ce type de missions, c'est certain.

Le président: Merci beaucoup à vous deux, madame la sous-commissaire et monsieur le directeur, d'avoir été avec nous aujourd'hui. Nous avons hâte d'en savoir plus d'ici le déploiement des nouveaux navires.

J'aimerais rappeler aux membres que, dans le cadre de notre prochaine réunion, le ministre répondra à des questions concernant le Budget supplémentaire des dépenses. Nous vous tiendrons au courant de l'emplacement de cette réunion. La greffière m'informe qu'elle aura lieu dans l'édifice du Centre. Nous nous revoyons mardi.

La séance est levée.