CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

44e LÉGISLATURE, 1re SESSION

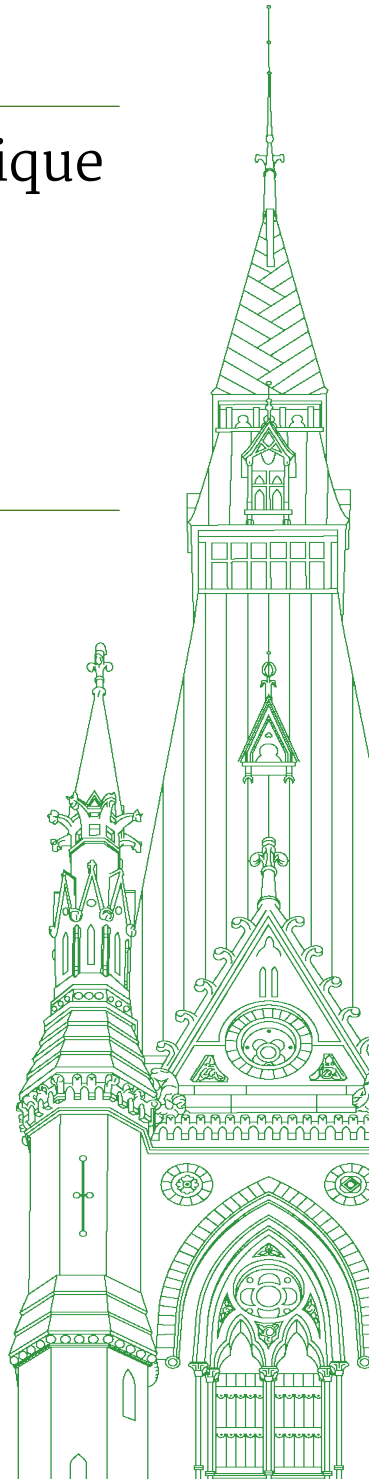
Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 037

PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY

Le jeudi 6 octobre 2022



Président : M. Ron McKinnon

Comité permanent de la sécurité publique et nationale

Le jeudi 6 octobre 2022

● (1100)

[*Traduction*]

Le président (M. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.)): Bienvenue à la 37e séance du Comité permanent de la sécurité publique et nationale de la Chambre des communes.

Nous commencerons par reconnaître que nous nous réunissons sur le territoire traditionnel non cédé du peuple algonquin.

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

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

Ce matin, nous accueillons, du ministère de la Défense nationale, le général Wayne Eyre, chef d'état-major des Forces armées canadiennes; le vice-amiral Auchterlonie, commandant du Commandement des opérations interarmées du Canada; et le major-général Michael Wright, commandant du Commandement du renseignement des Forces canadiennes et chef du renseignement de défense. Du Centre de la sécurité des télécommunications, nous accueillons Mme Caroline Xavier, chef, et M. Sami Khoury, dirigeant principal du Centre canadien pour la cybersécurité.

Merci à tous de vous joindre à nous aujourd'hui. Nous avons hâte d'entendre vos observations.

Général Eyre, je vous invite maintenant à faire votre déclaration liminaire. Vous aurez plus ou moins cinq minutes. Nous ne serons pas trop durs avec vous.

Général Wayne D. Eyre (chef d'état-major de la défense, Forces armées canadiennes, ministère de la Défense nationale): Monsieur le président, je vous remercie de me donner l'occasion de discuter de notre environnement de sécurité géopolitique, en particulier, de la menace que la Russie représente pour le Canada.

Je suis heureux d'être accompagné du vice-amiral Auchterlonie, commandant opérationnel de nos opérations internationales et nationales, ainsi que du major-général Wright, commandant du Commandement du renseignement. Je suis également très heureux d'être ici avec mes collègues du CST, Caroline Xavier et Sami Khoury, que vous avez présentés.

Nous nous trouvons de nouveau dans un monde chaotique et dangereux où de grandes puissances, notamment la Russie et la Chine, sont déterminées à refaire l'ordre mondial pour parvenir à leurs fins et où les droits et libertés des États plus petits et moins puissants sont éliminés. Nous sommes également témoins de violations du caractère sacré de la souveraineté territoriale et du dialogue responsable sur l'utilisation des armes nucléaires.

La Russie et la Chine ne font pas la distinction entre la paix et la guerre.

[*Français*]

En cherchant à atteindre leurs objectifs nationaux, elles utiliseront tous les éléments de leur puissance nationale, agissant souvent juste sous le seuil d'un conflit violent à grande échelle. Cela dit, d'après ce que nous voyons en Ukraine, elles sont bien disposées à franchir ce seuil.

La Russie et la Chine visent non seulement la survie du régime, mais aussi son expansion.

[*Traduction*]

Dans ce contexte, ces pays se considèrent comme étant en guerre avec l'Occident.

Leur plus grande menace ne vient pas d'adversaires extérieurs, mais de leur propre population. Ils s'efforcent donc de miner la cohésion sociale des démocraties libérales et la crédibilité de nos institutions, pour que notre modèle de gouvernement soit perçu comme un échec.

Nous observons un exemple de cette guerre de l'information en temps réel, où les Ukrainiens gagnent la bataille entre la vérité et le mensonge en Occident, tandis que le discours russe domine dans beaucoup d'autres régions du monde.

Aurons-nous un ordre international fondé sur des règles ou un ordre fondé sur la puissance? Ce concours, à savoir quel ordre l'emportera, définira certainement le reste de notre temps en uniforme et, en fait, le reste de nos vies.

[*Français*]

Beaucoup de nos alliés et partenaires sont lucides à l'égard de ce qui menace notre avenir.

Nous devons l'être nous aussi.

L'enjeu est de taille.

Nous ne pouvons pas permettre à des puissances autoritaires de changer l'ordre mondial pour arriver à leurs fins.

● (1105)

[*Traduction*]

Nous devons être forts. Nous devons travailler avec nos partenaires et alliés et faire front commun pour éviter un mauvais calcul, tout en décourageant l'aventurisme et une guerre entre les grandes puissances.

En ce qui concerne notre propre sécurité nationale, la distance et l'isolement géographique dont le Canada bénéficie depuis longtemps ne constituent plus une stratégie défensive viable. En 2021, le Canada et les États-Unis ont convenu d'investir dans la modernisation du NORAD, qui est nécessaire depuis longtemps. Cependant, la Russie a elle aussi fait des investissements importants, y compris dans l'aviation à long rayon d'action et dans la capacité des missiles de croisière que transportent ses avions.

La Russie peut également représenter une menace pour le Canada dans d'autres domaines, non seulement le domaine maritime, mais aussi dans les domaines cybernétique et spatial, où elle a la capacité de menacer nos réseaux, notre infrastructure critique, nos communications et notre économie.

[*Français*]

Enfin, il y a la menace nucléaire, répétée de façon à peine voilée à de nombreuses reprises ces derniers temps.

À l'heure actuelle, nous ne pensons pas que la Russie compte utiliser des armes nucléaires stratégiques contre le Canada. Le déroulement de la crise en Ukraine et l'escalade possible nous obligent toutefois à la vigilance.

[*Traduction*]

La menace russe est très claire. Heureusement, les mesures qu'il faut prendre pour contrer cette menace sont également claires. En plus de nous préparer à la possibilité d'un conflit ouvert dans les domaines traditionnels, il faut développer notre capacité de gérer des affrontements dans les domaines cybernétique, spatial et cognitif.

Nous devons intégrer nos capacités dans tous les domaines. En matière de sécurité nationale, il faut élaborer une approche intégrée combinant des interventions militaires, des actions diplomatiques, ainsi que des mesures économiques et d'information à l'échelle locale, régionale, nationale et multinationale.

[*Français*]

Nous devons maintenir un avantage sur le plan intellectuel en générant diverses options et idées stratégiques au moyen d'un dialogue continu entre les alliés, les organisations, les industries, le milieu universitaire et les gouvernements. Ce sera crucial pour maintenir notre avantage stratégique.

[*Traduction*]

Nous ne devons pas être naïfs en ce qui concerne les menaces dans le monde. D'après nos adversaires, un compromis constitue une faiblesse devant être exploitée. Ils ne respectent que la force et ne réagissent qu'à cela.

L'ordre international fondé sur des règles, qui sous-tend depuis des générations la stabilité mondiale et, en effet, notre prospérité nationale, est maintenant incertain. Il doit être défendu. Nous devons tous être conscients de la gravité de ce moment.

Merci. Nous serons heureux de répondre à vos questions.

Le président: Merci, général.

J'invite maintenant Mme. Xavier à faire sa déclaration préliminaire.

Mme Caroline Xavier (chef, Centre de la sécurité des télécommunications): Bonjour. Je vous remercie, monsieur le président et membres du Comité, de m'avoir invitée à vous parler de la posture de sécurité du Canada par rapport à la Russie.

Je suis Caroline Xavier, et mon pronom est elle. Je suis la nouvelle chef du Centre de la sécurité des télécommunications, appelé le CST.

Je suis accompagnée aujourd'hui par Sami Khoury, dirigeant principal du Centre canadien pour la cybersécurité du CST, ou le cybercentre, comme vous l'avez déjà entendu.

Je suis heureuse de me joindre à vous. J'aimerais moi aussi prendre un moment pour reconnaître que la terre d'où je me joins à vous aujourd'hui est un territoire traditionnel non cédé de la nation algonquine Anishinabe.

[*Français*]

Je vais vous présenter une brève mise à jour sur le rôle du CST pour assurer la posture de cybersécurité du Canada par rapport à la Russie, et je vais vous donner de l'information sur les récentes activités du CST pour protéger les Canadiens de ces menaces.

[*Traduction*]

Le CST, qui relève de la ministre de la Défense nationale, est l'un des principaux organismes canadiens de sécurité et de renseignement. La Loi sur le Centre de la sécurité des télécommunications, ou Loi sur le CST, énonce cinq aspects de notre mandat, soit la cybersécurité et l'assurance de l'information, le renseignement étranger, les cyberopérations défensives, les cyberopérations actives et l'assistance technique et opérationnelle. Dans le cadre de ce mandat, le CST est l'autorité technique nationale du Canada en matière de cybersécurité.

[*Français*]

Le Centre canadien pour la cybersécurité est un secteur au sein du CST et un centre d'expertise unique pour toutes les questions techniques et opérationnelles en matière de cybersécurité.

[*Traduction*]

Permettez-moi de vous donner un aperçu des principales conclusions sur le contexte actuel des cybermenaces, particulièrement en ce qui concerne la Russie. Je tiens à souligner que cette année le CST a publié quatre bulletins sur des activités de cybermenaces et de désinformation parrainées par la Russie.

● (1110)

[*Français*]

Tout d'abord, voici quelques cybermenaces auxquelles le Canada doit faire face à l'heure actuelle. Nous présentons ces menaces plus en détail dans notre Évaluation des cybermenaces nationales, que je vous encourage à consulter pour avoir une meilleure compréhension du contexte des menaces.

[*Traduction*]

Dans cette évaluation, nous concluons que le cybercrime est la menace la plus courante et la plus répandue contre les Canadiens et les entreprises canadiennes. Des cybercriminels cherchent à s'infiltrer dans les systèmes canadiens. Ils proviennent, entre autres, de la Russie, de la Chine et de l'Iran. Ces auteurs de menace s'appuient sur diverses techniques, comme le rançongiciel, le vol de données personnelles et la fraude en ligne. Les exploitants d'infrastructures essentielles et les grandes entreprises constituent les cibles les plus profitables.

Bien que la cybercriminalité soit la menace la plus susceptible de toucher le Canadien moyen, les programmes de cyberopérations parrainés par des États, notamment la Chine, la Corée du Nord, l'Iran et la Russie, représentent les menaces stratégiques les plus importantes pour le Canada. Les activités de cybermenaces perpétrées par des États étrangers, dont la Russie, ciblent les exploitants de réseaux de l'infrastructure essentielle du Canada, de même que leurs technologies opérationnelles et technologies de l'information.

[*Français*]

La Russie possède d'importantes cybercapacités et a montré dans le passé qu'elle pouvait les utiliser à mauvais escient. On pense notamment à la cybercompromission de SolarWinds, aux perturbations visant les efforts d'élaboration de vaccins contre la COVID-19, aux menaces contre le processus démocratique en Géorgie et au maliciel NotPetya.

[*Traduction*]

En plus des défis à la cybersécurité canadienne soutenus par la Russie, comme je l'ai mentionné, les campagnes de désinformation russes menacent également le Canada et les Canadiens. En juillet de cette année, le Centre de la sécurité des télécommunications, CST, a fait savoir qu'il avait continué d'observer de nombreuses campagnes de désinformation en ligne soutenues par la Russie visant à appuyer l'invasion brutale et injustifiable de l'Ukraine par la Russie.

[*Français*]

Maintenant que je vous ai présenté les principales tendances et menaces, je vais vous donner un aperçu des façons dont le mandat du CST nous aide à résoudre ces problèmes.

Le CST possède des capacités techniques et opérationnelles uniques qui lui permettent d'intervenir lorsque surviennent divers types de menaces contre le Canada, notamment les auteurs de menaces d'États hostiles.

[*Traduction*]

Le programme de renseignement électromagnétique étranger du CST fournit des capacités perfectionnées qui nous permettent d'accéder aux cybermenaces actuelles et émergentes, de les traiter, de les décrypter et de rendre des comptes sur ces cybermenaces. Nous utilisons ensuite ces renseignements pour informer le gouvernement et les diffuser.

[*Français*]

Le renseignement étranger que le CST recueille nous permet de transmettre cette information non seulement aux propriétaires et aux exploitants de l'infrastructure essentielle au Canada, mais aussi à nos alliés, à nos partenaires de l'Organisation du Traité de l'Atlantique Nord, ou OTAN, et à l'Ukraine.

[*Traduction*]

Le fait de disposer de ces renseignements avant qu'une menace se matérialise leur permet de protéger et de défendre leurs systèmes de manière proactive. La Loi sur le CST nous permet en outre de fournir une assistance technique et opérationnelle aux partenaires fédéraux en matière d'application de la loi, de sécurité et de défense, notamment le ministère de la Défense nationale, les Forces armées canadiennes, la GRC et le Service canadien du renseignement de sécurité, ou SCRS. Cela signifie que le CST est autorisé à aider les FAC à soutenir les missions militaires autorisées par le gouvernement, comme l'opération Unifier. Cela comprend l'échange de renseignements et la cybersécurité.

[*Français*]

L'un des principaux rôles du CST est d'informer le gouvernement au sujet d'activités d'entités étrangères qui menacent le Canada ou ses alliés. Parmi ces menaces, il y a les cybermenaces étrangères, l'espionnage, le terrorisme, et même les campagnes de désinformation.

[*Traduction*]

Par exemple, depuis le début de l'invasion de l'Ukraine par la Russie, nous avons observé de nombreuses campagnes de désinformation en ligne soutenues par les Russes, qui visent à discréditer et à diffuser des renseignements erronés sur les alliés de l'OTAN, ainsi que de faux récits sur la participation du Canada dans le conflit russo-ukrainien.

[*Français*]

Par exemple, les médias contrôlés ont reçu l'ordre d'inclure des images trafiquées de membres des Forces canadiennes en première ligne et de fausses allégations selon lesquelles les Forces canadiennes commettent des crimes de guerre.

[*Traduction*]

Nous avons diffusé ces renseignements sur Twitter dans le cadre des efforts du gouvernement du Canada pour aider à informer les Canadiens sur la façon d'arrêter la propagation de la désinformation et de s'en protéger.

Nous continuerons de travailler en étroite collaboration avec nos partenaires du Groupe des cinq, de même que de mettre à contribution notre expertise pour assurer en toute confiance la résilience du Canada face aux menaces en termes de cybersécurité ou de désinformation.

[*Français*]

Malgré le niveau de sophistication toujours plus élevé de la désinformation et des auteurs de cybermenaces de la Russie, je peux vous assurer que nous travaillons sans relâche pour relever la barre en matière de cybersécurité au Canada et pour protéger tous les Canadiens contre les menaces émergentes.

[*Traduction*]

Nous disposons de l'expertise nécessaire pour surveiller, détecter et enquêter sur les menaces potentielles. Nous renforçons les capacités et les moyens supplémentaires pour prendre des mesures actives de protection, de dissuasion et de défense contre ces menaces.

● (1115)

[*Français*]

Nous continuons également à publier des avis et des conseils qui permettent aux Canadiens et aux entreprises canadiennes d'améliorer leurs pratiques en matière de cybersécurité.

[*Traduction*]

Nous continuerons de collaborer étroitement avec nos alliés du Groupe des cinq et de l'OTAN pour protéger l'infrastructure essentielle, les économies et les systèmes démocratiques de notre pays.

Sur ce, je serai ravi de répondre à vos questions.

[*Français*]

Je vous remercie.

[*Traduction*]

Le président: Merci, madame Xavier.

Nous allons commencer notre série de questions avec Mme Dancho.

La parole est à vous pour six minutes, je vous prie.

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

Merci beaucoup aux témoins d'être ici. C'est un honneur de les avoir ici.

Général Eyre, c'est un honneur de vous rencontrer en personne. Merci de tout ce que vos collègues et vous faites pour assurer la sécurité des Canadiens. J'ai quelques questions à vous poser.

J'ai passé en revue certains des médias que vous avez utilisés au cours des derniers mois. Je suis assez préoccupée par certaines des choses que vous avez racontées aux Canadiens sur l'état de nos forces armées et notre préparation militaire.

En mai 2022, vous avez mentionné, « Compte tenu de la détérioration de la situation mondiale, nous avons besoin que l'industrie de la défense se place sur un pied de guerre et augmente ses lignes de production ». Vous avez poursuivi en disant: « Nous sommes confrontés à une situation de sécurité dans le monde qui est aussi dangereuse, voire plus dangereuse, que la fin de la guerre froide. » Vous avez également déclaré: « Le Canada est loin d'être aussi en sécurité qu'il l'était autrefois. »

Tout au long de l'étude que nous avons menées, nous avons compris que depuis la fin de la guerre froide, notre infrastructure et les capacités de défense qui accompagnaient notre infrastructure du NORAD ont été négligées, tout comme notre armée canadienne, peut-être.

Pouvez-vous nous dire ce que vous en pensez, compte tenu du contexte de ce que vous dites sur la façon dont nous sommes peut-être dans une situation plus dangereuse que durant la guerre froide?

Gén Wayne D. Eyre: Monsieur le président, je pense que les observations que la députée me prête se reflètent également dans ma déclaration liminaire au sujet de l'urgence de la situation en matière de sécurité à laquelle nous sommes actuellement confrontés. Je suis préoccupé par le fait qu'au fur et à mesure que les menaces à la sécurité mondiale augmentent et que les menaces au pays augmentent, notre état de préparation diminue au sein des Forces armées canadiennes.

C'est la raison pour laquelle nous avons entrepris ce que nous appelons la reconstitution. La reconstitution est une opération militaire qui est utilisée après une opération à grande échelle pour reconstruire, réarmer et rééquiper.

La pandémie n'a pas été clémente pour les Forces armées canadiennes, car nos effectifs ont diminué. Nous nous engageons dans un effort prioritaire pour rétablir nos chiffres en matière de recrutement et de maintien en poste, afin de pouvoir assurer cette préparation.

L'état de préparation ne se limite pas aux personnes. L'état de préparation repose également sur la formation, l'équipement et le maintien en puissance. Nous travaillons également dans ces trois autres secteurs pour nous assurer que nous pouvons fournir l'état de préparation essentiel pour répondre rapidement et à grande échelle aux besoins des Canadiens. Nous avons beaucoup de travail qui nous attend.

Mme Raquel Dancho: Merci, général.

On vous a également cité dans le *Toronto Star* aujourd'hui, où vous dites que le processus de reconstruction doit être accéléré et que les lacunes dont vous avez parlé aujourd'hui empêchent les Forces armées canadiennes, plus précisément, « d'être dans la position où elles doivent être pour exceller en tant que force militaire moderne et prête au combat ». De plus, vous avez dit qu'au final, ces pénuries de personnel « compromettent l'état de préparation et la santé à long terme des capacités de défense du Canada ».

Pouvez-vous préciser vos propos pour le Comité et expliquer à quel point la situation est sérieuse? À quel point le gouvernement fédéral doit-il prendre au sérieux ces investissements qui sont clairement essentiels à notre sécurité nationale?

Gén Wayne D. Eyre: Monsieur le président, c'est un défi auquel non seulement toutes les armées occidentales sont confrontées, mais nous y sommes également confrontés ici, chez nous, avec des défis en matière de main-d'oeuvre et des défis réels dans ce domaine. Cela se reflète dans nos propres chiffres. Je suis très inquiet au sujet de nos chiffres. C'est pourquoi nous faisons de la reconstitution de notre armée un effort prioritaire.

Ce que nous faisons plus précisément, c'est que nous examinons notre système de recrutement. Nous avons doté notre système de recrutement à 100 %. Nous rationalisons le système de recrutement. Nous avons mis en place une stratégie de rétention. Il y a beaucoup d'autres choses sur lesquelles nous continuons à travailler pour nous assurer que la qualité du service offert à nos membres est ce qu'elle doit être.

Soyons réalistes, personne ne s'engage dans l'armée pour devenir riche. Ce que nous offrons est quelque chose de transcendant. C'est la possibilité de servir son pays. Nous devons nous assurer que la qualité du service s'étend à des aspects tels que la sécurité financière de nos membres et de leurs familles, un équipement de qualité, afin qu'ils puissent travailler sur de l'équipement moderne, une infrastructure de qualité qu'ils peuvent avoir, et un emploi intéressant, ce qui signifie des déploiements importants à l'étranger ainsi qu'un emploi valorisant ici au Canada.

● (1120)

Mme Raquel Dancho: Merci, général.

Pouvez-vous parler de l'importance d'atteindre nos engagements de dépenses de 2 % pour l'OTAN? Est-ce un niveau adéquat? Devrions-nous atteindre cette cible rapidement, ou à un rythme accéléré, comme vous l'avez dit?

Gén Wayne D. Eyre: Monsieur le président, je ne suis pas en mesure de parler des détails de nos dépenses de défense et de tout objectif arbitraire.

Je vous dirais que l'armée que nous avons à l'heure actuelle n'est pas l'armée dont nous avons besoin pour gérer les menaces qui se présenteront dans le futur. Nous devons continuer d'examiner et d'évaluer ces menaces et nous assurer d'avoir les capacités voulues pour contrer ces menaces émergentes.

Mme Raquel Dancho: Général, dans ma dernière minute, diriez-vous que le Canada est prêt à toute éventualité pour se défendre?

Gén Wayne D. Eyre: Monsieur le président, « toute éventualité » est une description très générale de l'environnement de sécurité. Nous devons tenir compte des probabilités, car l'imagination peut s'emballer.

Mme Raquel Dancho: J'allais simplement dire que quand la guerre a éclaté en Ukraine avec l'invasion russe, j'ai justement posé cette question à notre ministre de la Défense, la ministre Anand. Je lui ai demandé si le Canada était prêt à faire face aux menaces que la Russie fait peser non seulement sur l'Ukraine mais sur le monde entier et sur ceux qui aident à défendre l'Ukraine. Elle a répondu que le Canada était prêt à faire face à toute éventualité. À la lumière de vos commentaires et de ce que nous avons appris au cours de cette étude, je crains fort que ce ne soit pas le cas.

Pendant les quelques secondes qui me restent, pouvez-vous nous dire ce qu'il faut faire aujourd'hui et dans les mois à venir pour être prêts à faire face à l'éventualité la plus probable, ou à toute éventualité?

Gén Wayne D. Eyre: Monsieur le président, comme je l'ai dit, nous devons nous reconstruire et rehausser notre état de préparation afin de disposer de suffisamment de militaires pour pouvoir réagir à la vitesse requise. C'est ce sur quoi nous nous concentrons en ce moment, sur les quatre éléments de la préparation dont j'ai parlé.

Mme Raquel Dancho: Merci beaucoup, monsieur.

Le président: Merci, madame Dancho.

Nous passons maintenant à M. Chiang pour six minutes, s'il vous plaît.

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

Je tiens à remercier tous les témoins de prendre le temps d'être ici avec nous aujourd'hui.

Ma question s'adresse au général Eyre.

Le directeur de la CIA, William Burns, a récemment déclaré que bien que la CIA n'ait vu aucune preuve tangible que Poutine se rapproche de l'utilisation d'armes nucléaires tactiques, nous devons prendre la chose très au sérieux et surveiller les signes de préparation réelle.

À quoi ressembleraient de tels préparatifs en Russie, et quelle devrait être la réponse du Canada si cela se produisait?

Gén Wayne D. Eyre: Monsieur le président, c'est une chose que nous surveillons de près nous aussi. Il y a tout lieu de nous inquiéter de la possibilité d'une escalade. Cela dit, nous ne pouvons pas laisser la coercition nucléaire nous empêcher de faire ce que nous avons à faire. D'autres acteurs observent la situation, et cela deviendra un modèle à l'avenir.

Pour ce qui est des détails, je vais laisser le général Wright vous donner un peu plus de contexte.

Major-général Michael Wright (commandant, Commandement du renseignement des Forces canadiennes et chef du renseignement de la Défense, ministère de la Défense nationale): Monsieur le président, je suis absolument d'accord avec le directeur de la CIA pour dire que la Russie en a la capacité. Le Groupe des cinq et nos alliés de l'OTAN cherchent maintenant avant tout à déterminer si elle a l'intention de mettre sa menace à exécution.

En ce qui concerne les indicateurs, il s'agit évidemment d'une question à laquelle le Groupe des cinq accorde la plus grande attention. Nous suivons de près les indicateurs et les avertissements. C'est toutefois un sujet très sensible, et je ne pense pas que nous puissions en discuter ici.

M. Paul Chiang: Merci beaucoup.

Que savons-nous des politiciens russes qui demandent la destitution de Poutine et de l'accusation de haute trahison que certains ont portée contre lui? Le Canada suit-il ces développements internes de quelque façon que ce soit?

Gén Wayne D. Eyre: Je demanderais d'abord au général Wright de répondre à cette question.

Mgén Michael Wright: Monsieur le président, nous suivons de près tous les aspects du conflit avec la Russie, et nous le faisions avant même l'invasion, lorsque Vladimir Poutine mentait ouvertement en disant qu'il ne s'agissait que d'un exercice militaire. Nous essayons de vérifier ses intentions, mais aussi d'évaluer la force de l'État russe et le soutien dont il bénéficie.

Ce que je dirais, c'est que Vladimir Poutine a passé plus de 20 ans à consolider le pouvoir de l'État autour de lui et d'un très petit groupe de conseillers.

Mme Caroline Xavier: Si vous le permettez, monsieur le président, je n'ajouterais qu'une chose.

C'est le CST qui administre le programme national de renseignement électromagnétique sur l'étranger, ainsi nous fournissons des renseignements afin que les décideurs de haut niveau puissent avoir une idée des activités, des motivations, ainsi que des capacités et des intentions de nos adversaires étrangers, y compris de ceux que vous avez mentionnés.

C'est à peu près tout ce dont nous pouvons discuter ce matin.

M. Paul Chiang: Merci beaucoup.

Plus la guerre progresse en Russie et en Ukraine, plus la Russie semble désespérée d'annexer certaines régions de l'Ukraine et de revendiquer des victoires dans la région. Dans ce contexte, croyez-vous que les cybermenaces que la Russie fait peser sur le Canada augmentent, diminuent ou restent les mêmes, et pourquoi?

● (1125)

Mme Caroline Xavier: Monsieur le président, puis-je réentendre la question?

M. Paul Chiang: Bien sûr.

Plus la guerre progresse en Russie et en Ukraine, plus la Russie semble désespérée d'annexer certaines régions de l'Ukraine et de revendiquer des victoires dans la région. Dans ce contexte, croyez-vous que les cybermenaces que la Russie fait peser sur le Canada augmentent, diminuent ou restent les mêmes?

Mme Caroline Xavier: Merci de cette question, monsieur le président.

Ce que nous constatons, c'est que la Russie continue de multiplier les menaces et d'évoquer ses capacités cybernétiques; elle montre sa volonté de les utiliser. Depuis le début ou la mi-janvier, nous avons publié plusieurs bulletins. Nous diffusons de l'information sur les menaces proférées par la Russie et les vulnérabilités qu'elle aime exploiter, ainsi que des conseils et des directives sur la façon de les atténuer.

Dans notre « Évaluation des cybermenaces nationales », nous exposons notre point de vue sur les acteurs étatiques hostiles, dont la Russie fait partie. Par conséquent, nous avons des inquiétudes, mais ne savons pas si ces menaces se concrétiseront ou non. Cela dit, nous estimons que la Russie ne dirigerait peut-être pas ces cybermenaces directement contre nous et nos infrastructures essentielles, étant donné que nous ne sommes pas directement impliqués dans le conflit. Cependant, nous continuons de surveiller la situation et d'enquêter, pour déterminer si nous devons ou non conseiller des mesures à prendre.

M. Paul Chiang: Merci beaucoup.

Encore une fois, cette question s'adresse à Mme Xavier.

Lorsque vous parlez d'acteurs étatiques hostiles, pensez-vous que la Russie est impliquée de quelque façon que ce soit dans le conflit qui oppose actuellement l'Azerbaïdjan et l'Arménie?

Mme Caroline Xavier: Je ne peux pas vous parler choses dont la cote de sécurité ne me permet pas d'en discuter dans cet environnement non classifié; cependant, comme je l'ai mentionné, nous continuons de travailler en étroite collaboration avec nos alliés et à surveiller ce qui se passe dans le monde en ce qui concerne les acteurs étatiques hostiles.

Comme nous l'indiquons dans l'« Évaluation des cybermenaces nationales », nous constatons que la Russie est l'un des acteurs à disposer des moyens de pointe nécessaires pour déployer ses cyberprogrammes. Par conséquent, nous sommes très inquiets, et nous travaillons avec nos alliés à cet égard pour cerner les menaces, prodiguer les conseils nécessaires et fournir des renseignements aux décideurs pour qu'ils puissent prendre les mesures nécessaires.

M. Paul Chiang: Merci beaucoup.

Le président: Merci, monsieur Chiang.

[*Français*]

Madame Michaud, vous avez la parole pour six minutes.

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

Je remercie les témoins d'être avec nous aujourd'hui. Je leur en suis reconnaissante.

Ma première question s'adresse à Mme Xavier.

Madame Xavier, j'ai pris connaissance d'un article publié dans le *Journal de Montréal* en mai 2022. On y retrouve plusieurs chiffres concernant le Centre de la sécurité des télécommunications. Selon cet article, depuis l'invasion russe, le nombre de cyberattaques a grimpé de 16 % dans le monde entier. En 2021, le nombre d'attaques par rançongiciel a bondi de 151 % par rapport à 2020, également dans le monde entier. À lui seul, le Canada a essuyé 235 attaques connues.

Au bénéfice des membres du Comité, pourriez-vous nous expliquer pourquoi ces données ne sont pas toutes connues?

Vous disiez que cela représentait la pointe de l'iceberg, mais que les attaques ne sont pas toutes déclarées. Pourquoi ne le sont-elles pas toutes ? Devrions-nous davantage encourager les organisations victimes d'une attaque à le signaler?

Selon ce que je comprends, il n'y a rien de contraignant pour le moment. Toutefois, cela pourrait certainement être utile pour toutes les organisations susceptibles d'être victimes d'une attaque.

Qu'en pensez-vous?

Mme Caroline Xavier: Je vous remercie de la question.

Nous aimerions, bien sûr, que le Canada soit immunisé contre les cybermenaces, et notre organisation a pour but d'essayer de s'assurer que toutes les organisations et tous les Canadiens sont sensibilisés à la nécessité de prêter attention à la manière dont ils gèrent leurs données.

Comme vous l'avez mentionné, nous observons une augmentation des attaques par rançongiciel. C'est pourquoi nous travaillons de manière très étroite avec les industries, avec les différents paliers de gouvernement et avec les Canadiens. Nous cherchons à les informer et à les sensibiliser.

Nous travaillons également de façon étroite avec des organisations qui nous rapportent avoir été victimes de cyberattaques. Cependant, comme vous l'avez dit, plusieurs organisations ne le signalent pas. Nous continuons tout de même à en discuter ouvertement avec les industries.

Nous organisons beaucoup de séances d'information et de sensibilisation visant à les informer du fait que nous sommes là pour leur offrir le soutien nécessaire. Nous publions aussi beaucoup de bulletins d'information pour leur expliquer les risques, afin qu'elles se protègent et qu'elles préviennent les attaques possibles.

Cela nous inquiète, évidemment. Or, le Canada n'est pas le seul pays à souffrir du fait que plusieurs organisations ne veulent pas divulguer les attaques dont elles sont victimes. Nous en discutons avec tous nos alliés dans le monde, et nous continuons à mentionner aux organisations qu'il est important de nous contacter. Nous savons comment être discrets, en plus de savoir comment travailler avec elles pour les aider à trouver la solution à leur problème.

● (1130)

Mme Kristina Michaud: Je vous remercie, madame Xavier.

Général Eyre, je vous remercie de votre allocution d'ouverture. Je vous ai trouvé très honnête. Il est rafraîchissant d'avoir des gens qui viennent nous donner l'heure juste, même si certains propos peuvent parfois être effrayants. Je parle notamment de ce que vous avez dit concernant le fait que des pays comme la Russie et la Chine sont prêts à tout pour servir leurs propres intérêts.

Si je ne m'abuse, vous avez dit que vous ne craigniez pas que le Canada soit la cible d'une attaque nucléaire lancée par la Russie. Certains experts que nous avons reçus au Comité n'ont toutefois pas hésité à comparer l'arme nucléaire à l'arme cybernétique.

Si vous ne craignez pas une attaque nucléaire, craignez-vous des attaques cybernétiques, ce qui pourrait avoir des conséquences très importantes pour le Canada?

Gén Wayne D. Eyre: Je vous remercie beaucoup de la question.

Il est difficile de faire une comparaison exacte entre les deux menaces, soit les cyberattaques et les attentats nucléaires, mais les deux posent une menace pour notre pays et nous devons être prêts à y répondre.

Je voudrais céder la parole au major-général Wright, du Commandement du renseignement des Forces canadiennes, pour qu'il nous fasse part de ses commentaires.

Mgén Michael Wright: Je vous remercie.

La Russie a assurément la capacité de lancer des cyberattaques et de cibler les structures critiques au Canada. Il est aussi important de se rappeler que la Russie considère l'Amérique du Nord comme une cible. Elle ne fait pas de distinction entre les États-Unis et le Canada.

En ce qui concerne le sujet précis des cyberattaques, notre expert en la matière, ici, c'est la cheffe du CST.

Mme Kristina Michaud: Je vous remercie, major-général Wright.

C'est très intéressant, ce que vous dites sur l'Amérique du Nord en tant que cible unique. Je comprends que l'Amérique du Nord n'est pas dans la même situation que l'Ukraine, en ce moment. Tout de même, nous pourrions craindre les contrecoups à cause, notamment, des sanctions économiques qui ont été imposées à la Russie autant par le Canada que par les États-Unis.

Croyez-vous que nous sommes bien préparés, à l'heure actuelle, pour faire face aux cyberattaques, si jamais il devait y en avoir?

Gén Wayne D. Eyre: Je vous remercie de la question.

Il est toujours difficile de se préparer en cas d'attaque nucléaire. Nous devons continuer de travailler avec nos collègues du Commandement de la défense aérospatiale de l'Amérique du Nord, ou NORAD, afin qu'ils nous envoient un avertissement dans l'éventualité d'une attaque.

En fait, il est difficile de se préparer pour les conséquences d'une telle attaque. Selon moi, nous devons continuer d'accroître notre résilience nationale pour tous les types de désastres...

[*Traduction*]

M. Tony Van Bynen (Newmarket—Aurora, Lib.): J'invoque le Règlement, monsieur le président, je n'entends pas l'interprétation.

Le président: Merci, monsieur Van Bynen. Nous allons vérifier cela.

● (1135)

M. Tony Van Bynen: Très bien. Je vous entends en anglais maintenant.

Le président: Eh bien, je m'exprime en anglais en ce moment, donc...

Général, si vous pouviez reprendre votre réponse depuis le début, nous vous laisserons un peu plus de temps en conséquence.

[*Français*]

Gén Wayne D. Eyre: Comme je le disais, il est difficile de se préparer pour une attaque nucléaire, parce que les conséquences sont immenses.

D'après moi, nous devons continuer d'accroître notre résilience nationale pour répondre aux différents types de désastres.

En même temps, nous devons continuer de travailler étroitement avec nos collègues américains du NORAD. Selon nous, il est primordial que nous recevions les avertissements du NORAD dans l'éventualité d'une attaque sur notre continent.

[*Traduction*]

Le président: Madame Michaud, je pense que vous avez encore une minute.

[*Français*]

Mme Kristina Michaud: J'aimerais poser une dernière et brève question.

Nous pouvons nous inquiéter des menaces que représente la Russie, en ce moment.

Toutefois, considérant le fait que plus de 80 % des forces russes sont actuellement consacrées à l'invasion de l'Ukraine, pouvons-nous nous permettre d'être moins inquiets au sujet de la capacité de la Russie pour ce qui est d'attaquer, peu importe la façon, que ce soit un autre pays ou l'Amérique du Nord?

Par ailleurs, il ne faudrait pas sous-estimer cette capacité que pourrait avoir la Russie.

N'est-ce pas?

Gén Wayne D. Eyre: C'est une excellente observation. Je dois cependant dire que, même si la Russie a déployé la majeure partie de sa force terrestre, il lui reste beaucoup d'autres forces. En effet, il ne faut pas oublier la force aérienne, la force navale et la force stratégique. Par conséquent, la menace est toujours là.

Le président: Je vous remercie, madame Michaud.

[*Traduction*]

Nous allons maintenant passer à M. MacGregor pour six minutes, s'il vous plaît.

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

Je remercie les témoins d'être ici. Je sais à quel point votre temps est précieux, et notre comité vous remercie sincèrement d'être ici aujourd'hui.

Général Eyre, j'aimerais commencer par vous.

Nous avons pu observer, en Ukraine, ce qu'il est possible d'accomplir lorsqu'une force de combat déterminée bénéficie d'une formation occidentale et d'un arsenal occidental. Je pense que nous avons tous été assez ébahis par les capacités de l'armée ukrainienne.

En même temps, je pense que cela nous donne l'occasion d'en apprendre davantage sur les capacités militaires russes, la doctrine de combat de l'armée russe, le moral de ses troupes, etc. Nous savons, de sources d'information publiques, que les Russes ont essuyé de sérieux revers au cours du dernier mois.

Je sais que le Canada et tous ses alliés de l'OTAN prêtent attention à ce conflit. De manière générale, qu'avons-nous appris de ce conflit sur la capacité militaire russe, et comment la doctrine de l'OTAN évolue-t-elle à partir de cette évaluation?

Gén Wayne D. Eyre: Monsieur le président, je remercie le député de sa question.

Je vais dire quelques mots et ensuite donner au vice-amiral Auchterlonie, qui surveille cela au quotidien, la chance de faire quelques observations.

Je dirais que la volonté de vaincre que nous observons au sein des forces ukrainiennes est probablement le facteur déterminant de leur succès.

Nous avons été très heureux de voir les forces ukrainiennes prendre pleinement ce que nous appelons le commandement des missions, c'est-à-dire prendre le leadership sur le terrain, pour pouvoir improviser, tirer parti de la situation locale et créer le succès. Nous ne voyons pas cela du côté russe. Les Russes sont très attachés à la vieille mentalité soviétique, au style de commandement descendant et centralisé. C'est l'un des grands constats que nous faisons.

Nous avons remarqué des failles du côté russe, sur le plan stratégique, pour aligner les fins, les moyens et les ressources. Leurs moyens et leurs ressources militaires ne sont pas à la hauteur de leurs objectifs politiques. Nous constatons une déconnexion, en ce sens qu'ils sont constamment en train de réviser leurs objectifs. Encore aujourd'hui, nous doutons que leurs objectifs maximalistes soient réalisables.

Nous avons également constaté des problèmes systématiques dans leurs forces, notamment pour ce qui est de l'entraînement et de la capacité à intégrer des ressources interarmes, c'est-à-dire que l'artillerie, le génie et les forces aériennes travaillent ensemble. Ce n'est tout simplement pas le cas. Leurs lacunes logistiques sont assez importantes.

Nous avons appris, au sein de nos forces, à quel point l'autonomisation d'une force très motivée et le fait de lui donner les pouvoirs et les ressources nécessaires pour agir sur le terrain peuvent être puissants. Nous insistons là-dessus.

Je suis très fier de l'entraînement que nos forces ont reçu depuis 2015 et de la façon dont elles arrivent à transmettre ce style de leadership jusque sur le terrain. Cet entraînement se poursuit aujourd'hui dans le cadre de l'opération Unifier.

Sur ce, je cède la parole au vice-amiral Auchterlonie.

● (1140)

Vice-amiral J.R. Auchterlonie (commandant du Commandement des opérations interarmées du Canada, ministère de la Défense nationale): Merci, monsieur le président.

Merci, chef.

Comme le chef l'a souligné, nous menons l'opération Unifier depuis 2015, dans le cadre de laquelle nous formons nos partenaires des forces armées ukrainiennes en collaboration avec nos alliés (les États-Unis, le Royaume-Uni, la Lituanie et d'autres pays) pour faire en sorte qu'ils aient cette capacité et la formation nécessaire pour tirer le maximum de leurs capacités sur le terrain.

Je me fais vraiment l'écho des commentaires de mes collègues. Les forces armées ukrainiennes sont exceptionnellement impressionnantes, elles sont déterminées à se battre pour leur pays. C'est très impressionnant.

Vous avez parlé des leçons essentielles qu'on tire de tout cela. Il est évident que nous tirons des leçons de ce conflit. Nous avons appris des Ukrainiens en 2015. Dans le Donbass, nous avons tiré beaucoup d'enseignements de 2015 et modifié nos tactiques et procédures au sein de l'OTAN, du Canada et avec nos alliés. Nous apprenons aujourd'hui bien des choses contre les forces russes.

Il y a toutefois une chose sur laquelle je dois vous mettre en garde, c'est que nous apprenons des choses, mais les Russes et les Chinois en apprennent aussi. Le Comité doit être attentif à cela. Le fait est que nous ne sommes pas les seuls à apprendre de ces événements.

On voit qu'il y a une grande cohésion au sein de l'Occident, c'est phénoménal, et la cohésion au sein de l'OTAN est fantastique. Je pense que nos adversaires dans le monde entier le voient et qu'ils vont y réagir. Donc nous allons apprendre au fur et à mesure. Nous sommes une institution qui apprend. Les autres organisations vont également en tirer des enseignements.

M. Alistair MacGregor: Merci.

J'aimerais poser une autre question à la cheffe du CST. Il ne me reste que quelques minutes.

Vous connaissez sûrement le projet de loi C-26 du gouvernement, qui permettra de désigner des systèmes critiques et les fournisseurs de services critiques et qui apporte des modifications assez importantes à la Loi sur les télécommunications. Vous avez parlé des campagnes de désinformation, un phénomène que notre comité connaît très bien. Nous en avons beaucoup parlé pendant notre étude sur l'extrémisme violent à caractère idéologique.

Mis à part ce qu'on trouve dans le projet de loi C-26, je m'intéresse à la relation de travail du CST avec les entreprises de médias sociaux. Pouvez-vous nous décrire cette relation et nous dire à quoi les décideurs politiques et les législateurs doivent prêter attention afin de vous faciliter un peu plus la tâche dans cette relation?

Mme Caroline Xavier: Merci pour cette question, monsieur le président. Je vous en suis très reconnaissante.

Nous avons un excellent programme de partenariat avec l'industrie, le milieu universitaire et les organisations de médias sociaux en matière de cybersécurité. Je refilerai en fait cette question au chef du centre pour la cybersécurité, parce qu'il travaille avec eux pratiquement tous les jours.

M. Sami Khoury (dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Merci de cette question, monsieur le président.

Comme l'a souligné la cheffe, nous avons une très bonne relation de travail avec de nombreuses entreprises technologiques, dont les entreprises de médias sociaux. La nature de notre relation avec ces entreprises consiste à nous assurer de bien comprendre ce qu'elles font pour réduire les cybermenaces et comment nous pouvons faciliter la coopération au cas où nous aurions besoin de leur aide pour traquer des cyberactes ou des cybermenaces. Telle est la nature de notre relation avec les entreprises de cybertechnologie.

Nous avons également publié quelques documents, surtout cette année, pour aider les Canadiens à repérer les fausses informations ou du moins, à savoir où trouver des informations crédibles et comment repérer certains types de campagnes de désinformation. C'est l'approche que prend le centre pour la cybersécurité pour lutter contre la désinformation, dans ses relations avec les entreprises technologiques.

Le président: Il vous reste neuf secondes. Merci, monsieur MacGregor.

Cela conclut le premier tour. Nous en ferons un deuxième, mais nous ne pourrons pas faire un deuxième tour complet. Chaque parti n'aura de temps que pour une série de questions. Nous commençons par M. Lloyd, qui disposera de cinq minutes.

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

Merci à tous les témoins d'être ici.

Monsieur, compte tenu de ce que vous avez dit sur les problèmes de recrutement et de maintien en poste au sein des Forces canadiennes et de la gravité de ces problèmes du point de vue de notre état de préparation, je me demande si vous pouvez nous dire quels sont les obstacles à l'inclusion des résidents permanents dans les Forces armées canadiennes. Sont-ils d'ordre philosophique, législatif ou opérationnel?

Gén Wayne D. Eyre: Monsieur le président, c'est une excellente question.

À l'heure actuelle, il n'y a pas d'obstacles de ce type pour les résidents permanents. Nous sommes sur le point de rendre l'information beaucoup plus publique pour attirer ce segment de la population dans nos rangs.

M. Dane Lloyd: Je n'étais pas au courant. Je vous remercie de le dire. Je sais, pour avoir parlé avec des recruteurs, que bien des Néo-Canadiens ou des résidents permanents veulent servir le pays parce qu'ils aiment notre pays. C'est une bonne chose que nous trouvions des moyens de les inclure ici.

Monsieur, l'un des défis que nous observons au Canada atlantique — ous l'avons vu à Abbotsford l'année dernière —, c'est que la capacité des Forces canadiennes à réagir aux catastrophes est limitée, mais qu'elles jouent un rôle de plus en plus important en première ligne. Je me demande si vous pouvez nous faire part de votre point de vue sur les avantages, peut-être, ou les difficultés qu'il y aurait à nous doter d'une force de protection civile composée de civils, qui serait un multiplicateur de force pour soutenir les militaires dans ce genre de situations.

● (1145)

Gén Wayne D. Eyre: Monsieur le président, c'est une autre question qui nous tient à cœur dans l'examen de notre capacité d'intervention.

Permettez-moi d'abord de dire que notre priorité absolue est de protéger les Canadiens ici, au pays. Lorsque nous recevons un appel, nous mettons tout le reste de côté pour nous assurer d'être en mesure d'intervenir rapidement. Cela dit, compte tenu de la fréquence et de l'intensité croissantes des catastrophes naturelles, on nous demande de plus en plus d'intervenir pas nécessairement en dernier recours, mais parfois, comme force de premier recours.

De quoi aurions-nous besoin? De ressources supplémentaires. Celles-ci pourraient venir des services municipaux ou provinciaux. Cela dit — et je l'ai déjà dit publiquement —, étant donné l'ampleur des catastrophes auxquelles nous sommes confrontés, nous devons toujours demeurer cette force de dernier recours. Les Forces canadiennes doivent toujours être là, être la police d'assurance ultime pour le Canada lorsque les ressources manquent.

Ce que nous fournissons, et que toute autre organisation devrait pouvoir fournir, c'est un bassin de main-d'œuvre qualifiée et organisée, pleinement autonome pour s'approvisionner lui-même, se déplacer par ses propres moyens, assurer son propre commandement et contrôle et s'occuper de lui-même. C'est là toute la véritable valeur de ce que nous avons à offrir. Toute organisation similaire, toute organisation supplémentaire, devrait avoir les mêmes attributs.

M. Dane Lloyd: Cette question concerne l'étude en cours.

Comme nous le savons, des intervenants étatiques étrangers tentent de cibler nos infrastructures essentielles. Pouvez-vous nous en expliquer les raisons? Est-ce simplement en raison de l'intensité et de la fréquence de ces catastrophes que les Forces canadiennes sont sollicitées plus fréquemment ou est-ce parce que nous avons observé une dégradation de nos autres capacités et que cela mène les Forces canadiennes... ? Nos capacités non militaires sont-elles en train de se dégrader ? Est-ce la raison pour laquelle les Forces canadiennes sont sollicitées ? Pourquoi cela se produit-il ?

Gén Wayne D. Eyre: Encore une fois, monsieur le président, c'est une excellente question.

Nous pourrions discuter de ces autres capacités. Ont-elles réellement existé ou devraient-elles exister? Vous parlez aussi des attaques contre nos infrastructures essentielles. Dans le cadre de notre réflexion sur la dissuasion, nous pouvons réfléchir à la façon de dissuader ces attaques. L'une des notions ou l'un des sous-éléments de la dissuasion, c'est la dissuasion par le déni. Cela signifie que les attaques des adversaires ne sont pas fructueuses et qu'ils ne tenteront donc pas de nous attaquer du tout. Si nous pouvons cerner ces points de défaillance uniques, si nous pouvons prouver la capacité de notre société et de notre nation à contrecarrer l'intention de ces attaques, elles ne se produiront peut-être pas du tout.

Nos adversaires cherchent des cibles faciles, comme nous l'avons appris au cours d'opérations menées dans le monde entier. Si nous présentons une cible facile, nous nous exposons à une attaque.

M. Dane Lloyd: Je vous remercie.

Dans les 30 secondes qu'il me reste, j'aimerais seulement mentionner que si je me souviens bien, le général Omar Bradley a dit que les amateurs étudient la stratégie et les professionnels étudient la logistique. Je pense que nous pouvons voir que les compétences logistiques de la Russie sont en train de s'effondrer sur le front ukrainien. Que peut faire le Canada pour renforcer ses compétences logistiques à l'avenir?

Gén Wayne D. Eyre: Monsieur le président, c'est un autre sujet de préoccupation. En effet, au cours de la pandémie, nous avons notamment constaté que notre propre chaîne d'approvisionnement interne et notre système de maintien en puissance interne ont besoin d'améliorations.

Actuellement, dans le cadre de nos efforts, nous travaillons notamment sur une initiative qui consiste à renforcer notre capacité à répondre à nos propres besoins et à renforcer nos compétences logistiques. Ce travail est en cours, mais il faut de la main-d'œuvre, de la technologie et de l'équipement pour y arriver. Compte tenu de la nature et de la géographie de notre pays et de l'endroit où nous nous trouvons dans le monde, il faut un niveau élevé de compétences logistiques pour pouvoir envoyer nos capacités là où elles sont nécessaires à l'échelle internationale, mais aussi à l'échelle nationale. Nous devons donc continuer à investir dans ce domaine.

Le président: Je vous remercie, monsieur Lloyd.

Monsieur Noormohamed, vous avez cinq minutes.

M. Taleeb Noormohamed (Vancouver Granville, Lib.): Je vous remercie, monsieur le président.

J'aimerais me faire l'écho des commentaires de mes collègues et vous remercier tous du travail que vous faites pour assurer la sécurité du Canada. Nous vivons dans un monde complexe, et nous vous sommes reconnaissants de tous les efforts que vous déployez à cet égard.

Général, dans votre déclaration préliminaire, vous avez parlé de l'importance des démonstrations de force. Nous savons que nous ne serons jamais la plus grande force de combat dans le monde. Nous ne ferons pas les investissements les plus importants dans l'armée. Selon vous, à quoi doit ressembler la force dont vous parlez?

● (1150)

Gén Wayne D. Eyre: Monsieur le président, je suis fermement convaincu que l'avantage concurrentiel dont dispose notre pays réside dans le fait qu'il appartient à un groupe d'amis, d'alliés et de partenaires aux vues similaires — enfin, aux vues suffisamment similaires — qui ont suffisamment de valeurs communes pour pouvoir s'opposer ensemble à l'agression, à l'aventurisme et aux politiques expansionnistes. Il est donc extrêmement important de collaborer avec ces partenaires, ces alliés et ces amis, tout comme il est important de participer à cette démonstration de force et à ces efforts de dissuasion collectifs.

M. Taleeb Noormohamed: Je vous remercie.

La deuxième partie de votre conclusion m'a frappé. Vous avez dit que notre mode de vie « doit être défendu ». À quoi ressemble cette défense, selon vous?

Gén Wayne D. Eyre: Monsieur le président, à mon avis, cela signifie s'engager dans le monde de façon responsable, soutenir nos amis et alliés lorsqu'ils ont besoin de soutien, faire notre part pour les soutenir, être prêts à les soutenir et faire preuve de transparence quant à nos intentions.

Inutile de se le cacher: c'est l'ordre international fondé sur des règles qui est en place depuis la fin de la Deuxième Guerre mondiale qui sous-tend notre prospérité nationale et notre croissance économique. À mon avis, je crois qu'il vaut la peine d'être défendu.

[*Français*]

M. Taleeb Noormohamed: Madame Xavier, vous avez longuement parlé de la cybercriminalité parrainée par l'État et de la menace que la Russie représente pour notre mode de vie et le tissu de notre société canadienne par la propagation de la désinformation.

Sur la base de votre travail et de ce que vous avez vu, pouvez-vous nous parler des répercussions de ces menaces sur le Canada?

Mme Caroline Xavier: Je vous remercie de la question.

J'aimerais confirmer que j'ai bien compris votre question.

Vous me demandez de commenter ce que j'ai vu, sur la base de mon travail.

Est-ce cela?

M. Taleeb Noormohamed: Je parle de ce que vous avez vu dans le cadre de votre travail.

Je sais qu'il y a de l'information classifiée et que vous ne pouvez pas discuter de cela avec nous. Parmi les menaces dont vous pouvez discuter, quelles sont celles que vous avez pu observer et quelles en ont été les répercussions sur le Canada?

Mme Caroline Xavier: Je vous remercie de la question.

Ce que je peux vous dire, c'est que la Loi sur le Centre de la sécurité des télécommunications nous autorise à procéder à des interruptions à l'aide des outils mis à notre disposition, afin de nous protéger et de nous assurer que nos systèmes sont capables de se défendre contre les menaces en question. Ce que nous essayons de faire, c'est de continuer à nous assurer que nos systèmes peuvent se défendre contre ce type de menaces.

Comme il a été mentionné plus tôt, nous travaillons en étroite collaboration avec nos partenaires internationaux, surtout ceux qui font partie du Groupe des cinq.

Nous nous assurons d'avoir la capacité de connaître les types de menaces existantes afin de pouvoir transmettre l'information aux Canadiens et aux entreprises qui en ont besoin. Il s'agit de protéger non seulement les systèmes gouvernementaux, mais aussi les systèmes critiques qui sont essentiels à la gestion du Canada.

[*Traduction*]

M. Taleeb Noormohamed: Vous avez également mentionné — et c'était presque un commentaire en passant — que vous avez dû recourir à Twitter pour expliquer quelque chose aux Canadiens.

Comment les intervenants du CST ont-ils dû changer leur façon de concevoir la lutte contre la désinformation dans leurs propres activités et, en particulier, dans leur façon de parler aux Canadiens?

Pendant très longtemps, personne ne savait ce qu'était le CST, et tout le monde s'en portait bien. Lorsque j'étais un jeune fonctionnaire, quelqu'un a essayé de me recruter au CST, et je n'avais aucune idée de ce qu'était cet organisme. Aujourd'hui, vous avez adopté une position plus publique, car c'est nécessaire dans le monde dans lequel nous vivons. Comment cela a-t-il changé la façon dont vous informez les Canadiens de ce qu'ils doivent savoir, et qu'est-ce que cela implique pour votre organisme?

Mme Caroline Xavier: Je vous remercie beaucoup de votre question. Je vous en suis très reconnaissant.

Vous avez raison de dire que nous avons dû envisager les choses sous un angle différent. Nous avons dû modifier notre façon de travailler. Nous sommes très fiers d'avoir pu faire ce changement catégorique sur la question de l'utilisation de Twitter et de la déclassification de certains renseignements pour pouvoir les communiquer aux Canadiens, mais aussi aux alliés qui combattent… avec les partenaires qui sont en Ukraine. C'est sans précédent.

Nous n'avons jamais eu à faire ces choses auparavant, mais nous continuons d'explorer tous les moyens possibles d'informer les Canadiens des menaces existantes sans perturber notre façon de procéder ou de fonctionner.

Nous sommes en terrain inconnu, et nous continuerons donc à explorer les possibilités à cet égard. Nous avons utilisé quelques méthodes qui se sont révélées efficaces dans cet espace, par exemple lorsque nous avons déclassifié des renseignements et que avons veillé à diffuser des renseignements exacts et à encourager les gens à mettre l'accent sur ces renseignements exacts.

● (1155)

M. Taleeb Noormohamed: Je vous remercie beaucoup.

Je vais partager le temps qu'il me reste.

Le président: Je vous remercie, monsieur Noormohamed.

[*Français*]

Madame Michaud, vous avez la parole pour deux minutes et demie.

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

Général Eyre, vous avez dit tout à l'heure que le Canada avait peut-être quelque chose à craindre et que, en tant que pays de l'Amérique du Nord surtout, il pourrait représenter une cible.

Par ailleurs, n'a-t-il pas plus à craindre que les autres pays en raison de sa vaste frontière septentrionale avec la Russie, dans l'Arctique?

J'imagine que oui, mais pourriez-vous nous donner plus de détails sur la façon dont vous prêtez attention à l'Arctique dans vos discussions avec les États-Unis, par exemple, et avec l'OTAN ou le NORAD?

De quelle façon prêtez-vous une attention particulière à ce qui pourrait survenir en Arctique?

Gén Wayne D. Eyre: Je vous remercie de la question.

Nous devons continuer à nous concentrer sur l'Arctique pour protéger notre souveraineté, pas seulement aujourd'hui, demain ou au cours des prochaines semaines, mais bien pendant la prochaine décennie.

Les menaces quant à notre souveraineté ne sont pas très critiques pour l'instant, mais, dans la prochaine décennie, elles pourraient s'aggraver. Nous devons donc investir pour protéger nos capacités dans chaque domaine, que ce soit sur terre, en mer, dans l'air, dans l'espace ou dans le cyberespace.

En ce qui concerne nos opérations actuelles, je vais passer la parole au commandant du Commandement des opérations interarmées, M. Auchterlonie.

Vam J.R. Auchterlonie: Je vous remercie.

C'est un grand défi pour les Forces armées canadiennes.

[*Traduction*]

Nous faisons face à certains défis dans le Nord. L'un d'entre eux est la formation, comme l'a souligné le général. Il y a également des défis en matière d'infrastructure et de capacité dans le Nord. Il est difficile de gérer tout cela en raison de l'immensité de la région.

En ce qui concerne plus précisément la formation, nous offrons chaque année de la formation dans la région. Nous observons une augmentation constante de la formation offerte dans tous les domaines dans le Nord, avec la participation des forces terrestres, maritimes et aériennes, ainsi que celle de nos alliés et partenaires du monde entier. Nous effectuons une série d'exercices annuels pour nous assurer que nous sommes en mesure de mener nos activités dans le Nord, car il s'agit d'un environnement très hostile.

Comme je l'ai dit, la consolidation de cette infrastructure, de ce soutien, de cette formation et de ces exercices nous permet de disposer des capacités nécessaires dans le Nord pour soutenir les Canadiens.

[*Français*]

Mme Kristina Michaud: Général Eyre, ma prochaine question ne porte pas sur une menace contre le Canada en particulier, mais sur une menace susceptible de perturber l'ordre mondial.

Il a été question de la Chine et de la Russie, mais il y a des États, au Conseil de sécurité et à l'Assemblée générale des Nations unies, qui se sont abstenus de voter sur une motion qui visait à condamner l'annexion de territoires ukrainiens par la Russie.

Craignez-vous que ces États puissent s'unir à des États comme la Russie et la Chine pour perturber davantage l'ordre mondial dans les prochaines années?

Gén Wayne D. Eyre: Je vous remercie de la question.

Effectivement, certains États, autoritaires pour la plupart et amis ou clients de grands pays puissants comme la Russie et la Chine, adoptent la même position que ces derniers sur le monde.

Il y a aussi des pays qui ne veulent pas s'unir avec l'Ouest ou des pays autoritaires. Ils veulent protéger leur espace stratégique et pouvoir prendre les décisions qu'ils jugent nécessaires pour protéger leurs intérêts.

Mme Kristina Michaud: Je vous remercie.

● (1200)

Le président: Je vous remercie, madame Michaud.

[*Traduction*]

La parole est maintenant à M. MacGregor. Il a deux minutes et demie.

Vous avez la dernière série de questions.

M. Alistair MacGregor: Je vous remercie, monsieur le président.

J'ai seulement une question pour les représentants du CST. Nous parlons de cybercriminalité. J'aimerais me concentrer sur la cybercriminalité qui vient de la Russie.

Nous savons que de nombreuses entreprises canadiennes craignent que les attaques ou les menaces dont elles font l'objet soient rendues publiques. En effet, une telle chose pourrait nuire à leur réputation, car cela pourrait entraîner une perte de confiance chez les investisseurs et miner l'image de ces entreprises.

Je sais qu'il s'agit d'un véritable défi pour votre organisme, mais pourriez-vous décrire à notre comité les types de profils que vous observez en ce qui concerne les organismes ou les individus qui lancent ce genre d'attaques? S'agit-il d'organismes criminels vaguement affiliés en Russie? Quel type de relation ces organismes entretiennent-ils avec l'État russe? Observez-vous une sorte de stratégie coordonnée?

Je sais qu'une grande partie de ces renseignements sont probablement confidentiels, mais pourriez-vous les décrire de façon assez générale pour notre comité?

Mme Caroline Xavier: Je vous remercie, monsieur le président, de cette question.

Comme il a déjà été mentionné, nous ne pouvons pas parler des détails, mais ce que nous pouvons divulguer, c'est que lorsque nous prenons connaissance des caractéristiques d'un cybercriminel ou de son profil et que nous sommes en mesure de déclassifier ces renseignements, nous voulons certainement les communiquer à l'industrie.

C'est ce qui est arrivé dans le communiqué que nous avons publié en janvier dernier. Nous avons informé le secteur privé de ce que la Russie pouvait être en mesure de faire dans le domaine des infrastructures essentielles, juste pour donner un avertissement général sur ce dont il faudrait s'inquiéter, car nous savons que ce pays peut opérer de manière sophistiquée.

En ce qui concerne les États hostiles en général et pas seulement la Russie en particulier, lorsque nous comprenons un profil, comme celui que nous avons observé pour la Russie, nous fournissons aux intervenants de l'industrie les conseils nécessaires pour qu'ils puissent corriger leurs systèmes afin d'éliminer toute vulnérabilité et pour qu'ils exercent une surveillance accrue à cet égard. C'est l'autre élément qui est réellement important, c'est-à-dire qu'il faut toujours vérifier si les choses se déroulent comme prévu.

Nous proposons régulièrement des séances d'information, ainsi que des communiqués dans lesquels nous formulons des conseils. Dès que nous sommes en mesure de fournir des renseignements qui sont transparents au public, nous le faisons.

Cela revient à la question posée plus tôt sur la façon dont nous n'épargnons aucun effort pour trouver des moyens de déclassifier les renseignements et de les rendre publics, afin que les gens soient informés de ce que les Russes sont potentiellement capables de faire.

Malheureusement, c'est à peu près tout ce que je peux dire.

M. Alistair MacGregor: D'accord. Bien entendu.

Je vais terminer en remerciant encore une fois chacun d'entre vous d'avoir comparu aujourd'hui. Je vous en suis reconnaissant.

Le président: Je vous remercie, monsieur MacGregor.

C'est ce qui met fin à nos séries de questions.

Au nom du Comité, je tiens à remercier tous les témoins de nous avoir accordé du temps aujourd'hui. Nous savons que vous êtes des gens très occupés, et nous vous sommes donc reconnaissants d'avoir comparu aujourd'hui. Vous nous avez beaucoup aidés, et je vous en remercie.

Nous allons maintenant suspendre la séance pour nous réunir à huis clos. Les membres du Comité qui participent virtuellement à la réunion devraient avoir reçu un lien pour la partie à huis clos.

Nous allons donc suspendre la séance pendant cinq minutes.

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

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

PERMISSION DU PRÉSIDENT

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

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

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

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

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

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

SPEAKER'S PERMISSION

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

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

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

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

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