CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

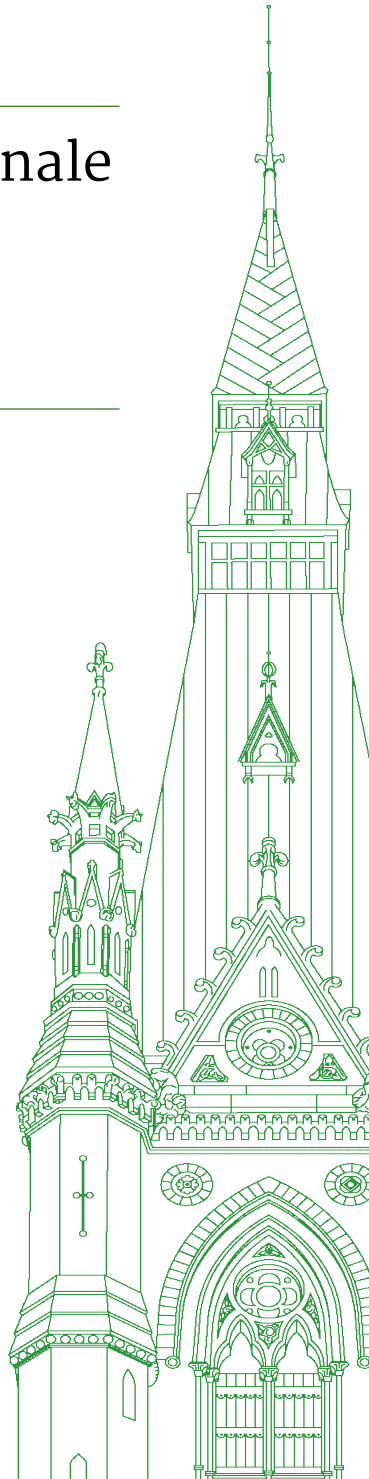
44e LÉGISLATURE, 1re SESSION

Comité permanent de la défense nationale

TÉMOIGNAGES

NUMÉRO 050

Le mardi 14 février 2023



Président : L'honorable John McKay

Comité permanent de la défense nationale

Le mardi 14 février 2023

● (1530)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Je déclare la séance ouverte.

Nous accueillons aujourd'hui l'une des personnes qui témoignent le plus souvent devant notre comité, soit M. Quinn. Bienvenue à nouveau.

Nous accueillons également l'amiral Carosielli. Bienvenue à vous également.

Vous ferez tous les deux une déclaration préliminaire de cinq minutes.

Avant de vous demander de le faire, je veux dire à mes collègues que nous prévoyons discuter de la question du ballon — à défaut d'un meilleur terme — vendredi. Nous avons presque la confirmation de la part des autorités compétentes qu'elles comparaîtront vendredi matin. Je le dis dans le contexte où, aujourd'hui, vous voudrez peut-être grandement poser des questions sur le sujet. J'encourage les membres du Comité à attendre à vendredi pour le faire.

De plus, nous avons presque la confirmation que la ministre comparaîtra peu de temps après.

Cela dit, est-ce que c'est l'amiral Carosielli ou M. Quinn qui fera la déclaration préliminaire?

Vous disposez de cinq minutes, monsieur Quinn.

M. Jonathan Quinn (directeur général, Politique de défense continentale, ministère de la Défense nationale): Merci beaucoup, monsieur le président. Je vais faire quelques observations, puis je céderai la parole à l'amiral Carosielli, qui en ajoutera quelques-unes.

Merci beaucoup de m'avoir invité à témoigner dans le cadre de votre étude sur la cybersécurité et la cyberguerre.

Je m'appelle Jon Quinn et j'occupe le poste de directeur général de la Politique de défense continentale au ministère de la Défense nationale. La cyberpolitique fait partie de mon portefeuille.

Le cyberespace est devenu un domaine important dans le contexte d'une concurrence stratégique mondiale croissante. Il est à la base des systèmes et des infrastructures auxquels non seulement le MDN et les FAC, mais aussi tous les Canadiens ont recours quotidiennement pour le travail, la vie personnelle et les services essentiels.

Les cybermenaces sont répandues, et les auteurs de menace étatiques et non étatiques investissent davantage dans leurs cybercapacités et le développement de celles-ci. Dans ce contexte, nos partenaires et alliés font également évoluer leurs cybercapacités militaires au moyen d'investissements importants et de partenariats entre des organismes militaires et civils pour être mieux à même de se défendre contre les menaces et de promouvoir leurs intérêts.

Parallèlement à la croissance des cybermenaces, nous devons examiner les possibilités qu'offrent les cybercapacités. Les cybercapacités sont un outil stratégique que le gouvernement du Canada peut utiliser pour atteindre ses objectifs dans les domaines des affaires étrangères, du renseignement et de la défense.

Le cyberespace est devenu un autre domaine d'opérations militaires et de sécurité nationale, qui se caractérise par une concurrence constante en deçà du seuil qui attire tant les alliés que les adversaires. Le conflit en Ukraine montre que les cybercapacités jouent un rôle essentiel dans la guerre moderne.

Conformément à la politique de défense du Canada — « Protection, Sécurité, Engagement » —, les FAC doivent adopter une posture plus délibérée dans le cyberdomaine, mettre sur pied des cybercapacités offensives et les utiliser contre des adversaires potentiels à l'appui des missions militaires autorisées par le gouvernement.

[*Français*]

À mesure que nous développons les cybercapacités militaires et menons des opérations, le Canada assure aussi un leadership sur la scène mondiale pour favoriser un comportement responsable de la part des États dans le cyberespace.

L'année dernière, le Canada a publié la « Déclaration du Canada sur le droit international applicable dans le cyberespace », laquelle expose notre position sur cette question.

De plus, les cyberopérations des Forces armées canadiennes respectent toutes les lois nationales pertinentes et sont assujetties à un système éprouvé de contrôles et de contrepoids qui assure une surveillance complète et une responsabilisation.

[*Traduction*]

Le MDN et les FAC sont résolus à saisir les occasions offertes par le cyberespace d'une façon responsable. Ils continueront de travailler pour l'avancement des capacités de leurs cyberforces militaires afin de mener des cyberopérations de façon autonome avec les alliés et d'autres ministères fédéraux et, ainsi, de mieux protéger le Canada contre les cybermenaces.

Merci. Je cède maintenant la parole au contre-amiral Carosielli.

Contre-amiral Lou Carosielli (commandant de la Force cybernétique, Forces armées canadiennes, ministère de la Défense nationale): Je vous remercie de l'invitation, monsieur le président.

Je suis le contre-amiral Carosielli, commandant de la force cybernétique des Forces armées canadiennes. C'est pour moi un grand honneur d'être ici aujourd'hui et d'avoir l'occasion de vous informer du travail exceptionnel qu'accomplissent nos militaires et nos civils pour défendre le Canada dans le cyberdomaine.

Le cyberespace est essentiel dans la conduite des opérations militaires modernes et est considéré par le Canada et ses alliés comme un domaine d'opérations militaires, un véritable domaine de combat, et j'y reviendrai plus tard.

Par conséquent, les FAC s'en remettent à l'effet multiplicateur de force qu'ont les systèmes de communication, de renseignement et d'armes axés sur la technologie, qui doivent être adéquatement sécurisés et protégés contre les cybermenaces. Les FAC défendent leurs propres réseaux et systèmes d'information contre les auteurs de cybermenaces et appuient leurs partenaires et leurs alliés selon leurs capacités.

Nos adversaires ont démontré qu'ils disposaient de capacités de cyberespionnage et de cyberattaque de pointe qu'ils peuvent utiliser en cas de concurrence, de crise et de conflit.

[*Français*]

En effet, nos adversaires potentiels mettent à profit le développement des cybercapacités pour tenter d'exploiter des vulnérabilités de nos systèmes de commandement, de contrôle, de communication, d'informatique, de renseignement, de surveillance et de reconnaissance.

En plus de la menace que représentent les puissances étrangères, divers auteurs de menaces aux différentes motivations, comme les cybercriminels, les cybermilitants, les groupes terroristes, les amateurs de sensation forte et les agents internes, continuent d'utiliser des moyens de plus en plus complexes pour perturber nos réseaux.

Les cyberforces des Forces armées canadiennes contribuent à la paix et à la sécurité internationale à l'aide du partage de renseignement sur les cybermenaces avec ses alliés et ses partenaires et de la conduite de la gamme complète des cyberopérations autorisées par le gouvernement du Canada.

Par exemple, en réponse à l'agression perpétrée par la Russie, au début de 2022, les Forces armées canadiennes ont immédiatement mis sur pied une cyberforce opérationnelle pour aider l'Ukraine à renforcer ses cybercapacités de défense.

● (1535)

[*Traduction*]

Le Canada fournit à l'Ukraine une expertise en cybersécurité, des renseignements sur les cybermenaces, des outils logiciels et des solutions techniques qui lui permettent de mieux défendre ses réseaux contre la cyberactivité malveillante.

La menace ne se limite pas à l'Ukraine, et donc, en réponse à une demande de soutien de la part de la Lettonie, les FAC ont déployé une cyberforce opérationnelle pour mener des opérations conjointes de repérage des menaces afin d'aider ce pays à mieux se défendre contre les menaces et de démontrer l'engagement du Canada envers ses alliés.

Les leçons tirées de l'expérience de détection des activités d'adversaires en Lettonie sont utilisées pour mieux protéger les réseaux de la défense nationale du Canada et représentent donc un rendement considérable du capital investi.

M. Quinn et moi serons heureux de répondre à vos questions, monsieur le président.

Le président: Merci.

Pour commencer le premier tour, dont les interventions seront de six minutes, je cède la parole à Mme Kramp-Neuman.

Mme Shelby Kramp-Neuman (Hastings—Lennox and Addington, PCC): Merci.

Je vous remercie de votre présence. Merci de participer à notre réunion d'aujourd'hui.

Permettez-moi de parler brièvement du sujet tabou, soit du ballon dans le contexte la cybernétique. Des responsables de la cybernétique au sein des FAC ont-ils participé à des discussions ou ont-ils été consultés au sujet d'un quelconque cyberrisque lié aux quatre objets qui ont été abattus par le Commandement de la défense aérospatiale de l'Amérique du Nord, ou NORAD, au cours des deux dernières semaines?

Cam Lou Carosielli: La force cybernétique participe à tous ces types de discussions quant a l'échange de renseignements et de renseignements liés à la cybernétique. Les cyberforces ont donc participé aux discussions, mais, comme vous l'avez su hier, nous ne menons pas ces discussions.

Mme Shelby Kramp-Neuman: Dans un autre ordre d'idées, vous avez parlé tout à l'heure de la politique « Protection, Sécurité, Engagement ». On y indique que la Force régulière augmentera ses effectifs de 3 500 personnes, pour un total 71 500 militaires, et que cette croissance permettra de réaliser des investissements essentiels dans des domaines importants, comme l'espace et le cyberespace. Nous croyons comprendre que cela ne s'est pas produit. La crise du recrutement et du maintien en poste a-t-elle retardé les investissements dans la cyberforce?

Cam Lou Carosielli: Comme vous le savez, la reconstitution des FAC et le recrutement sont une priorité pour les Forces armées canadiennes. De plus, nous nous efforçons d'améliorer notre culture, d'accroître les effectifs et de représenter la diversité du Canada et de sa population. Nous déployons des efforts pour accélérer le recrutement en veillant à ce que nos systèmes soient numérisés et simplifiés et à ce que nous puissions procéder avec efficacité.

En ce qui concerne les cyberforces, en 2017, le poste de cyberopérateurs a été créé. Je suis heureux de pouvoir dire qu'au cours des trois dernières années, nous avons atteint tous nos objectifs de recrutement de cyberopérateurs. Nous n'avons pas eu à déployer de stratégies de recrutement de cyberopérateurs, car nous n'avons aucun problème à pourvoir ces postes. Les Forces armées canadiennes génèrent des cyberopérateurs et répondent aux besoins généraux des Canadiens à l'échelle du pays.

Mme Shelby Kramp-Neuman: Merci.

Compte tenu de la nature unique du rôle de la force cybernétique, a-t-on envisagé de l'exempter des exigences liées au principe d'universalité du service, par exemple de l'exigence d'être en bonne condition physique?

Cam Lou Carosielli: Des discussions ont eu lieu au sujet de l'universalité du service dans le cas des cyberopérateurs et d'autres métiers. Comme vous le savez peut-être, l'universalité du service est très importante pour les Forces armées canadiennes, car elle garantit que nos membres sont en mesure de participer à des opérations, et les cyberopérateurs participent à des opérations.

À ce stade-ci, il n'a pas été beaucoup question d'exemptions. Nous avons des cyberopérateurs qui peuvent devenir des fonctionnaires et mener des cyberopérations du côté de la fonction publique pour aider l'équipe du ministère de la Défense nationale et des Forces armées canadiennes.

● (1540)

Mme Shelby Kramp-Neuman: Excellent. Merci.

Pour revenir à la politique « Protection, Sécurité, Engagement », on y indique « que les Forces armées canadiennes doivent tenir compte de leurs capacités de supériorité spatiale alors qu'elles continuent à développer le programme spatial de la Défense du Canada ».

Le Canada possède-t-il la technologie et le personnel nécessaires pour le faire aujourd'hui?

Cam Lou Carosielli: Votre question porte sur les capacités de supériorité spatiale, madame. Puisque ce n'est pas mon portefeuille, je ne serais pas en mesure d'y répondre.

Mme Shelby Kramp-Neuman: Très bien.

Par ailleurs, dans le rapport, on insistait sur la nécessité de maintenir en poste les effectifs des FAC dans des domaines hautement techniques, comme le cyberespace, notamment par l'ajout de 120 nouveaux postes de renseignement chez les militaires et de 180 nouveaux postes de renseignement chez les civils.

Cet objectif a-t-il été atteint? Quels sont les chiffres dans ce secteur particulier, si vous les connaissez?

Cam Lou Carosielli: Votre question porte spécifiquement sur des postes dans le domaine du renseignement. Ce n'est pas quelque chose que je suis en train de suivre, madame. Nous pouvons en prendre note et vous répondre par écrit.

Mme Shelby Kramp-Neuman: Je vous en saurais gré. Parfait. Merci.

En ce qui concerne la croissance dans le domaine de la cybersécurité, quels sont, selon vous, les chiffres à atteindre pour que nous puissions nous affirmer et nous assurer que nous sommes des concurrents dans ce domaine?

Cam Lou Carosielli: Je vous remercie de la question.

Les Forces armées canadiennes investiront bientôt dans la croissance de la force de cybersécurité, tant du point de vue technique que du personnel.

Comme je l'ai indiqué, au cours des trois dernières années, nous avons atteint nos objectifs en matière de recrutement. Nous continuerons à les surveiller et à accroître les capacités au besoin pour soutenir les missions et les opérations des Forces armées canadiennes.

Mme Shelby Kramp-Neuman: Recrutez-vous davantage parmi les réservistes, dans le bassin du secteur privé ou dans la cyberexpertise?

Cam Lou Carosielli: La particularité du métier de cyberopérateur au sein des Forces armées canadiennes est que nous recrutons directement à la base. Nous avons la capacité de recruter des gens qui sortent de l'école secondaire. Nous pouvons recruter directement dans l'industrie ou dans des établissements d'enseignement d'autres niveaux, comme les universités.

Nous avons toutes ces possibilités à notre disposition, et nous nous développons à partir de la base dans ces métiers.

Mme Shelby Kramp-Neuman: Savez-vous combien il y a de cyberopérateurs de réserve actuellement?

Cam Lou Carosielli: Je n'ai pas ce nombre sous la main, mais c'est une donnée que nous pourrions prendre en note et vous fournir si nécessaire.

Mme Shelby Kramp-Neuman: Cela serait très utile. Merci.

En avril 2021, dans le rapport intitulé *Évaluation des cyberforces*, on indiquait que l'un des problèmes des cyberforces, c'était « [l]'absence de plan d'avancement de carrière ».

S'agit-il toujours d'un problème?

Cam Lou Carosielli: C'est une excellente question et elle est liée à ce que j'ai dit sur le recrutement et la création des postes de cyberopérateurs.

La création de ces postes s'accompagne d'un plan de carrière et d'un plan d'avancement, de l'entrée à la retraite.

Mme Shelby Kramp-Neuman: Excellent. Merci.

Le président: Merci, madame Kramp-Neuman.

Monsieur Fisher, vous disposez de six minutes.

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

Merci, monsieur Quinn, d'être ici.

Merci, contre-amiral. Je dois vous avouer que j'aimerais avoir votre carte de visite, parce que, quand on peut se dire le commandant de la Force cybernétique… J'imagine les jeunes enfants canadiens d'aujourd'hui qui rêvent de le devenir un jour. Ça ressemble au titre d'un emploi du futur qui leur est destiné.

La semaine dernière, un témoin est venu essentiellement nous dire que les relations entre les Forces armées canadiennes et le Centre de la sécurité des télécommunications étaient foncièrement dictées par les besoins, c'est-à-dire presque inexistantes et officieuses. Ça m'a étonné.

Ce jugement est-il juste? Sinon, messieurs, veuillez nous éclairer sur les modalités de la cybercoopération entre les deux.

Cam Lou Carosielli: Votre question est très importante, alors que les deux ont des relations de longue date, qui se prolongent dans la cyberdéfense. Les deux collaborent quotidiennement en liaison étroite.

Comme vous auriez pu l'entendre la semaine dernière, à la faveur de la discussion sur le Centre de la sécurité des télécommunications, certains de ses membres sont intégrés dans des équipes des Forces armées canadiennes et vice versa. Nous partageons l'information, les outils, le renseignement et nous nous appuyons mutuellement dans des opérations pour le Centre de la sécurité des télécommunications comme pour les Forces armées canadiennes.

M. Darren Fisher: Les rapports entre les deux sont-ils officialisés? Sinon, prévoyez-vous de les améliorer ou de les officialiser?

Je viens de m'apercevoir que M. Quinn voulait intervenir. Désolé de vous avoir interrompu.

M. Jonathan Quinn: Il n'y a pas de mal.

Je voulais seulement ajouter que l'amiral Carosielli a exposé les relations et les liens opérationnels vraiment étroits qui existent entre le ministère de la Défense nationale, les Forces armées canadiennes et le Centre de la sécurité des télécommunications. J'allais ajouter qu'ils englobent aussi la sphère stratégique.

Je travaille en relation extraordinairement étroite et en concertation parfaite avec mes homologues du Centre de la sécurité des télécommunications sur des questions stratégiques. Avec le Centre de la sécurité des télécommunications, nous collaborons de très près et sur toute la ligne.

● (1545)

M. Darren Fisher: Comment cette relation se compare-t-elle à celle que nous avons avec nos alliés?

Cam Lou Carosielli: Nos relations avec nos alliés et le Centre de la sécurité des télécommunications sont aussi importantes l'une que l'autre. Nous travaillons de très près avec les États-Unis. Bien sûr, c'est important de le faire non seulement pour la défense, mais, également, pour la prospérité de l'Amérique du Nord.

Nous sommes sur la même longueur d'onde que l'U.S. Cyber Command, à tel point que nous avons un officier de liaison intégré dans ce dernier de même que de nombreux opérateurs, qui vont des cyberopérateurs aux planificateurs de cyberopérations. C'est d'une très grande importance pour nous. C'est un plus pour nous d'avoir ces conversations quotidiennes. Les discussions hebdomadaires auxquelles je participe avec l'U.S. Cyber Command nous sont indispensables.

Nous collaborons avec l'U.S. Cyber Command et nos alliés du Groupe des cinq et de l'OTAN pour nous assurer de satisfaire aux exigences de nos alliés et partenaires ainsi que du Canada.

M. Darren Fisher: En quoi les cybercapacités des Forces armées canadiennes diffèrent-elles de celles du Centre de la sécurité des télécommunications?

Cam Lou Carosielli: Leurs cybercapacités diffèrent principalement parce que nous ne voulons pas de redondance. Le Centre de la sécurité des télécommunications se spécialise dans l'aspect technique, tandis que les Forces armées canadiennes servent ordinairement à franchir le dernier bout de chemin, pour nous assurer de posséder le renseignement qui les appuiera tous les deux.

M. Darren Fisher: Vous avez dit que vous conseillez l'Ukraine sur les questions de cybersécurité. Quand participez-vous ensemble, les Forces armées canadiennes et le Centre de la sécurité des télécommunications, à des opérations? Selon quelles modalités? Dans quelles circonstances les Forces armées canadiennes agiraient-elles de façon indépendante?

Cam Lou Carosielli: Les deux agissent de concert selon le soutien nécessaire et en fonction des autorités sous lesquelles certaines opérations sont réalisées.

Si telle opération militaire se fait sous l'autorité des Forces armées canadiennes et que nous ayons besoin d'appui sous la forme de renseignements ou d'outils, nous pouvons les obtenir sous le régime de l'article 20 de la Loi sur le Centre de la sécurité des télécommunications.

De même, si le Centre de la sécurité des télécommunications travaille à un projet et a besoin de nos experts en la matière, il lui est possible de demander notre appui. Nous pouvons le lui fournir et l'appuyer en vertu des pouvoirs qu'il possède, pour répondre aux exigences du Canada.

M. Darren Fisher: Merci beaucoup.

Parlons, très rapidement, de cybercapacités.

Nous classons presque toujours la Russie parmi les quatre premières puissances. Elle est peut-être au premier rang en ce qui concerne les cybercapacités. Nous avons toujours cru qu'il en allait de même pour sa puissance militaire jusqu'à la guerre illégitime d'Ukraine.

La pensée critique est-elle de retour? Les cybercapacités russes sont-elles moins impressionnantes que nous le pensions? Je sais que ce pays pratique la guerre hybride, avec un peu de désinformation, un peu de cybercapacités, puis du combat traditionnel, comme nous le voyons en Ukraine.

Cam Lou Carosielli: Votre question, qui est très importante, est très pertinente en ce qui concerne la guerre russo-ukrainienne.

La Russie demeure un cyberacteur de premier plan. Comme vous l'avez dit, les quatre premiers sont la Russie, la Chine, l'Iran et la Corée du Nord.

Relativement à vos observations sur la cyberguerre et la guerre plus traditionnelle, nous avons sûrement vu, au début de l'automne, un lien entre des cyberévénements et des activités cinétiques. Immédiatement ou peu avant le bombardement d'une région et l'atteinte d'une cible, nous constations une augmentation de l'utilisation des serveurs et des systèmes informatiques.

Un lien existe entre la cyberactivité de la Russie et son activité cinétique, dite conventionnelle.

Le président: Merci, monsieur Fisher.

Avant que je n'accorde la parole à Mme Normandin, pouvez-vous expliquer ce qu'est le « dernier bout de chemin »?

Cam Lou Carosielli: Absolument.

L'expression est employée sur place, sur le théâtre des opérations. Habituellement, le personnel du Centre de la sécurité des télécommunications ne va pas en zone de guerre ou de conflit, de sorte que, pendant les missions canadiennes, cette distance est parcourue par le personnel des Forces armées canadiennes.

Le président: Merci.

Madame Normandin, vous disposez de six minutes.

[*Français*]

Mme Christine Normandin (Saint-Jean, BQ): Merci beaucoup.

Je vous remercie de votre présence, messieurs.

Commandant Carosielli, j'aimerais que vous nous parliez davantage des cyberopérations. Vous avez mentionné le cas de l'Ukraine, qui a été aidée par le Canada à la suite d'attaques. J'aimerais en savoir plus sur la rapidité avec laquelle vous êtes capable d'obtenir les autorisations gouvernementales pour développer des cyberprojets.

Y a-t-il un problème de rapidité, ou est-ce que ça va bien? Avez-vous des recommandations à faire sur le plan des autorisations?

● (1550)

Cam Lou Carosielli: Je vous remercie de votre question.

Les opérations cybernétiques des Forces armées canadiennes peuvent se faire en vertu d'un mandat que celles-ci ont reçu au cours d'une mission. Dans ce genre de cas, les autorisations sont données par le gouvernement du Canada ou par le Cabinet.

Des opérations se font aussi en vertu d'un mandat donné par le Centre de la sécurité des télécommunications, le CST. Je crois que celui-ci doit recevoir les autorisations du ministère de la Défense nationale et de celui des Affaires étrangères.

Les opérations venant des missions relèvent d'un processus très bien rodé. Pour ce qui est de celles venant du CST, je ne peux malheureusement pas vous en dire davantage.

Mme Christine Normandin: J'aimerais en savoir plus sur l'acquisition du matériel qui permet de soutenir ces missions-là. Je pense au matériel informatique, car il faut souvent être à la fine pointe de la technologie.

Les Forces armées canadiennes réussissent-elles à fonctionner avec le matériel dont elles disposent?

Devraient-elles avoir accès du matériel plus à la fine pointe et pouvoir l'acquérir rapidement?

Cam Lou Carosielli: Comme les autres ministères et l'industrie, les Forces armées canadiennes et les forces cybernétiques ont des problèmes de soutien logistique, comme pendant la pandémie de COVID-19, par exemple.

Pour ce qui est de l'approvisionnement au Canada, cela demande un effort du ministère au complet. Nous travaillons avec Services publics et Approvisionnement Canada et Innovation, Sciences et Développement économique Canada pour nous assurer de faire progresser nos projets de manière efficace et de trouver du matériel innovant.

Nous allons certainement continuer de faire le lien avec les industries afin qu'elles puissent conserver une chaîne d'approvisionnement libre et concurrentielle et qu'elles soient au fait ce que prépare l'avenir.

Mme Christine Normandin: Merci beaucoup.

Ma prochaine question s'adresse peut-être davantage à vous, monsieur Quinn, mais, je vous en prie, répondez tous les deux, si cela vous dit.

Vous avez parlé de la politique internationale en matière de cyberespace. De ce que je comprends, cela implique une obligation de reddition de comptes pour les États, qui doivent faire connaître les activités malveillantes qui se passent sur leur territoire. J'aimerais savoir s'il est facile d'obtenir ces informations des autres États, en mettant notamment l'accent sur le privé.

Le secteur privé, dans les autres États comme chez nous, représente-t-il un enjeu? En effet, on ne veut pas nécessairement dévoiler l'information sur les attaques que nous pouvons avoir subies, par exemple.

M. Jonathan Quinn: Je vous remercie de votre question.

[*Traduction*]

Absolument. Il est difficile d'attribuer à quiconque des cyberattaques ou une cyberactivité malicieuse. De par leur nature, elles ont tendance à être secrètes. La position du Canada exprimée dans la déclaration à laquelle j'ai fait allusion sur notre interprétation du droit international dans ma déclaration liminaire visait seulement à faire preuve de transparence et à nous responsabiliser au Canada ainsi qu'à fixer une norme de notre propre comportement dans le cyberespace et à énoncer notre interprétation de la loi.

Quand un cyberévénement malicieux survient au Canada, on s'applique à en déterminer la provenance, mais, comme vous le dites si bien, le cyberespace ne se plie pas facilement à la volonté. Nos homologues d'Affaires mondiales Canada ont mis au point un processus pour attribuer publiquement, quand il va de notre intérêt de le faire, l'origine de ces attaques et divulguer certains détails, mais c'est seulement quand les preuves de l'origine de l'attaque sont vraiment solides et défendables qu'on l'attribue publiquement à quelqu'un.

[*Français*]

Mme Christine Normandin: Merci.

Les autres États du monde sont-ils aussi transparents quant aux informations qu'ils donnent lorsqu'ils subissent des attaques?

M. Jonathan Quinn: Je vous remercie de votre question.

[*Traduction*]

Parmi nos alliés et les pays en communion d'idées avec nous, on fait un effort concerté de transparence.

Ici, aussi, je sors un peu de mon domaine — ça relève plutôt d'Affaires mondiales Canada —, mais tel que je le comprends, la publication de l'interprétation du droit international par divers États, en ce qui concerne le cyberespace, a d'abord été une initiative du G7. Il est certain que nos alliés en communauté d'idées avec nous y tiennent, mais, comme c'est le cas sur beaucoup de questions de ce domaine, leur adhésion et leur engagement envers la transparence dans ce domaine sont très divers.

● (1555)

Le président: Merci, madame.

Monsieur Bachrach, soyez le bienvenu à notre comité.

M. Taylor Bachrach (Skeena—Bulkley Valley, NPD): Merci, monsieur le président.

Je remercie les membres du Comité de m'autoriser à remplacer ma collègue Mme Mathyssen pour discuter de ce sujet très important et très intéressant.

Je tiens également à remercier les témoins Carosielli et Quinn.

Revenons sur quelques questions qui ont été posées. À la lumière, particulièrement, de l'actualité de la semaine dernière, je pense que la cybersécurité éveille de plus en plus l'intérêt et les inquiétudes des Canadiens.

Une certaine confusion règne sur l'origine de la stratégie du Canada en matière de cybersécurité. Il y a la Force cybernétique que vous commandez, contre-amiral; le Centre de la sécurité des télécommunications, qui relève de la Défense nationale; le Service canadien du renseignement de sécurité et Services partagés Canada qui, tous ensemble, collaborent à la protection de nos infrastructures essentielles contre les cyberattaques et à la prévention de nos vulnérabilités. Lequel d'entre eux a le premier rôle dans l'établissement de la stratégie du Canada en matière de cybersécurité?

M. Jonathan Quinn: Monsieur le président, je commencerai, et l'amiral pourra compléter ma réponse.

Votre question est excellente. Le cyberespace est compliqué. On compte beaucoup de joueurs fédéraux dans ce domaine. Le premier rôle fédéral en matière de cybersécurité — assurer la sécurité des réseaux de l'État, prêter assistance aux détenteurs de réseaux d'infrastructures essentielles et ce genre de choses — appartient globalement à la Sécurité publique.

On a particulièrement créé le Centre canadien de cybersécurité, qui relève du Centre de la sécurité des télécommunications, mais qui harmonise son travail avec la politique établie par Sécurité publique. Il y a un rôle important dans la diffusion des pratiques exemplaires, l'aide aux entreprises canadiennes et l'identification ainsi que l'atténuation des menaces.

Les Forces armées canadiennes entrent en scène. L'amiral Carosielli pourra en dire davantage, également. Contrairement aux autres ministères fédéraux, la Défense nationale et les Forces armées canadiennes sont chargées de défendre et de sécuriser leurs propres réseaux classifiés. C'est exceptionnel à l'échelon fédéral.

Comme je le disais dans ma déclaration préliminaire, le gouvernement, dans *« Protection, Sécurité, Engagement »,* a annoncé son intention d'autoriser les Forces armées canadiennes à mener des cyberopérations offensives également, dans la poursuite des intérêts du Canada. Comme il en a été question, avant, nous le faisons en liaison étroite avec nos collègues du Centre de la sécurité des télécommunications.

Amiral, je vous cède la parole.

Cam Lou Carosielli: Merci, Jon.

Je tiens à réitérer l'absolue responsabilité des Forces armées canadiennes dans la défense des réseaux et des systèmes informatiques leur appartenant à elles ainsi qu'au ministère de la Défense nationale.

Cela étant dit, nous travaillons de près avec nos partenaires du Centre de la sécurité des télécommunications, de la GRC, d'Affaires mondiales Canada, etc. Nous nous appliquons à mettre en commun tous les renseignements que, entre les partenaires, nous recevons sur le renseignement, par exemple les compromissions, etc., pour que tous, nous ayons amplement de renseignements et une bonne compréhension de ce qui se passe dans les autres réseaux. Bien sûr, ce qui survient dans un réseau pourrait n'être qu'un précurseur de choses à venir dans un autre réseau.

M. Taylor Bachrach: Merci pour ces renseignements. C'est visiblement une réponse complexe. Le premier rôle dépend de l'aspect de cybersécurité dont il est question.

Qui est le stratège des cyberopérations contre d'autres pays?

M. Jonathan Quinn: Je commence, puis je céderai la parole à l'amiral, s'il veut ajouter quelque chose.

Les Forces armées canadiennes possèdent l'autorité pour mener des cyberopérations offensives dans le contexte de missions militaires autorisées. Dans ce cas, c'est elles qui les dirigent et les mènent sous sa propre autorité, souvent avec l'aide de collègues du Centre de la sécurité des télécommunications.

D'autres opérations de cette nature sont menées sous l'autorité du Centre de la sécurité des télécommunications, en application de la Loi sur le Centre de la sécurité des télécommunications. Je crois que vous avez entendu des témoins qui représentaient le Centre de la sécurité des télécommunications et qui seraient beaucoup plus compétents que moi pour exposer en détail la conduite de ces opérations. De même, comme l'amiral l'a dit, quand le Centre de la sécurité des télécommunications conduit ces opérations sous le régime de la loi susmentionnée, il peut adresser des demandes d'aide aux Forces armées canadiennes, comme il est prévu dans l'article 20 de la même loi.

● (1600)

Cam Lou Carosielli: Monsieur Quinn, je n'ai rien d'autre à ajouter.

Le président: Il vous reste environ une minute.

M. Taylor Bachrach: Je vous en remercie.

Pourriez-vous en dire un peu plus sur les relations entre les Forces armées canadiennes et le Centre de la sécurité des télécommunications?

Vous avez parlé de l'intégration de vos opérations. Je suis curieux de connaître la taille relative de ces cyberopérations. Laquelle des équipes est la plus nombreuse, et comment caractériseriez-vous la taille relative de ces deux opérations?

Cam Lou Carosielli: Impossible pour moi de vous donner des chiffres définitifs, faute de chiffres sur le Centre de la sécurité des télécommunications. C'est en dehors de mon domaine.

En ce qui concerne l'importance de la collaboration entre les deux équipes, comme je l'ai laissé entendre, elle se poursuit à longueur de journée chaque semaine. Nous avons du personnel intégré dans les équipes de l'autre pour que nous en comprenions bien les techniques, tactiques et politiques et pour que nous puissions le mieux nous appuyer mutuellement dans l'atteinte de nos besoins opérationnels respectifs.

Nous nous rencontrons régulièrement, à divers niveaux. J'ai eu des rencontres hebdomadaires avec mes homologues du Centre de la sécurité des télécommunications et, plus généralement, des rencontres mensuelles ou trimestrielles. Elles sont indispensables pour nous assurer que chacune de nos deux organisations possède les moyens et les capacités qu'elle sera appelée à fournir à l'autre.

Le président: Merci, monsieur Bachrach.

Chers collègues, nous n'avons qu'un seul témoin dans la deuxième moitié de la réunion. Je pense que nous devrions faire un deuxième tour complet de questions.

Sur ce, madame Gallant, vous disposez de cinq minutes.

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

Les ballons de surveillance peuvent-ils engorger les cybercommunications ou gêner le fonctionnement des infrastructures canadiennes comme les autres plateformes ne pourraient le faire?

Le président: Chers membres, je vous encouragerais à… J'avais dit que nous nous occuperions des ballons vendredi.

Mme Cheryl Gallant: Monsieur le président, c'est du domaine de la cybernétique.

Le président: Je sais.

J'autorise la question, mais ne nous éparpillons pas.

Mme Cheryl Gallant: Faites repartir le chronomètre.

Cam Lou Carosielli: Malheureusement, impossible de répondre, faute de connaître les technologies associées à ces objets qui dérivent à haute altitude. Je ne voudrais pas faire de suppositions sur leurs capacités.

Mme Cheryl Gallant: Les radiotélescopes peuvent-ils détecter les cybercommunications à haute altitude?

Cam Lou Carosielli: Les radiotélescopes n'entrent pas dans mon domaine de compétences. Je ne saurais répondre à cette question.

Mme Cheryl Gallant: D'accord.

Vous avez dit qu'il y avait une augmentation du nombre de cyberincidents avant une attaque cinétique.

Fin janvier, le système d'avertissement de la Federal Aviation Agency a subi une panne et, dans la foulée, le système d'avis aux navigants de l'aviation civile canadienne. Puis, quelques jours plus tard, il y a eu cet avion qui a traversé notre atmosphère.

Est-ce que ce serait considéré comme une activité cinétique consécutive à des cyberopérations annonciatrices?

Cam Lou Carosielli: Je ne peux pas vous répondre, car je crois que ces deux exemples en matière de transport aux États-Unis et au Canada étaient liés à des problèmes de logiciel et non à des enjeux de nature cybernétique. Je ne suis pas au courant du lien qu'il y aurait à faire entre ces événements s'étant déroulés il y a plusieurs semaines et les objets qui volaient à haute altitude. Je ne suis pas au fait des détails dans ce dossier.

● (1605)

Mme Cheryl Gallant: Si le gouvernement actuel ne peut surmonter l'anathème qu'il a jeté sur les sous-marins à propulsion nucléaire, nous devrons nous en remettre aux drones pour sonder les milieux marins. Les drones sous-marins sont-ils vulnérables aux éventuelles cyberattaques?

Cam Lou Carosielli: Vous conviendrez que la réponse à cette question est éminemment complexe, car elle porte sur diverses technologies. En tant qu'officier et ingénieur naval, je peux néanmoins affirmer que les techniques de détection sous-marine comptent parmi les plus difficiles à contrecarrer. La communication avec ces drones peut toutefois se montrer ardue, en raison du milieu où ils évoluent.

Je vais en rester là, étant donné que ce n'est ni mon champ d'expertise, ni mon domaine de responsabilité à l'heure actuelle.

Mme Cheryl Gallant: D'accord.

La question suivante s'adresse aussi à monsieur Quinn.

Les Forces armées canadiennes emploient-elles des installations ou reçoivent-elles du matériel doté de composantes provenant de chaînes d'approvisionnement où la Chine a un rôle à jouer? Je parle de tous les types de matériel, pas seulement du matériel informatique.

M. Jonathan Quinn:

Je ne suis pas un expert dans les composantes électroniques qui se retrouvent dans le matériel qu'utilisent les Forces armées canadiennes. Je présume que certaines composantes sont fabriquées en Chine, mais je vous prie de m'excuser, car ce n'est pas mon domaine d'expertise.

Mme Cheryl Gallant: Comment nos Forces armées s'y prennent-elles pour protéger leur matériel contre les attaques commises à l'aide de l'Internet des objets?

Cam Lou Carosielli: Je répète que les Forces armées canadiennes sont responsables de la défense de nos réseaux et de nos systèmes de technologie de l'information. Nous assurons leur protection par divers moyens selon une approche graduelle. Notre périmètre de défense protège autant nos réseaux externes que chaque espace de travail individuel, comme un ordinateur ou un portable.

Bien que des motifs sécuritaires m'empêchent de vous communiquer le détail de nos opérations, sachez que nous assurons à toute heure la sécurité de nos réseaux.

Mme Cheryl Gallant: De nos jours, même le réfrigérateur dans la salle du personnel peut être doté du WiFi. Que faites-vous pour que les logiciels militaires ne se connectent pas aux divers objets sur Internet, comme les réfrigérateurs?

Cam Lou Carosielli: Nous menons des analyses de sécurité exhaustives — , et ce, pour l'ensemble de nos systèmes — dans le cadre de nos processus de sécurité et d'accréditation. Avant de permettre l'utilisation du matériel, nous vérifions comment et avec qui il peut se connecter. Cependant, je ne suis pas autorisé à vous transmettre plus de renseignements sur quelque système que ce soit, en raison des habilitations de sécurité exigées.

Mme Cheryl Gallant: Les services de cybersécurité italiens ont indiqué que la sécurité de serveurs en Europe et en Amérique du Nord avait été compromise le 5 février 2023. Que pouvez-vous nous dire sur l'attaque mondiale qui a été perpétrée au courant de cette semaine-là, à l'aide d'un logiciel de rançon qui a touché des serveurs au Canada?

Cam Lou Carosielli: Je ne possède aucune information sur l'attaque en question.

Mme Cheryl Gallant: Est-ce que des pressions s'exercent...

Le président: Je suis désolé, mais vos cinq minutes sont écoulées, madame Gallant.

La parole va maintenant à Mme Lambropoulos; vous avez cinq minutes.

Mme Emmanuella Lambropoulos (Saint-Laurent, Lib.): Merci, monsieur le président, et merci aux témoins parmi nous aujourd'hui de répondre à certaines de nos questions.

Dans vos réponses à quelques questions posées par mes collègues sur le travail que nous réalisons avec nos partenaires dans d'autres pays, vous avez parlé de notre relation avec les États-Unis et des liens étroits qui vous unissent, en matière de cyberactivités touchant nos deux pays.

J'aimerais vous entendre sur le travail que les Forces armées canadiennes effectuent avec nos partenaires du Groupe des cinq. Plus particulièrement, comment pouvons-nous apprendre en travaillant avec eux? Y a-t-il une différence entre vos méthodes? Le Groupe des cinq est-il meilleur dans certains domaines, et comment peut-on s'y prendre pour tirer des enseignements de leurs façons de faire?

Cam Lou Carosielli: J'ai en effet mentionné nos interactions avec les États-Unis, mais nous coordonnons nos efforts et discutons avec tous nos partenaires du Groupe des cinq. C'est essentiel pour nous de collaborer de la sorte, et nous le faisons à divers niveaux.

Nous avons de nombreuses interactions au fil des différentes conférences et des autres activités auxquelles nous participons avec eux. Nos agents de liaison échangent directement avec nos partenaires du Groupe des cinq, mais avant tout, nos meilleures conversations se tiennent durant les exercices conjoints. Tous les partenaires faisant partie du Groupe des cinq participent aux exercices, qui nous donnent l'occasion d'en savoir plus sur les pratiques exemplaires et de consolider nos relations, afin de réagir adéquatement lorsque les choses tournent mal. Nous avons des points de contact et pouvons aisément communiquer de l'information entre partenaires.

● (1610)

Mme Emmanuella Lambropoulos: Je vous remercie beaucoup.

Ma prochaine question porte sur un gazouillis publié la semaine dernière par le commandant de l'Armée canadienne, disant que nos principaux alliés procédaient à une transformation numérique rapide et que nous devions en faire autant, sans quoi notre pertinence en tant qu'allié fiable s'en trouverait compromise.

Tout d'abord, que pensez-vous de cette déclaration? J'aimerais connaître les mesures précises que prend le ministère de la Défense nationale pour maintenir notre pertinence de façon continue en matière de cybersécurité.

Cam Lou Carosielli: Comme monsieur Quinn l'a exposé en début de séance, nos alliés investissent sans conteste et améliorent leurs capacités de cybersécurité. C'est ce que fait le Canada, lui aussi. Nous prenons la question très au sérieux en vue de fournir au gouvernement du Canada les capacités nécessaires à la réalisation de nos missions militaires et des opérations du Centre de la sécurité des télécommunications. Nous nous assurons de disposer du bon matériel et de déployer les gens compétents. C'est ce que nous avons fait avec les cyberopérateurs, et nous renforçons nos capacités dans ce domaine.

Nous avons atteint nos cibles de recrutement ces trois dernières années, et nous sommes en bonne voie de répondre à toutes nos exigences en matière de sécurité cybernétique.

Mme Emmanuella Lambropoulos: À l'exception du recrutement et des mesures relatives au personnel, avez-vous mis en oeuvre d'autres mesures dont vous pouvez parler durant cette séance?

Cam Lou Carosielli: Je ne puis mentionner ici aucune des mesures que nous avons prises à cet égard.

Mme Emmanuella Lambropoulos: Combien de temps me reste-t-il?

Le président: Vous disposez d'un peu moins de deux minutes.

Mme Emmanuella Lambropoulos: Vous avez beaucoup parlé de la relation entre les Forces armées canadiennes et le Centre de la sécurité des télécommunications. Or, les témoignages entendus la semaine dernière divergent de votre témoignage aujourd'hui. Qu'est-ce qui expliquerait cette divergence d'opinions? Considérez-vous que vos points de vue concordent? Pouvez-vous nous en dire plus long à ce sujet?

Cam Lou Carosielli: D'après la transcription de votre séance la semaine dernière et les conversations que nous avons tenues aujourd'hui, je ne vois pas de quelle différence ou divergence il serait question. Pourriez-vous préciser votre question? Sinon, il faudrait peut-être me transmettre plus de renseignements pour que je sois en mesure de vous répondre.

M. Jonathan Quinn: Si vous le permettez, monsieur le président, je suis d'accord avec le contre-amiral Carosielli. Nos collègues au CST ont donné à peu près les mêmes réponses que nous. Un universitaire a peut-être présenté un point de vue contradictoire selon lequel, aux yeux de la population, nos organismes ne se parleraient pas beaucoup, mais je vous assure que le ministère de la Défense nationale, les Forces armées canadiennes et le Centre de la sécurité des télécommunications collaborent étroitement.

Le président: Je vous remercie.

[*Français*]

Madame Normandin, vous avez deux minutes et demie.

Mme Christine Normandin: Merci beaucoup.

Un témoin nous a mentionné, la semaine dernière, qu'on devrait peut-être moins se concentrer sur l'analyse d'attaques qui auraient, par exemple, une grande incidence sur les infrastructures critiques, parce que, si elles présentent des risques élevés, en revanche, la probabilité qu'elles se produisent est faible. Selon ce témoin, on devrait plutôt se concentrer davantage sur les petites attaques qui risquent d'être plus nombreuses et faire aussi mal. On peut penser à SolarWinds, par exemple.

J'aimerais que vous nous parliez de la formation donnée aux membres des forces armées, et même aux civils, pour s'assurer que des petites attaques ne se produisent pas, que l'hygiène informatique est bonne, d'une certaine façon. Donne-t-on de la formation dès que quelqu'un entre, par exemple, à la qualification militaire de base? Y a-t-il des suivis par la suite et de la formation continue? J'aimerais vous entendre à ce sujet.

Cam Lou Carosielli: Je vous remercie de votre question.

Comme je l'ai mentionné, la formation des cyberopérateurs des Forces armées canadiennes est progressive. À la base, ils apprennent comment se défendre de petits réseaux, de petites attaques. Avec l'expérience et la formation additionnelle, ils sont prêts, sur le plan de la défense, à affronter des attaques plus sophistiquées.

Toute l'information qu'on reçoit sur un réseau est transmise à tous nos partenaires, dont la CST et les corps policiers, afin de s'assurer que cette information se rend chez tous ceux qui ont besoin d'être au courant, c'est-à-dire ceux qu'on verra sur notre réseau pendant les jours ou les semaines à venir.

● (1615)

Mme Christine Normandin: Les employés des Forces armées canadiennes qui ne sont pas des cyberopérateurs, qui oeuvrent dans d'autres domaines, comment peut-on s'assurer qu'ils ne sont pas des portes d'entrée de cyberattaques?

Cam Lou Carosielli: Je vous remercie. Je n'avais pas compris cet aspect de votre question.

Nous donnons une formation générale à tous les membres des Forces armées canadiennes et à ceux des services publics. Nous venons tout juste de terminer la semaine de sécurité. Il y a des cours de sécurité formelle qu'ils doivent réussir. Il y a aussi les messages habituels pour contrer l'hameçonnage. Il faut s'assurer que les gens savent qu'ils doivent vérifier d'où vient un courriel avant d'ouvrir les fichiers joints ou les liens qui s'y trouvent.

[*Traduction*]

Le président: Je vous remercie, madame Normandin.

La parole va maintenant à M. Bachrach pour deux minutes et demie.

M. Taylor Bachrach: Je vous remercie, monsieur le président.

J'aimerais revenir à mes questions précédentes sur la taille relative des forces de cybersécurité travaillant au Centre de la sécurité des télécommunications. Sans révéler le nombre précis d'employés ou ce genre de renseignements, le contre-amiral Carosielli pourrait-il nous en dire plus là-dessus? Quelle équipe compte, proportionnellement, le plus vaste effectif? Une équipe détient-elle le double des ressources qu'on trouve dans une autre équipe?

Pourriez-vous nous donner une idée de la taille des effectifs au sein de ces deux organisations?

Cam Lou Carosielli: Je ne pourrais pas vous répondre quant à la taille de nos équipes. Je répète que j'ignore quels effectifs compte le CST. Sachez que je ne suis en poste que depuis l'été dernier. Puisque nous n'avons pas eu de discussions à ce sujet, je ne suis pas en mesure de vous répondre.

M. Taylor Bachrach: D'accord, il n'y a pas de problème.

Contre-amiral, auriez-vous participé avec les forces de cybersécurité à la collecte de données sur les Canadiens, dans le cadre des programmes du ministère de la Défense, des Forces armées canadiennes ou d'un autre ministère fédéral?

Cam Lou Carosielli: L'équipe de cybersécurité des Forces armées canadiennes travaille dans le contexte des missions des FAC. Nous ne recueillons donc pas de renseignements sur les Canadiens. Comme les représentants du Centre de la sécurité des télécommunications vous l'ont dit, son mandat ne lui permet de colliger des renseignements ni sur les Canadiens, ni sur le personnel se trouvant en sol canadien.

M. Taylor Bachrach: Dites-vous que votre équipe ne recueille pas les métadonnées accessibles au public sur les réseaux sociaux? La modélisation du comportement des Canadiens d'après leurs activités sur les réseaux sociaux ne ferait pas partie des opérations des forces de cybersécurité.

Cam Lou Carosielli: À ma connaissance, de telles opérations ne relèvent pas de notre champ de compétence. Je n'ai pas entendu parler de ce genre d'opération.

M. Taylor Bachrach: D'accord.

Je présume qu'il ne me reste que quelques secondes, monsieur le président. Je voudrais poser quelques questions sur l'infrastructure essentielle que possède et contrôle le secteur privé.

Lorsque le réseau de Rogers est tombé en panne l'été dernier, on a clairement vu que le gouvernement fédéral jouait un rôle très marginal dans la protection et la remise sur pied de ce réseau.

Contre-amiral Carosielli, pourriez-vous nous parler de l'écart qui s'observe entre les capacités des forces de cybersécurité et leur accès limité à l'infrastructure essentielle que contrôlent des intérêts privés? Vos effectifs sont-ils en mesure...

Le président: M. Bachrach avait raison de dire qu'il lui restait très peu de temps, et son temps de parole est maintenant écoulé.

M. Taylor Bachrach: C'était une belle introduction en vue de la prochaine occasion qu'il aura de me répondre.

Le président: Je comprends qu'il s'agissait là d'une question préparatoire.

D'accord. Monsieur Kelly, vous avez la parole pour les cinq prochaines minutes.

M. Pat Kelly (Calgary Rocky Ridge, PCC): Merci.

Nous avons entendu vendredi le témoignage d'Alexander Rudolph qui nous a notamment dit: « Les Forces armées canadiennes ne sont aucunement préparées à une cyberguerre en cas de conflit. Je me demande même dans quelle mesure elles sont capables de coopérer et d'échanger avec les alliés, notamment avec les États-Unis. »

Et il a ajouté: « La politique de cyberdéfense du Canada est à tout le moins incomplète et ponctuelle. Sa stratégie et sa définition ne s'harmonisent pas à celles des alliés du Canada, notamment les États-Unis. »

Il s'agit d'allégations assez fortes que nous avons pu entendre vendredi. Est-ce que M. Rudolph a raison?

Cam Lou Carosielli: Comme je l'indiquais précédemment, les Forces armées canadiennes offrent déjà du soutien à l'Ukraine et à la Lettonie. Nous menons d'ores et déjà des opérations avec nos partenaires des États-Unis et du Groupe des cinq, et nous continuons d'effectuer des exercices avec eux afin d'améliorer nos capacités, d'harmoniser nos forces et de mettre en commun nos pratiques les plus efficaces.

● (1620)

M. Pat Kelly: D'accord.

Vous avez parlé tout à l'heure de l'intégration des forces. Est-ce que cela se fait uniquement avec les États-Unis ou y a-t-il aussi intégration avec l'OTAN, nos alliés du Groupe des cinq, l'Ukraine, la Lettonie ou d'autres pays?

Cam Lou Carosielli: Nous avons effectivement du personnel intégré aux forces américaines. C'est aussi le cas avec le Royaume-Uni. Comme vous le savez, nous avons également des gens qui travaillent à l'OTAN dans le cadre d'un échange de personnel. Nous avons…

M. Pat Kelly: Je vois, merci.

M. Rudolph nous a aussi indiqué que la Russie s'est servie de maliciels de nettoyage à l'encontre de l'Ukraine pour détruire des données désormais irrécupérables. Est-ce que les protocoles de protection et de sauvegarde mis en place par le Canada et les redondances intégrées délibérément seraient suffisants pour contrer une attaque similaire contre les infrastructures canadiennes?

Cam Lou Carosielli: Comme je l'ai indiqué, l'une des principales raisons d'être de notre Force cybernétique est de défendre les réseaux et les systèmes informatiques des Forces armées canadiennes. Nous avons mis en place les protocoles nécessaires pour protéger nos données et nous assurer d'y avoir toujours accès.

M. Pat Kelly: Si jamais le conflit avec la Russie prenait de l'ampleur ou si la situation mondiale se détériorait dans le contexte du différend avec la Chine concernant le détroit de Taiwan, est-ce que le Canada serait en mesure de contrer une attaque en règle à son endroit?

Cam Lou Carosielli: En collaboration avec ses alliés, le Canada verrait à repousser les attaques cybernétiques et conventionnelles lancées contre lui.

M. Pat Kelly: Est-ce que l'infrastructure de cybersécurité du Canada est prête à utiliser les capacités de renseignement et de partage du renseignement avec les forces alliées qu'offrent les F-35 dont nous avons fait l'acquisition?

Cam Lou Carosielli: Il va de soi que notre force de cybersécurité ainsi que le dirigeant principal de l'information du Canada collaborent avec l'Aviation royale canadienne afin que tout soit prêt lorsque ces aéronefs nous seront livrés.

M. Pat Kelly: Serons-nous capables de transmettre et d'échanger des renseignements avec nos alliés?

Cam Lou Carosielli: Nous le faisons déjà. Maintenant que nous avons signé les contrats pour l'acquisition des F-35, nous allons intensifier nos échanges. Il s'agit de s'assurer que l'Aviation royale canadienne est prête à utiliser toutes les capacités offertes par ces avions dès que nous en prendrons possession.

M. Pat Kelly: Vous avez indiqué dans vos observations préliminaires — ou peut-être était-ce M. Quinn — que le cyberespace est un nouveau domaine de conflit. On nous a amplement parlé de l'importance de bien connaître la situation dans les différents domaines et des lacunes en la matière. Il en a été beaucoup question dans le contexte des incursions de notre espace aérien au cours des deux dernières semaines. On nous a répété que nous n'étions pas vraiment au fait de la situation qui prévaut dans notre domaine sous-marin. Quelles sont les lacunes pour ce qui est de la connaissance de notre cyberdomaine? Sommes-nous conscients des véritables risques auxquels nous nous exposons? Comment pourrions-nous atteindre un plus grand degré de certitude?

Cam Lou Carosielli: Étant donné la classification de sécurité de renseignements semblables, il m'est bien sûr impossible de vous parler ici des lacunes et des risques, car c'est de l'information qui pourrait être utile à nos adversaires.

M. Pat Kelly: D'accord.

J'ai une autre question pour conclure. Est-ce que le Canada est actuellement prêt à se défendre lui-même si un conflit devait éclater ou prendre de l'ampleur dans le cyberespace?

Cam Lou Carosielli: Comme je l'ai indiqué précédemment, le Canada est déjà actif dans le domaine du cyberespace. Nous allons continuer de coopérer avec nos alliés pour les défendre et défendre notre pays si cela se révèle nécessaire.

Le président: Merci, monsieur Kelly.

Madame O'Connell, vous avez cinq minutes.

Mme Jennifer O'Connell (Pickering—Uxbridge, Lib.): Merci, monsieur le président.

Merci à nos deux témoins de leur présence aujourd'hui.

Mes questions vont un peu dans le sens de celles auxquelles vous venez de répondre. Des témoins précédents semblaient vouloir dire que le Canada n'est pas prêt à évoluer dans le cyberespace, mais vous nous avez parlé dans vos observations préliminaires de l'aide que vous apportez aussi bien à la Lettonie qu'à l'Ukraine. Pourquoi des pays comme ceux-là feraient-ils appel à d'autres États si ceux-ci n'étaient pas des chefs de file dans le domaine en question? N'est-ce pas la raison pour laquelle l'aide du Canada a été sollicitée?

Cam Lou Carosielli: Tout à fait. À n'en pas douter, le Canada se démarque en volant ainsi au secours de ses alliés pour qu'ils ne perdent pas le contrôle de leurs réseaux. Nous leur fournissons le soutien dont ils ont besoin, aussi bien en matière de génie logiciel que du point de vue du renseignement.

En outre, nos capacités à ce chapitre ne cessent de s'améliorer. Nous avons encore beaucoup de pain sur la planche. Nous collaborons avec nos alliés pour faire en sorte que tous puissent ainsi se donner de meilleurs moyens d'agir. Nous nous assurons dans ce contexte d'éviter tout dédoublement des efforts.

● (1625)

Mme Jennifer O'Connell: Dans le même ordre d'idées, les attaques de toutes sortes lancées dans le cyberespace ont fait la manchette beaucoup plus fréquemment ces derniers temps. Il n'en demeure pas moins que, lorsque je me suis rendue en Estonie — il y a bien des années, avant même la pandémie —, il était déjà question du cyberespace et des problèmes vécus dans ce pays à cause de la Russie. C'était bien avant l'invasion de la Crimée. Dans une perspective mondiale, peut-on dire que le Canada s'est employé depuis à peaufiner sa préparation pour le cyberespace et à développer les ressources nécessaires à cette fin?

Vous venez de nous parler, contre-amiral, de la menace en constante évolution qui nous oblige à toujours demeurer prêts, non pas comme nous aurions voulu l'être par le passé, mais plutôt en prévision d'une situation qui risque d'être très différente dans les semaines, les mois ou les années à venir. Je reviens au cas de l'Estonie qui a vu toute son infrastructure numérique être piratée par la Russie. Est-ce que cela a alors sonné le réveil pour le Canada? Comment poursuivez-vous votre préparation à la lumière de ce qui arrive dans d'autres pays et en évitant de tenir compte uniquement des sujets retenant l'attention des médias?

Cam Lou Carosielli: Je ne pourrais pas vous parler des sujets qui étaient d'actualité à ce moment-là, car je n'avais alors aucun rôle à jouer dans le dossier. Je peux toutefois vous assurer que depuis l'adoption de la politique Protection, Sécurité, Engagement, la cybersécurité est au cœur des préoccupations aussi bien des Forces armées canadiennes que du Centre de la sécurité des télécommunications. C'est ce que nous avons pu constater avec la mise en place du Centre canadien pour la cybersécurité et les différentes responsabilités que le CST assume pour la protection de notre pays.

La question porte sur la menace qui pèse sur tout le Canada, et pas uniquement sur les Forces armées canadiennes, et cette menace est prise très au sérieux. Comme on l'a souligné, les médias font fréquemment état de l'utilisation de rançongiciels et cyberattaques, et il est important que ces menaces soient prises au sérieux et que nous nous préparions en conséquence. Pour ce faire, les Forces armées canadiennes s'assurent que les systèmes de défense de leurs réseaux fonctionnent bien et font l'objet de vérifications quotidiennes. Nous veillons en outre à effectuer des exercices faisant intervenir des scénarios très complexes de manière à bien nous préparer non seulement pour les combats du passé, mais aussi pour ceux que nous pourrions avoir à livrer dans l'avenir. Les efforts de recherche et développement sont importants à ce chapitre.

Mme Jennifer O'Connell: Merci.

Pour ce qui est de l'universalité du service et de la capacité de recrutement, les gens du CST ont indiqué... Je pense qu'il est bien connu que vous devez livrer concurrence dans ce contexte à la Silicon Valley et à d'autres entités semblables. Est-ce que l'universalité du service peut devenir un obstacle au recrutement des travailleurs les plus qualifiés dans ce domaine?

Il y a aussi la question de la diversité vers laquelle il faut tendre dans ce secteur. Êtes-vous en mesure de recruter des femmes? Pouvez-vous recruter des gens de différentes origines? Attirez-vous des gens dont les compétences linguistiques pourraient être utiles en ne vous limitant pas aux seules langues officielles du Canada? Vous assurez-vous que ceux et celles qui travaillent dans le cyberespace souhaitent vraiment faire partie des Forces armées canadiennes et de nos effectifs de cyberdéfense?

Cam Lou Carosielli: Comme je l'ai déjà indiqué, le recrutement d'effectifs représentatifs de la diversité canadienne est primordial pour nous, non seulement dans cette volonté de diversité, mais aussi à des fins opérationnelles, car il nous est utile de pouvoir compter sur des gens qui maîtrisent plusieurs langues. Je parle moi-même trois langues, et je peux vous confirmer que c'est un avantage. C'est donc l'un de nos objectifs.

Nous n'avons aucun contrôle sur l'universalité du service pour ce qui est des différents corps de métier; cela relève des Forces armées canadiennes. Je répète que nous faisons partie du personnel opérationnel et qu'il doit continuer d'en être ainsi. Nos employés peuvent choisir d'aller grossir les rangs de la fonction publique. Il faut cependant surtout noter que l'un des principaux attraits des Forces armées canadiennes et du CST réside dans le genre de travail que nous y accomplissons. Il n'y a pas beaucoup d'entités au pays, ou même de par le monde, qui pourraient faire ce travail en s'appuyant sur les pouvoirs dont nous disposons. C'est donc l'un de nos plus puissants attraits. Comme quelqu'un l'a dit précédemment, le simple fait d'avoir « cyberforce » dans son appellation permet de susciter l'intérêt de bien des gens.

Le président: Merci, madame O'Connell.

● (1630)

Mme Jennifer O'Connell: Merci.

Le président: Je crois que M. Fisher ne va pas manquer de se précipiter pour obtenir cette carte professionnelle.

Des voix: Ha, ha!

Le président: Avant de vous permettre de partir, j'aurais une question concernant les opérations offensives.

Le CST doit composer avec certaines restrictions lorsqu'il s'agit de lancer des opérations offensives visant des Canadiens. Il y a toutefois une guerre qui fait rage, et il est raisonnable de présumer qu'il y a des gens au Canada qui appuient l'ennemi, si je puis m'exprimer ainsi, et qui pourraient donc être des personnes d'intérêt pour nos services de sécurité. Je pense tout particulièrement à ceux dont le nom figure sur la liste des sanctions, mais ils ne sont pas les seuls.

En quoi cette politique interdisant les opérations offensives contre des Canadiens — ce qui peut sans doute inclure les résidents permanents — entre-t-elle en conflit avec les mesures de sécurité que nous devons prendre dans le contexte de cette guerre?

M. Jonathan Quinn: Je vais répondre, et le contre-amiral pourra peut-être vous en dire plus long.

C'est une excellente question. C'est assurément une préoccupation, mais cela ne relève pas du mandat des Forces armées canadiennes. Il y a d'autres agences au sein de la famille fédérale qui pourraient prendre en charge les dossiers semblables. La première qui vient à l'esprit serait le SCRS.

Le président: Le CST est une composante du ministère de la Défense nationale, et c'est lui qui est visé par cette politique restrictive. Je ne vais pas m'éterniser sur ce point, mais je pense que c'est un peu là où voulait en venir M. Fisher en posant des questions sur les restrictions à l'égard des opérations visant des Canadiens.

Par respect pour mes collègues et compte tenu de la grande estime que j'ai pour vous, monsieur Quinn, je ne vais pas insister sur cette question.

Ce sera tout pour cette portion de notre séance.

Au nom de tous les membres du Comité, je tiens à vous remercier de votre présence et surtout de la franchise avec laquelle vous avez répondu à nos questions. Merci encore une fois.

Nous allons maintenant nous interrompre un instant.

● (1630)

_____(Pause)_____

● (1635)

Le président: Nous voilà de retour. J'ose espérer que tout le monde a bien entendu le maillet cette fois-ci.

Une députée: Pas vraiment.

Des voix: Ha, ha!

Le président: Non? Je vais devoir m'entraîner. Je devrais peut-être suivre un cours avec M. Bezan.

Chers collègues, nous accueillons maintenant M. Kolga qui est loin d'en être à sa première comparution devant notre comité.

Je crois pouvoir vous faire grâce des consignes d'usage. Vous avez cinq minutes pour nous présenter vos observations préliminaires.

Merci.

M. Marcus Kolga (agrégé supérieur, Institut Macdonald-Laurier, à titre personnel): Merci, monsieur le président et distingués membres du Comité.

Mes observations vont porter principalement sur les opérations d'information dans un contexte de guerre cybernétique et les menaces qui en découlent pour notre environnement d'information et notre sécurité nationale. Je vais vous entretenir des répercussions directes de la guerre de l'information menée par la Russie sur notre compréhension de l'invasion de l'Ukraine par Poutine ainsi que de la manière dont le gouvernement russe s'y prend pour intimider et réduire au silence ceux qui critiquent cette guerre au Canada.

La semaine dernière, Alina Kabaeva, dirigeante de l'un des grands médias d'État russes et partenaire de Vladimir Poutine, a affirmé que les opérations d'information menées par le gouvernement russe sont des armes de guerre. Elle a dit que l'information représente pour la Russie une arme dont l'importance n'a rien à envier à celle d'un fusil d'assaut Kalachnikov.

Au fil de la dernière décennie, la guerre de l'information est effectivement devenue l'un des outils de prédilection au sein de l'arsenal hybride et cybernétique de la Russie, alors que le Canada était directement ciblé. Ainsi, des campagnes de désinformation menées par la Russie ont ciblé des Canadiens pendant la pandémie et lors de la manifestation des camionneurs à Ottawa l'an dernier. D'autres opérations d'information russes ont visé les membres des Forces canadiennes basés en Lettonie. Dans le cadre de la campagne de Ghoswriter pour le compte de l'agence de renseignement militaire de la Russie, on a diffusé de faux reportages affirmant que les soldats canadiens ont propagé la COVID en Lettonie pendant la pandémie. Aujourd'hui, les discours antiukrainiens du Kremlin visent à éroder le soutien public en faveur de l'Ukraine et à intimider et déshumaniser les Canadiens d'ascendance ukrainienne, y compris ceux qui sont élus au gouvernement.

La guerre de l'information livrée par la Russie a d'abord et avant tout pour but de miner la confiance de la population envers nos démocraties et la cohésion de nos sociétés. On utilise comme armes à cette fin les enjeux et les discours les plus susceptibles de polariser les gens. On pousse à l'extrême des argumentaires exploitant les préjugés aussi bien conservateurs que libéraux en mettant de l'avant toutes les questions susceptibles de diviser les Canadiens.

Depuis la première invasion de l'Ukraine par la Russie en 2014, nous avons été témoins d'opérations d'information russes ciblant les chefs conservateurs et libéraux. Les premiers ministres Harper et Trudeau et leurs gouvernements ont ainsi été faussement accusés d'appuyer le néonazisme ukrainien par les médias d'État russe et leur constellation de plateformes mandataires. Tout cela parce que les gouvernements canadiens ont exprimé leur appui à la souveraineté de l'Ukraine et critiqué le régime de Poutine.

Depuis le début de la présente invasion russe, le Kremlin a considérablement intensifié ses campagnes d'information visant à éroder l'appui des Canadiens en faveur de l'Ukraine. Le Kremlin est particulièrement efficace à ce titre en multipliant les propos alarmistes quant à une éventuelle escalade du conflit armé, évoquant même le spectre d'une guerre nucléaire. C'est ce qui nous a empêchés de fournir des armements à l'Ukraine après que la Russie a envahi la Crimée en 2014. C'est également ce qui a fait en sorte que nous n'avons pas fait parvenir en Ukraine d'abord des missiles antichars tirés à l'épaule, puis de l'artillerie et des chars d'assaut. C'est ce qui nous empêche aujourd'hui de fournir des avions-chasseurs à l'Ukraine.

Il y a un an, on nous disait que l'opération spéciale de trois jours de Vladimir Poutine avait pour but de démilitariser et de dénazifier le gouvernement ukrainien. Ce même argumentaire quant au soutien ukrainien pour le nazisme est maintenant repris avec virulence pour déshumaniser et dévaloriser de façon discriminatoire les Canadiens d'ascendance ukrainienne. La diffusion de différents discours en ce sens entraîne une hausse alarmante des menaces et de la violence à l'encontre de Canadiens ayant des racines en Ukraine ou dans d'autres pays d'Europe centrale et de l'Est.

Il y a tout lieu de se préoccuper également des actions directes menées pour intimider les membres de ces communautés et les détracteurs du régime de Poutine. Un article publié récemment par *Meduza*, un média russe indépendant, nous apprend que l'ambassade de la Russie au Canada surveille de près les activités des membres de la diaspora russe et des détracteurs du régime de Poutine au Canada sur les médias sociaux. C'est ainsi qu'un Russo-Canadien a reçu de l'ambassade russe à Ottawa un avertissement lui indiquant: « Nous savons qui vous êtes; nous vous surveillons; nous savons ce que vous faites. » L'an dernier, le consul honoraire de l'Estonie à Toronto a reçu une lettre le menaçant d'une attaque à l'anthrax si les Estoniens ne retiraient pas leur soutien à l'Ukraine. En outre, différentes communautés diasporiques ont signalé des tentatives d'hameçonnage par courriel.

Les parlementaires canadiens sont eux-mêmes exposés à un barrage quotidien de courriels et de messages de trolls qui se servent des médias sociaux pour essayer d'influer sur leurs décisions. Des députés m'ont indiqué que leur appui à l'Ukraine les expose à des attaques fréquentes à partir de comptes anonymes sur les médias sociaux. De telles manœuvres d'intimidation politique, qu'elles soient artificielles ou non, peuvent mener au retrait du soutien politique et militaire à l'Ukraine.

● (1640)

Je vous ai surtout parlé des menaces qui nous viennent actuellement de la Russie, mais il ne faut pas oublier que les opérations d'information du gouvernement chinois mettent aussi constamment en péril notre sécurité nationale et la défense de notre pays.

Je n'en dirai pas plus pour l'instant, et je serai vraiment ravi de répondre à vos questions.

Le président: Merci, monsieur Kolga.

Monsieur Kelly, vous avez la parole pour six minutes.

M. Pat Kelly: Merci de votre intervention.

Lors de votre dernier témoignage au Comité il y a environ un an, vous aviez décrit la manière dont Poutine exploite les pays démocratiques et tente de diviser les alliances occidentales comme l'OTAN. De toute évidence, beaucoup de choses ont changé au cours de cette dernière année. Pour nous aider dans notre étude sur la cybersécurité, je me demandais comment a évolué votre réflexion sur la situation?

M. Marcus Kolga: Je pense que nous étions en mesure d'anticiper il y a un an que la Russie intensifierait ses opérations de désinformation dans le contexte de la guerre en Ukraine. Nous avions également prévu que la Russie tenterait d'affaiblir le soutien de la population canadienne envers l'Ukraine. Ces opérations de désinformation n'ont fait que s'intensifier au cours des 12 derniers mois.

En tant qu'observateur de ce type d'opérations et de discours, que j'analyse au quotidien, je suis profondément préoccupé par le fait que des individus au Canada, situé tant à l'extrême gauche qu'à l'extrême droite, adoptent certains de ces discours et les instrumentalisent pour diviser la population. Cela revient, en réalité, à légitimer certains de ces discours, qui s'inscrivent dans une stratégie de propagande russe. Je pense que dans un contexte de sécurité nationale, nous devrions être très inquiets par rapport à cette situation.

M. Pat Kelly: Vous avez déclaré que les Forces armées canadiennes ont été ciblées par des campagnes de désinformation. Pouvez-vous décrire en quoi elles consistent?

M. Marcus Kolga: Avec plaisir. Ces campagnes de désinformation contre nos Forces armées se poursuivent depuis l'année 2015 environ, date à laquelle le premier ministre Harper avait ordonné à nos forces de se rendre en Ukraine et en Lettonie dans le cadre de l'opération UNIFIER et de l'opération REASSURANCE. Lors de nos opérations en Lettonie, en 2017 ou 2018, les médias encadrés par l'État russe qui exercent leurs activités en Lettonie ont lancé une campagne de propagande. Par exemple, certaines de leurs histoires laissaient entendre que le ministre canadien de la Défense de l'époque, Harjit Sajjan, en raison de son apparence, était en réalité à la tête d'une armée musulmane dont l'objectif était de conquérir la Lettonie.

Un autre discours de propagande présentait une image de Russell Williams, un meurtrier en série déclaré coupable, en sous-vêtements féminins. On laissait ainsi entendre que le Canada avait envoyé cet individu diriger nos troupes pour, je cite, « homosexualiser » la Lettonie.

Ce sont deux discours bien connus dont les médias russes se sont servis pour cibler les Lettons russophones et les monter contre nos forces. Par ailleurs, j'ai mentionné...

● (1645)

M. Pat Kelly: Il me semble que ces campagnes étaient davantage conçues pour influencer la population d'un pays dans lequel nos Forces armées étaient déployées. Ce n'étaient pas nos Forces armées elles-mêmes qui étaient prises pour cible.

M. Marcus Kolga: Je n'en suis pas si certain. Ces campagnes s'adressaient précisément aux Lettons et aux russophones qui habitent en Lettonie, mais par la bande, elles visaient également nos Forces armées. Les médias russes tentaient de manipuler l'opinion publique en Lettonie pour monter ses habitants contre nos troupes.

M. Pat Kelly: D'accord, j'ai compris. Tout ça est vraiment hallucinant.

Vous avez parlé des bureaux consulaires de l'ambassade russe au Canada, ainsi que de la mission diplomatique. Vous avez décrit la manière dont ces officines font de l'intimidation contre les citoyens canadiens et contre les diasporas ukrainienne et russe au pays.

En ce qui a trait aux cyberattaques, y compris celles qui peuvent être lancées à partir du Canada au moyen des missions diplomatiques russes, diriez-vous que nous sommes toujours en retard par rapport à nos alliés, pour ce qui est d'appliquer les sanctions prévues dans la loi de Magnitski? Sommes-nous capables d'identifier des individus qui portent atteinte à notre sécurité, ici au Canada, et sommes-nous en mesure de sévir contre eux?

M. Marcus Kolga: Je vous remercie de votre excellente question.

Je pense que nous pourrions déployer notre régime de sanctions de manière plus efficace pour cibler les organes de propagande russes qui répandent ce genre de discours visant à nuire aux intérêts du Canada et de l'Ukraine. Nous devrions veiller à ce que ce genre de sanctions soient appliquées. Nous devrions également faire en sorte que les Canadiens ne contribuent pas, consciemment ou non, aux plateformes utilisées par les médias d'État russes pour lancer des opérations de désinformation contre notre pays.

J'ai vu récemment quelques Canadiens accepter une invitation sur RT. Il s'agit de la chaîne de médias étatiques de la Russie qui a été écartée de nos ondes depuis près d'un an déjà, et qui figure sur notre liste de sanctions. Nos citoyens devraient refuser toute invitation de la part de RT, et éviter de faire le jeu des campagnes de désinformation orchestrées par cette plateforme.

À mon avis, nous devons faire appliquer nos sanctions contre ce genre de plateformes de propagande russes. Il faut éviter que les Canadiens tombent dans le piège ou puissent tirer profit d'une manière ou d'une autre de leur apparition sur ces plateformes. Nous devons empêcher les Russes d'instrumentaliser des Canadiens pour légitimer leurs discours.

Le président: Il vous reste environ 15 secondes.

M. Pat Kelly: Devrions-nous continuer de permettre à la Russie d'avoir une représentation consulaire au Canada, ou doit-on obliger le personnel à faire ses valises?

M. Marcus Kolga: Devrions-nous...

M. Pat Kelly: Comme il vous reste très peu de temps, répondez par oui ou par non, je vous prie.

Le président: Je trouve intéressant que lorsqu'on avertit un député qu'il ne lui reste que 10 secondes, il parvienne quand même à poser une dernière question pour arracher une dernière bribe d'information au témoin.

Si vous pouvez obtenir une réponse du témoin en 10 secondes, alors allons-y.

M. Marcus Kolga: Je me demande pourquoi la Russie a besoin de maintenir une équipe de près de 80 diplomates, voire plus, au Canada. À mon avis, c'est un non-sens. Que font tous ces gens ici?

Le président: D'accord. Nous allons maintenant passer à M. May.

Monsieur May, la parole est à vous pour six minutes.

M. Bryan May: Je vous remercie, monsieur le président.

D'abord, je tiens à vous remercier de vous être de nouveau joint à nous pour nous aider à mener cette étude.

Je sais que nous venons tout juste d'entamer cette étude, mais nous entendons de plus en plus parler des risques encourus par nos infrastructures essentielles et, en particulier, de la façon dont elles pourraient être la cible de cyberattaques commanditées par des États. Ce genre d'attaques permettrait à nos adversaires d'attaquer notre pays ou l'un de nos alliés sans avoir recours à des moyens militaires conventionnels.

À votre avis, quels sont les secteurs les plus vulnérables?

● (1650)

M. Marcus Kolga: Les secteurs les plus vulnérables aux cyberattaques russes sont évidemment les infrastructures essentielles.

Nous avons constaté au cours des derniers mois, depuis au moins un an en fait, que notre secteur de la santé est devenu la proie de rançongiciels. Un grand nombre d'organisations qui se livrent à des activités criminelles comme l'utilisation de rançongiciels sont établies en Russie, leurs activités ayant reçu l'aval du Kremlin. Je pense que les autorités russes représentent hors de tout doute une menace pour nos infrastructures de santé et l'ensemble de nos infrastructures essentielles. Lors de l'invasion de l'Ukraine, le régime russe a fait la démonstration qu'il est prêt à s'en prendre aux infrastructures essentielles d'un pays. S'il a agi ainsi en Ukraine, je ne vois pas pourquoi il épargnerait le Canada ou nos alliés.

J'imagine qu'à l'heure actuelle, toute l'attention du régime russe est concentrée sur l'Ukraine, mais que le Canada pourrait éventuellement être aussi dans sa mire.

M. Bryan May: Le Canada est-il suffisamment protégé? Comment pourrions-nous renforcer la protection de nos infrastructures essentielles?

M. Marcus Kolga: Je ne peux pas vous répondre sur ce point précis. Mon champ d'expertise se limite à l'enjeu de la désinformation. Je crois savoir que le Centre de sécurité des télécommunications, ou CST, s'intéresse de près à cette question.

M. Bryan May: Pourriez-vous formuler des recommandations quant aux améliorations à apporter aux politiques en place? Devrait-on élaborer de nouvelles politiques dans ce domaine?

M. Marcus Kolga: Je pense que la solution passe en grande partie par la sensibilisation. Au cours des dernières années, nous avons constaté que ce sont des problèmes de cyberhygiène de base qui ont exposé certaines grandes institutions à des cyberattaques. Il faut faire de la sensibilisation et nous assurer que les personnes qui travaillent au sein de nos institutions, incluant le gouvernement, possèdent de solides compétences en matière de cyberhygiène, notamment l'utilisation de mots de passe robustes. Selon moi, c'est par là que nous devons commencer pour protéger nos infrastructures essentielles et nos institutions.

M. Bryan May: Le signalement d'une cyberattaque devrait-il être obligatoire?

M. Marcus Kolga: Il s'agit d'une très bonne question. Je serais porté à dire qu'en effet, de telles attaques devraient être signalées. Je ne pense pas que nous aurions avantage à les balayer sous le tapis. De cette manière, nous allons acquérir une meilleure compréhension de l'origine des menaces.

M. Bryan May: De quelle façon le gouvernement fédéral peut-il mieux collaborer avec les gouvernements provinciaux et territoriaux afin de renforcer la défense de nos infrastructures essentielles?

M. Marcus Kolga: Je ne pourrais pas me prononcer précisément sur la relation que le gouvernement fédéral entretient à l'heure actuelle avec les provinces et les territoires en matière de cybersécurité.

M. Bryan May: Est-ce qu'il me reste du temps, monsieur le président?

Le président: Il vous reste deux minutes.

M. Bryan May: Vous vous êtes jusqu'à présent beaucoup concentré sur la Russie. Y a-t-il d'autres acteurs potentiellement menaçants dont nous devrions nous méfier dans le contexte actuel?

M. Marcus Kolga: Tout à fait. La Russie mène des cyberattaques depuis très longtemps, mais la Chine se dote de moyens de plus en plus sophistiqués dans ce domaine; nous devrions donc la surveiller de très près. La Chine est en train de renforcer ses capacités en matière de cyberattaques, et je suis certain que le Canada va devenir, et il l'est d'ailleurs déjà, la cible de cyberactivités chinoises.

M. Bryan May: En quoi les cyberactivités menées par la Chine sont-elles différentes de celles de la Russie?

M. Marcus Kolga: Comme je ne suis pas un expert en cybernétique, je ne peux pas répondre précisément à cette question. Je ne saurais vous dire en quoi la menace posée par la Chine diffère de celle de la Russie.

M. Bryan May: Voyons voir si je peux aborder ma question sous un autre angle.

Vous nous avez parlé de certaines campagnes de désinformation et de certains événements qui se sont produits au Canada au cours des dernières années. Comment le gouvernement fédéral peut-il s'occuper du volet de la sensibilisation sans que cela ait l'air partisan? Une campagne de sensibilisation mise sur pied par tel ou tel parti politique pourrait avoir une connotation partisane.

M. Marcus Kolga: Vous avez tout à fait raison. Tout effort visant à s'attaquer précisément à la désinformation d'acteurs étrangers se doit d'être non partisan. Je plaide depuis longtemps en faveur d'une approche pansociétale. Je suis également d'avis que le Parlement canadien pourrait éventuellement se doter d'un comité multipartite chargé d'étudier l'enjeu de la désinformation.

● (1655)

M. Bryan May: Quels sont les pays qui ont connu du succès dans ce domaine?

M. Marcus Kolga: Je songe à plusieurs pays qui font un excellent travail. Il s'agit de pays qui partagent une frontière avec un voisin qui mène des activités de désinformation, notamment l'Estonie, la Lettonie et la Lituanie. Je pense aussi à Taïwan, qui fait un travail exceptionnel dans la lutte contre la désinformation chinoise. Par ailleurs, la Finlande et la Suède ont intégré des activités de sensibilisation à la désinformation dans les programmes d'éducation de la petite enfance. Ils s'assurent ainsi que toutes les prochaines générations de Suédois et de Finlandais disposent des ressources cognitives nécessaires pour évaluer de manière critique les informations auxquelles ils sont exposés.

Le président: Je vous remercie, monsieur May.

[*Français*]

Soyez le bienvenu au Comité, monsieur Perron.

Vous avez la parole pour six minutes.

M. Yves Perron (Berthier—Maskinongé, BQ): Je vous remercie, monsieur le président, de me recevoir au Comité.

Monsieur Kolga, je vous remercie d'être parmi nous aujourd'hui.

Dans votre dernière réponse, vous avez mentionné que vous saviez déjà que le Canada était la cible de cyberattaques des Chinois.

Pouvez-vous nous en dire davantage?

[*Traduction*]

M. Marcus Kolga: Nous savons que la Chine nous a pris pour cible et a tenté de miner notre démocratie au moyen de campagnes de désinformation au cours des trois dernières élections.

Au cours de la dernière campagne électorale, DisinfoWatch, l'organisme que j'ai fondé et que je préside, a débusqué certains acteurs étatiques chinois qui se sont adonnés à des activités de désinformation en utilisant les médias d'État. Nous avons également constaté que différentes plateformes canadiennes en langue chinoise se sont mises à véhiculer certains de ces discours en ciblant un parti politique en particulier.

Au chapitre de la désinformation étrangère, je peux vous dire que le Canada a souvent été la cible de la Chine au cours des deux ou trois dernières années au moins.

[*Français*]

M. Yves Perron: Merci beaucoup.

Il y a même des rumeurs de financement de certains candidats. Je présume que vous n'avez pas de données là-dessus.

[*Traduction*]

M. Marcus Kolga: Non, je n'ai malheureusement pas de données sur les candidats qui ont reçu du financement et du soutien du gouvernement chinois.

[*Français*]

M. Yves Perron: Revenons à la préparation du Canada en vue de se défendre de futures cyberattaques.

Comment qualifieriez-vous la capacité du Canada à se défendre dans une guerre hybride, c'est-à-dire une guerre où il y aurait une attaque partiellement physique, mais très cybernétique? Le Canada est-il équipé pour y faire face? Est-il assez développé de façon indépendante de ses alliés?

En effet, le Canada pourrait perdre, par exemple, la capacité de défense des États-Unis sporadiquement. Le Canada se retrouverait-il vraiment démuni, dans un tel cas?

Je sais que c'est une grande question.

[*Traduction*]

M. Marcus Kolga: Lorsque nous parlons de guerre hybride, de cybernétique et du domaine de l'information, le Canada pourrait avoir du mal à se défendre.

D'après ce que j'ai compris, les FAC étaient en train de développer des capacités de défense contre la guerre psychologique et les activités d'information. Cet effort a été interrompu en 2020, d'après ce que j'ai compris, en raison de certains reportages dans les médias qui laissaient entendre que les Forces armées canadiennes se préparaient à utiliser la guerre psychologique et les activités d'information contre les Canadiens. Je ne suis pas sûr qu'il y avait beaucoup de preuves à l'appui.

Depuis, les Forces armées canadiennes ne semblent pas avoir continué ou commencé à perfectionner ces efforts pour défendre nos forces contre les activités d'information que j'ai mentionnées plus tôt, y compris la campagne d'hameçonnage du service de renseignement militaire russe, GRU, qui ciblait des membres de nos forces en Lettonie en laissant entendre qu'ils répandaient la COVID dans ce pays. D'après ce que j'ai compris, les Forces armées canadiennes ne disposent pas des capacités nécessaires pour se défendre contre ces types d'attaques d'information à l'heure actuelle.

[*Français*]

M. Yves Perron: La question a été posée tantôt, toutefois, avez-vous une recommandation précise sur cet aspect?

Quelles mesures faudrait-il prendre?

Je sais qu'en 2020, il y a eu un doute et que ces opérations ont cessé. Cependant, il faut trouver l'équilibre entre la protection de la vie privée des citoyens et la protection nationale. Ce n'est pas facile.

● (1700)

[*Traduction*]

M. Marcus Kolga: Encore une fois, c'est une excellente question.

Ayant lu certaines informations sur ces capacités lorsqu'elles étaient en train d'être développées, je sais que les Forces armées canadiennes prennent très au sérieux la guerre de l'information et la guerre psychologique. Comme je l'ai mentionné plus tôt, la partenaire de Vladimir Poutine, Alina Kabaeva, a dit que l'information était comme une kalachnikov. Je pense que nos forces armées le comprennent également.

Il n'a jamais été question que les activités d'information soient utilisées contre des citoyens canadiens. Elles n'allaient être utilisées que là où il y avait des activités actives. Le fait que nos forces armées n'aient pas cette capacité à l'heure actuelle est inquiétant pour quelqu'un comme moi qui surveille et analyse les activités d'information étrangères...

[*Français*]

M. Yves Perron: Merci beaucoup.

Que savez-vous de l'informatique quantique qui se développerait de façon assez importante et qui pourrait révolutionner les capacités de piratages de l'extérieur?

Considérez-vous que nous sommes laxistes à cet égard?

Est-ce qu'il se prépare quelque chose, au Canada? Sommes-nous en train de nous préparer à ces potentielles attaques?

[*Traduction*]

M. Marcus Kolga: Je trouve que toutes les technologies futures sont très préoccupantes, surtout lorsqu'il s'agit du domaine de l'information. L'intelligence artificielle évolue très rapidement. La vitesse à laquelle nos adversaires étrangers peuvent diffuser de l'information et de la désinformation va devenir très alarmante. Je ne suis pas certain que nous sommes prêts à faire face à cette menace croissante.

L'autre menace qui prend de l'ampleur et qui deviendra problématique dans les années à venir est la création d'hypertrucages. Il s'agit de fausses vidéos, de fausses images et de faux enregistrements audio qui sont de plus en plus créés par l'intelligence artificielle. Cette technologie prendra une image du président Biden, par exemple, et fera croire qu'il dit quelque chose qu'il ne dit pas en réalité. La technologie utilisée pour créer ces vidéos devient d'une précision terrifiante.

Je répète que je ne suis pas certain que nous sommes prêts à faire face à l'émergence de ces hypertrucages.

[*Français*]

Le président: Merci, monsieur Perron.

[*Traduction*]

Le prochain intervenant est M. Bachrach, pour six minutes.

M. Taylor Bachrach: Merci, monsieur le président, et merci, monsieur Kolga, de votre témoignage jusqu'à présent.

Vous avez écrit à propos de l'incidence de la désinformation sur différents événements, y compris la pandémie, le convoi et la guerre en Ukraine. Je suis curieux d'en savoir plus, en commençant peut-être avec la pandémie.

Pourriez-vous expliquer un peu si, à votre avis, ces tentatives de désinformation par des acteurs étrangers ont eu des répercussions plus précisément sur le discours politique concernant la pandémie? Avez-vous vu si ces efforts ont eu une incidence sur l'évolution du discours politique au Canada au cours des trois dernières années?

M. Marcus Kolga: Merci de cette question...

Le président: Je suis désolé. Attendez une seconde.

C'est une bonne question et une question intéressante, mais nous nous éloignons un peu de l'étude.

M. Marcus Kolga: Je vous remercie, monsieur le président.

Les activités d'information étrangères — les cyberopérations — dans ce contexte visaient absolument le Canada pendant la pandémie. Nous l'avions déjà prévu en 2020, alors que la pandémie ne faisait que commencer. Nos alliés de l'Union européenne au StratCom de l'Est avaient également prévu que les acteurs étrangers, y compris la Russie, utiliseraient la désinformation et les plateformes en ligne, notamment, pour intensifier les effets de la pandémie.

Au cours de l'été 2020, nous avons vu des plateformes telles que RT et d'autres plateformes de médias d'État russes légitimer des mouvements contre la vaccination et contre le confinement en Allemagne. Nous les avons également vues donner une plateforme et amplifier des mouvements semblables en Amérique du Nord, y compris ici même au Canada. Une organisation anti-confinement extrêmement agressive qui avait un compte sur Twitter avait passé l'année ou les deux années précédant l'invasion russe de l'Ukraine à publier des messages contre la vaccination et contre le confinement. Le 24 février, ces messages sont devenus des messages contre l'Ukraine. En fait, cette organisation a publié et amplifié des messages soutenus par l'ambassade russe ici même au Canada, et a continué à le faire plusieurs centaines de fois en février et en mars.

Nous avons vu un lien clair et distinct entre les deux. Nous avons certainement vu les acteurs étatiques russes amplifier ces messages durant la COVID.

● (1705)

M. Taylor Bachrach: Je vous remercie, monsieur Kolga.

En ce qui concerne les observations précédentes du président, je suis curieux de savoir si vous pensez que la désinformation est une forme de menace pour la cybersécurité. Vous pourriez peut-être nous dire si le milieu de la cybersécurité au Canada la reconnaît comme telle.

M. Marcus Kolga: Eh bien, tout à fait. La désinformation est souvent une forme de communication numérique. Elle est utilisée par nos adversaires, comme je l'ai mentionné plus tôt, pour déstabiliser notre démocratie, pour nous monter les uns contre les autres. Ils le font à l'aide de différentes plateformes de médias sociaux.

J'ai mentionné également que le courrier électronique est utilisé à cette fin, et puis, bien sûr, dans le domaine cybernétique, nous voyons des tentatives de divulgation et d'hameçonnage pour essayer d'attirer les gens à fournir des données et autres et nous voyons des individus ouvrir leurs ordinateurs aux cyberattaques ou aux cyberpirates pour voler des données et autres. C'est ce qui s'est passé en 2016, bien sûr, lorsque des pirates russes ont pénétré dans les serveurs du Parti démocrate, ont volé des informations et les ont exposées. Il existe une ligne floue entre la cyberactivité et la désinformation. Je pense qu'elles appartiennent tout à fait au même domaine.

M. Taylor Bachrach: Je vous remercie.

Pour poursuivre dans la même veine, vous avez mentionné des tentatives de désinformation liées à la pandémie, au convoi et à la guerre en Ukraine. Vous avez aussi mentionné que les parlementaires canadiens ont été la cible de certaines de ces tentatives de désinformation.

À votre avis, les parlementaires canadiens se sont-ils montrés vulnérables à ces attaques de désinformation? Pourriez-vous donner quelques exemples de la façon dont cela pourrait être le cas?

M. Marcus Kolga: Il y a eu des cas clairs où des parlementaires provinciaux en Ontario ont été victimes d'activités d'information étrangères pendant la pandémie. Un député provincial de l'Ontario soutenait des opinions contre la vaccination et contre le confinement, ce qui est parfaitement normal au Canada, mais le gouvernement russe, les médias d'État russes, l'ont reconnu et lui ont demandé de se rendre sur RT. Il a été invité sur RT, ce qui a contribué à fournir une plateforme mondiale pour ses opinions. Après avoir donné une entrevue sur RT, il a écrit sur Twitter à tous les abonnés qu'ils ne devaient pas suivre les médias traditionnels mais plutôt RT, car les médias d'État russes étaient les seuls dignes de confiance...

Le président: Nous allons devoir...

M. Marcus Kolga: ... donc, oui, il y a certainement des parlementaires qui ont...

Le président: Nous allons devoir laisser tomber le rester de la réponse.

Encore une fois, chers collègues, nous sommes dans la même situation que d'habitude: il nous reste 20 minutes et 25 minutes de questions. Je vais prendre une minute sur le temps de parole de chacun, et nous commencerons avec Mme Kramp-Neuman.

Mme Shelby Kramp-Neuman: Je vous remercie.

Monsieur Kolga, merci de votre intéressant témoignage qui donne matière à réflexion.

J'aimerais ajouter à ce que mon collègue a suggéré plus tôt dans la conversation que vous avez eue concernant le fait que nos forces sont régulièrement ciblées. Comment pouvons-nous mieux former le personnel des FAC pour nous assurer qu'il est équipé pour relever les défis associés à la guerre cognitive et à la cybersécurité?

● (1710)

M. Marcus Kolga: Je vous remercie. C'est une excellente question.

Je ne pense pas qu'il s'agisse uniquement de nos forces. Je pense qu'il faut une sensibilisation plus exhaustive en général pour tous les Canadiens afin qu'ils puissent reconnaître les activités d'information et se défendre contre elles. Dans le contexte de nos forces, encore une fois, je pense que nous devons créer cette capacité à gérer directement ces messages que j'ai mentionnés plus tôt, à les contester et à les repousser.

Dans une situation de conflit, comme nous l'avons vu en Ukraine, la Russie n'hésite pas. La guerre cognitive est un outil extrêmement important dans la boîte à outils, et nous devons nous assurer que nous disposons des capacités nécessaires pour faire face à ces menaces et passer à l'offensive contre nos adversaires lorsqu'ils s'engagent dans ce type de guerre.

Mme Shelby Kramp-Neuman: Je vous remercie.

Dans les observations que vous avez formulées le 16 février 2022, il y a près d'un an, vous avez mentionné que la cybernétique sera le principal champ de bataille du XXI^{e} siècle et que le Canada a besoin de ressources et de connaissances pour relever ces défis. Je pense que vous aviez une boule de cristal.

Un an plus tard, le Canada a-t-il suivi ce conseil et s'est-il préparé à gérer ces menaces?

M. Marcus Kolga: Je pense que le Canada et tous nos alliés ont eu une énorme prise de conscience le 24 février de l'année dernière. Je pense que la plupart d'entre nous, y compris le Canada, ont rapidement renforcé leurs capacités pour tenter de faire face à cette menace. Je pense que maintenant, enfin, notre gouvernement et certainement nos forces et celles de nos alliés prennent la menace russe au sérieux.

Sommes-nous préparés? Sommes-nous mieux préparés? Je dirais que nous le sommes. Sommes-nous complètement préparés? Probablement pas.

Mme Shelby Kramp-Neuman: D'accord. L'état d'urgence a certainement été noté, mais il est temps de continuer dans la voie que nous avons empruntée.

En outre, vous avez écrit à plusieurs reprises sur l'importance de l'infrastructure de l'industrie énergétique pour la guerre en Russie. Vous avez indiqué que le Canada a été victime du chantage et de la tromperie de Poutine en matière d'énergie.

Comment des cyberattaques dans le secteur de l'énergie pourraient-elles jouer un rôle dans la réussite ou l'échec de cette guerre avec la Russie? À l'heure actuelle, dans quelle mesure l'industrie énergétique du Canada est-elle vulnérable à une attaque?

M. Marcus Kolga: Je n'ai pas d'évaluation de la qualité de la défense de notre industrie énergétique. Je pense que chaque entreprise a probablement ses propres protocoles.

Je pense qu'il serait sage, en tant que nation, d'essayer d'élaborer une sorte de normes en matière de cybersécurité pour différentes industries et autres, afin qu'il y ait des lignes directrices pour ces entreprises, qu'il s'agisse des exploitations pétrolières ou des sociétés de pipelines, pour qu'elles comprennent les normes minimales qu'elles doivent respecter afin de se protéger. Je ne pense pas que nous en soyons encore là, mais c'est une politique que nous devrions envisager.

Mme Shelby Kramp-Neuman: Comme dernière question avec le temps qui m'est imparti, pensez-vous que suffisamment de mesures ont été prises pour protéger les infrastructures civiles contre les pannes potentielles?

M. Marcus Kolga: Nous pouvons toujours faire plus. La menace évolue sans cesse, et nous devons nous assurer que nous suivons son évolution. Je crois comprendre que les capacités du CST s'accroissent, mais nous devons nous assurer que, dans les organisations en question qui contrôlent les différentes parties de l'infrastructure, les employés sont bien formés et savent comment se défendre contre ces cyberattaques. Je ne suis pas sûr que nous en soyons encore là.

Le président: Merci, madame Kramp-Neuman.

Madame O'Connell, vous avez la parole pendant quatre minutes.

Mme Jennifer O'Connell: Merci, monsieur le président.

Je vous remercie de votre présence, monsieur Kolga. J'ai quelques questions à vous poser.

En ce qui concerne les plans et les capacités des FAC pour lutter contre la désinformation qui vise nos troupes, vous avez déclaré que les forces n'en avaient pas. Mais est-ce vraiment une évaluation correcte de la situation? Pourquoi publierions-nous des informations en ligne, par exemple, ou pourquoi les FAC communiqueraient-elles leurs plans d'attaques à venir et d'autres renseignements de ce genre pour permettre à nos adversaires d'en prennent connaissance?

M. Marcus Kolga: Je vous remercie de votre question.

Je pense que le commandement du renseignement des FAC fait un excellent travail en affichant les différents récits de désinformation que la Russie diffuse en ce moment et en les démystifiant. Cette capacité existe certainement du point de vue des affaires publiques. Cependant, si nos forces étaient engagées dans un conflit, elles n'auraient plus accès à la capacité tactique, qui a été développée jusqu'en 2020.

Je ne sais pas si, à l'heure actuelle, on discute de la possibilité de reconstituer ou développer cette capacité dans les FAC. En ce moment, lorsque nos forces sont engagées dans un conflit, elles n'ont pas la capacité de se défendre ou de passer à l'offensive contre un adversaire qui a recours à la guerre psychologique ou à des opérations d'information.

● (1715)

Mme Jennifer O'Connell: Cette clarification concerne-t-elle précisément les situations de conflit?

M. Marcus Kolga: Oui.

Mme Jennifer O'Connell: D'accord.

En ce qui concerne la désinformation ou la mésinformation, vous avez parlé d'exemples liés à la COVID-19 et aux mouvements antivaccins. Je pense que c'était en réponse à une question concernant la vulnérabilité des parlementaires, et vous avez donné un bon exemple de quelqu'un qui fait la promotion de la télévision russe. Les informations à venir seraient alors envoyées à un nouveau groupe de personnes qui, autrement, ne seraient probablement jamais tombées sur la chaîne de télévision RT.

J'ai remarqué la même chose aux États-Unis. Un grand nombre d'humoristes américains présentent, d'une manière qui se veut satirique, certaines de ces croyances dans le cadre de fausses entrevues ou en posant des questions. J'ai vu des entrevues dans lesquelles les gens pensent que l'ancien président Trump est toujours président, ou qu'il y a deux armées, une que le président contrôle et une qu'il ne contrôle pas. En fait, c'est triste à regarder parce que ces gens croient vraiment ces informations.

Sachant comment cette désinformation voit le jour, puis vole de ses propres ailes, n'est-ce pas là le but de nos adversaires étrangers? La désinformation ne cible pas vraiment les vaccins, les complots liés à la COVID-19 ou les confinements; elle cherche vraiment à éveiller la méfiance envers le gouvernement. Quand j'utilise cet exemple comique, je cherche en fait à dire que nous ne faisons plus confiance à nos dirigeants. Nous ne croyons même pas au résultat des élections. La désinformation cherche en fait à détruire les institutions démocratiques.

M. Marcus Kolga: Je vous remercie encore une fois, je crois, de votre question.

Le problème survient lorsque nos adversaires étrangers s'emparent de ces enjeux, qui nous polarisent, et les utilisent contre nous. En tant que Canadiens, nous jouissons du droit à la liberté d'expression. Par conséquent, si nous n'aimons pas notre gouvernement, nous sommes tout à fait libres de dire que nous ne l'aimons pas. Si nous n'aimons pas la politique de vaccination et si nous ne voulons pas être vaccinés, nous sommes également libres de faire ce choix.

Lorsqu'un adversaire étranger, comme les médias d'État russes, nous dit que le vaccin va nous tuer, il n'a pas la liberté de le faire. Ses propos nous occasionnent des coûts et pourraient causer des décès, et c'est à ce moment-là que nous devons prendre la parole et faire reculer cet adversaire.

Le président: Merci, madame O'Connell. Je suis désolé de l'interruption.

[*Français*]

Monsieur Perron, vous avez une minute.

M. Yves Perron: Merci, monsieur le président.

Monsieur Kolga, quand nous avions terminé tantôt, on parlait d'informatique quantique et vous me disiez que nous n'étions pas préparés. Vous avez aussi parlé d'hypertrucages, et vous avez dit que, là encore, nous n'étions pas préparés.

J'aurais envie de vous parler du « left of launch ». Je ne sais pas si vous êtes au courant de cette rumeur. Il semble qu'il y aurait des capacités de piratage du lancement des missiles. Cela aurait déjà été testé.

Que doit-on faire pour se préparer à ces menaces?

Vous avez l'occasion de faire une recommandation au gouvernement pour qu'on soit mieux préparé.

[*Traduction*]

M. Marcus Kolga: Afin d'être mieux préparés, nous devons nous assurer que nous disposons des ressources nécessaires pour former des spécialistes de ce domaine, pour que les programmeurs soient capables de localiser ces menaces et de les reconnaître lorsqu'elles visent nos systèmes militaires et nos infrastructures essentielles. C'est la seule façon de nous défendre contre ces menaces.

[*Français*]

M. Yves Perron: Serait-il pertinent de créer un comité transpartisan sur la désinformation au Canada?

● (1720)

[*Traduction*]

M. Marcus Kolga: Absolument. Je pense qu'il faudrait créer un comité pour les cybermenaces et, je dirais, un autre pour la désinformation. Un comité multipartite semblable au Comité des parlementaires sur la sécurité nationale et le renseignement pourrait être créé, un comité non partisan qui pourrait se réunir régulièrement pour discuter de la désinformation. Les récits de désinformation pourraient y être mis en lumière et discutés. Tous les partis pourraient convenir ou non qu'il s'agit de récits de désinformation étrangers et en informer les membres de leur caucus.

Le président: Merci.

Vous avez la parole pendant une minute, monsieur Bachrach.

M. Taylor Bachrach: Merci, monsieur le président.

Monsieur Kolga, vous avez fait valoir que l'établissement national de cybersécurité devrait avoir une stratégie pour combattre la désinformation émanant d'acteurs étrangers. Nos organismes de sécurité devraient-ils également se préoccuper de la désinformation dangereuse qui provient de sources nationales?

M. Marcus Kolga: Absolument, et je crois que nos organismes de renseignement restent à l'affût de tout. Plus précisément, le SCRS surveille l'extrémisme intérieur et les autres menaces, tout comme la GRC. Cela se produit certainement, mais je ne crois pas que nous fassions un travail remarquable ou efficace de surveillance de la façon dont les acteurs étrangers amplifient et intensifient la radicalisation au sein de certaines de ces organisations, car cela arrive. Ces types de récits surgissent des plateformes étatiques et de leur multitude d'intermédiaires. Les intermédiaires russes, en tout cas, contribuent à alimenter cette radicalisation et cet extrémisme qui sévissent actuellement.

Le président: Merci, monsieur Bachrach. Je vous présente toutes mes excuses; mes collègues me reprochent de mal prononcer votre nom depuis deux heures.

Des voix: Ha, ha!

M. Taylor Bachrach: Cela ne pose pas de problème, monsieur le président. Je réponds à pratiquement toutes les appellations.

Le président: Eh bien, je ne vous invite pas à dîner. Alors, voilà où vous en êtes.

Des voix: Ha, ha!

Le président: Ces mauvaises blagues deviennent embarrassantes, n'est-ce pas?

Vous avez la parole, madame Gallant.

Mme Cheryl Gallant: Merci.

Comment la Chine tire-t-elle parti de la désinformation diffusée par la propagande russe à ses propres fins?

M. Marcus Kolga: C'est une excellente question.

Nous assistons actuellement à un rapprochement entre la désinformation chinoise et la désinformation russe. Elles se soutiennent mutuellement. L'écosystème d'information chinois ou son écosystème médiatique, pour ainsi dire, répète assurément la désinformation russe, en ce qui concerne l'Ukraine et d'autres sujets. Les médias d'État russes font de même avec la Chine. Ils travaillent de concert en ce moment et se soutiennent mutuellement.

Mme Cheryl Gallant: Nous disposons de cyberguerriers de haut niveau, mais ils ne veulent pas être déployés sur un théâtre de guerre. Dans quelle mesure est-il nécessaire que nos cyberguerriers puissent être déployés?

M. Marcus Kolga: Eh bien, en ce qui concerne les cyberguerriers, je dirais aussi que, dans le domaine de la désinformation, il est très important que nous disposions de capacités offensives et que nous ripostions. Je pense que nous avons passé les dernières années à tenter de comprendre à quoi ressemble cette menace et comment nous en défendre. Si nous sommes constamment sur la défensive, nous ne parviendrons pas à arrêter la Russie ou la Chine.

L'Ukraine a également démontré que la seule façon d'arrêter l'agression de Poutine est de l'arrêter lui-même. Cela veut dire qu'il faut passer à l'offensive et repousser les attaques, comme l'Ukraine le fait actuellement en contrant les forces russes. Nous devons faire de même dans le domaine cybernétique en contrant la désinformation. C'est en repoussant les attaques et en passant à l'offensive que nous arrêterons Vladimir Poutine et les autres dirigeants autoritaires semblables à lui.

Mme Cheryl Gallant: Toutefois, pouvons-nous le faire sans enrôler dans l'armée les personnes qui sont très douées pour faire exactement ce que vous venez de décrire?

M. Marcus Kolga: Eh bien, je pense que certaines de ces personnes deviennent chevronnées en n'étant pas nécessairement toujours... C'est une bonne question. Je dirais qu'à mon avis, nous pouvons former les bonnes personnes, au moins dans le domaine de l'information. Nous n'avons pas besoin de recruter des acteurs qui travaillent avec d'autres groupes, qu'il s'agisse d'organisations criminelles ou d'adversaires étrangers. Nous pouvons les former ici même, au Canada.

Mme Cheryl Gallant: D'accord.

L'un des récits qui se propagent, c'est que de hauts responsables ukrainiens utilisent à leurs propres fins les contributions internationales à l'effort de guerre. Comment peut-on démasquer cette désinformation afin de ne pas contrer les efforts des parlementaires canadiens qui tentent de faire ce qui s'impose pour protéger la démocratie dans le monde entier?

● (1725)

M. Marcus Kolga: Je vous remercie de votre question.

C'est l'un des principaux récits que la Russie essaie de promouvoir en Occident pour tenter d'éroder le soutien que nous apportons à l'Ukraine. Ce sont les faits et la vérité qui démoliront ce récit. Le fait que l'Ukraine lutte contre la corruption en Ukraine...

Tout le soutien militaire que nous leur envoyons est suivi de près et contrôlé. Ces récits qui insinuent que certains de ces équipements sont vendus sur le marché noir sont complètement faux, et des preuves existent à cet égard. Le problème, c'est que les médias d'État russes ignorent les faits. Ils ne rapportent pas la vérité, et ils continueront de diffuser des mensonges de ce genre. Tout ce que nous pouvons faire, c'est nous assurer que nos médias connaissent les faits, que nos élus connaissent les faits, lorsqu'ils parlent de soutenir l'Ukraine, que ces faits sont diffusés adéquatement dans notre pays et que les Canadiens en sont informés.

Le président: Merci, madame Gallant.

Monsieur Fisher, vous avez la parole pendant les quatre dernières minutes.

M. Darren Fisher: Merci, monsieur le président.

Merci, monsieur Kolga.

Certains sujets commencent à s'embrouiller un peu, et certaines des questions identiques sont posées par les mêmes personnes.

Je crois que vous étiez là, au fond de la salle, pendant la première heure de la réunion. L'étiez-vous?

M. Marcus Kolga: Oui, j'étais là.

M. Darren Fisher: J'ai également posé la question suivante au cours d'une réunion antérieure. La réponse donnée aujourd'hui par le contre-amiral était très différente de celle que j'ai reçue la semaine dernière. Je veux vous demander votre point de vue à ce sujet.

En général, le monde croit que la Russie est une cyberpuissance et, vraisemblablement, on peut dire qu'elle l'est. Nous pensons qu'elle est la plus douée en matière de désinformation et de cyberguerre. Je crois que le monde entier estimait également qu'elle était une superpuissance militaire. Je pense que certaines de ces idées ont été démenties au cours de l'année dernière.

Je suis curieux de savoir ce que vous pensez de leur philosophie de guerre hybride, qui consiste à utiliser un peu de cyberattaques et à y ajouter une bombe. Je sais que cette question a été effleurée avec certains des autres députés, mais j'aimerais connaître vos réflexions à propos de la question de savoir si les Russes sont décevants dans le domaine cybernétique et le domaine militaire, ou si vous pensez que c'est simplement un mauvais point de vue. Vos pensées à ce sujet m'intéressent.

M. Marcus Kolga: Je pense que la Russie a échoué à bien des égards au cours des 12 derniers mois.

Comme vous l'avez mentionné, elle n'est clairement pas la force que nous craignions qu'elle soit sur le plan militaire. En ce qui concerne la désinformation, ils ont certainement perdu le combat contre le président Zelenskyy et son gouvernement, qui ont fait un travail incroyable pour contrer un grand nombre de ces récits russes. Les opérations d'information et les cyberopérations russes ont également visé la cohésion de nos alliés et de nos alliances. Le fait que nous soyons plus alignés que jamais sur l'Ukraine, le fait que nous continuions de soutenir l'Ukraine... Nous leur envoyons des chars d'assaut. Nous allons, espérons-le, commencer à leur envoyer des F-18 à l'avenir. Je pense que tout cela démontre que, dans ces deux domaines, la Russie n'est pas l'adversaire que nous craignions qu'elle soit.

En ce qui concerne les cyberattaques, je pense que nous assistons à une accalmie de ces activités. La Russie a vraiment concentré ses efforts sur l'Ukraine en particulier. Je crains fort qu'une fois cette guerre terminée — et elle se terminera —, lorsque la Russie sera en mesure de se ressaisir dans le cyberespace et dans le secteur de l'information, mais surtout dans le cyberespace, et qu'elle pourra se concentrer sur nos alliés européens et sur nous, nous ne soyons toujours pas prêts à l'affronter. Je ne crois pas que nous puissions vraiment évaluer les cybercapacités de la Russie à l'heure actuelle, parce qu'elles ont changé et que leur point de mire s'est déplacé. Par conséquent, je pense que leurs cybercapacités restent à voir.

Comme je l'ai indiqué, lorsque cette guerre prendra fin, je pense que nous verrons Poutine déchaîner ces cyberguerriers contre nous. Espérons que nous serons prêts à ce moment-là.

● (1730)

M. Darren Fisher: Vous avez donné quelques exemples qui étaient probablement censés être un peu absurdes. Vous avez parlé d'envoyer des personnes vêtues de robes — je ne sais pas de quoi vous parliez — en Estonie et en Lettonie. Pouvez-vous nous citer quelques exemples?

Je me souviens qu'une fois, alors que je consultais Facebook, j'ai vu que quelqu'un avait publié sur ma page Facebook cet incroyable faux bulletin de nouvelles télévisées selon lequel les Américains venaient d'attaquer les Russes. Ce bulletin avait l'air tellement véridique.

Je me demande si vous pourriez nous donner quelques exemples de mesures qu'ils ont prises et qui auraient pu être dignes de la crainte que nous aurions pu leur permettre...

Le président: Veuillez répondre de manière très concise.

M. Marcus Kolga: Les deux exemples que je vous ai donnés ont eu une incidence considérable sur les russophones de Lettonie, ce qui est très préoccupant. En 2020, la campagne menée par le Ghostwriter du GRU, qui laissait entendre que les troupes canadiennes avaient attrapé la COVID-19 pendant qu'elles étaient au Canada et qu'elles infectaient maintenant les Lettons, a fait la une des journaux en Lettonie. C'était une pure invention, mais la nouvelle a été reprise.

Des histoires comme celle-là peuvent sembler mineures, insignifiantes et absurdes, mais elles ont une incidence.

Le président: Cela conclut la séance d'aujourd'hui.

Au nom du Comité, je tiens à remercier M. Kolga de son témoignage toujours perspicace. Nous vous sommes reconnaissants d'avoir participé à la réunion.