CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

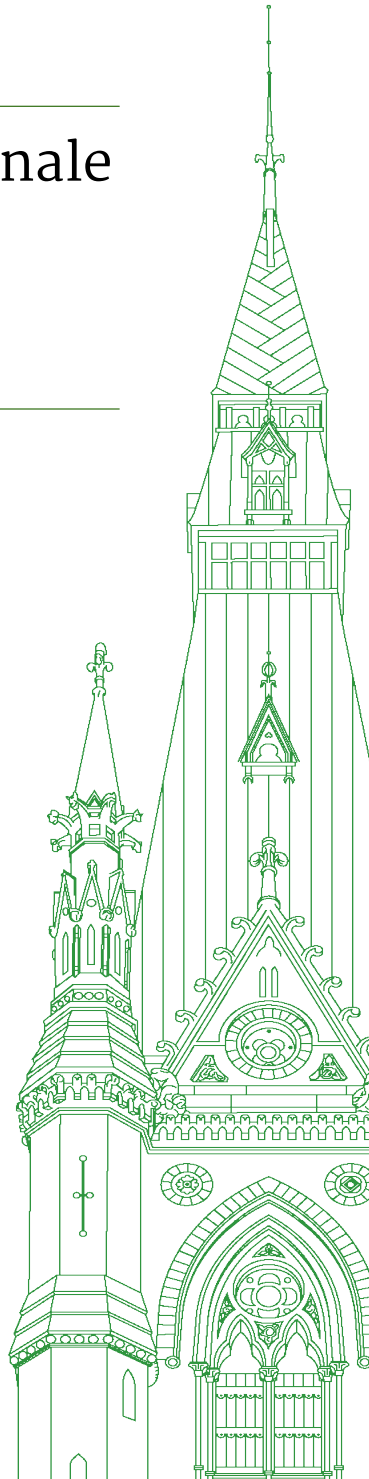
44e LÉGISLATURE, 1re SESSION

Comité permanent de la défense nationale

TÉMOIGNAGES

NUMÉRO 048

Le mardi 7 février 2023



Président : L'honorable John McKay

Comité permanent de la défense nationale

Le mardi 7 février 2023

● (1540)

[*Traduction*]

Le vice-président (M. James Bezan (Selkirk—Interlake—Eastman, PCC)): Je déclare la séance ouverte.

En cette 48e séance, nous recevons le Centre de sécurité des télécommunications, ou CST, pendant la première partie de notre étude sur la cybersécurité et la cyberguerre, conformément au paragraphe 108(2) du Règlement.

Nous ne disposerons pas d'une heure complète, puisque nous commençons avec 10 minutes de retard. Nous accorderons donc 55 minutes à la première partie de la séance et 55 minutes au prochain groupe de témoins.

Pendant la première heure, nous recevons Sami Khoury, dirigeant principal du Centre canadien pour la cybersécurité, et Alia Tayyeb, chef adjointe des renseignements électromagnétiques, du CST.

Je vous laisse la parole. Vous disposez de sept minutes pour faire vos allocutions d'ouverture.

M. Sami Khoury (dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): Je vous remercie, monsieur le président et distingués membres du Comité, de nous avoir invités à témoigner aujourd'hui.

Je m'appelle Sami Khoury. Mes pronoms sont « il » et « lui ». Je suis à la tête du Centre canadien pour la cybersécurité, connu sous le nom de centre de cybersécurité, du Centre de la sécurité des télécommunications.

Je suis accompagné aujourd'hui par ma collègue Alia Tayyeb, chef adjointe des renseignements électromagnétiques du CST.

[*Français*]

Je suis heureux de me présenter devant le Comité pour discuter de cybersécurité et de cyberopérations.

[*Traduction*]

Comme il s'agit de votre première séance réservée à cette étude, je voudrais commencer en vous disant ce qu'il en est actuellement des cybermenaces et ce que le CST fait pour protéger le Canada et les Canadiens. Je mettrai principalement l'accent sur le volet de notre mandat portant sur la cybersécurité, alors que ma collègue, Mme Tayyeb, traitera du renseignement étranger, du soutien que nous offrons à nos partenaires et de nos capacités actives et défensives dans le cadre de nos cyberopérations.

Maintenant plus que jamais, nous comprenons que la cybersécurité constitue les fondements de l'avenir au Canada, que cela concerne notre économie numérique, la sécurité de notre personne et de nos renseignements personnels, ou la prospérité et la capacité concurrentielle de notre pays. En octobre, le centre de cybersécurité a publié sa troisième évaluation des cybermenaces nationales, dans laquelle il fait état de la situation sur le plan de la cybermenace.

[*Français*]

Un des principaux points soulevés par l'évaluation des cybermenaces nationales est que la cybercriminalité demeure la plus grande activité de cybermenace visant la population canadienne et que les infrastructures essentielles sont la principale cible des cybercriminels et des auteurs de menace parrainés par des États.

[*Traduction*]

Les rançongiciels, notamment, ont été particulièrement préoccupants au cours des deux dernières années et demeurent une menace persistante pour les organisations canadiennes. Les cyberprogrammes parrainés par les États chinois, russe, iranien et nord-coréen continuent de représenter la plus grande cybermenace stratégique pour le Canada. Face à ces menaces, le CST, à titre d'autorité technique et opérationnelle du Canada en matière de cybersécurité, défend les réseaux du pays, alors que le centre de cybersécurité dirige la réaction du gouvernement aux cyberincidents. La cybersécurité ne représente toutefois pas une responsabilité et une préoccupation seulement pour le gouvernement fédéral, puisque les cybermenaces continuent de cibler et de toucher des citoyens et des organisations du Canada.

[*Français*]

Le Centre de la sécurité des télécommunications, ou CST, travaille avec des partenaires de l'industrie, dont des partenaires non gouvernementaux, pour échanger de l'information sur les menaces et les pratiques exemplaires en matière de cybersécurité. Le Centre canadien pour la cybersécurité, quant à lui, publie constamment des avis et conseils d'experts à l'intention des Canadiennes et des Canadiens.

[*Traduction*]

Dans l'avenir, pour continuer de nous adapter à l'évolution de la menace, renforcer les défenses et mieux protéger le Canada et les Canadiens, nous espérons que le projet de loi C-26, loi concernant la cybersécurité, continuera de progresser au Parlement. Cette mesure législative établirait un cadre de réglementation pour renforcer la cybersécurité dans les services et les systèmes essentiels à la sécurité nationale et publique, et conférerait au gouvernement un nouvel outil pour réagir aux cybermenaces émergentes.

Nous entendons également continuer de travailler afin de soutenir la sécurité publique dans le cadre du renouvellement de la Stratégie nationale de cybersécurité du Canada, laquelle établira la stratégie à long terme du Canada afin de protéger notre sécurité et notre économie nationales, de dissuader les acteurs présentant une cybermenace et de favoriser l'adoption de comportements fondés sur des normes dans le cyberespace.

[*Français*]

Pour le CST, le renouvellement de la Stratégie est l'occasion de faire le point et de poursuivre sur la lancée des réalisations du Centre canadien pour la cybersécurité des cinq dernières années. En effet, la création de ce Centre était l'une des principales initiatives de la Stratégie nationale de cybersécurité de 2018 de 2018.

[*Traduction*]

Enfin, alors que nous nous employons à renforcer nos relations avec l'industrie canadienne et d'autres ordres de gouvernement, nous misons également sur la collaboration avec nos partenaires étrangers dans le cadre du Groupe des cinq et d'autres organisations.

Je céderai maintenant la parole à ma collègue, Mme Tayyeb, qui traitera de son domaine de responsabilité.

Mme Alia Tayyeb (chef adjointe des renseignements électromagnétiques (SIGINT), Centre de la sécurité des télécommunications): Je vous remercie, monsieur Khoury.

Comme mon collègue l'a indiqué, je suis chef adjointe des renseignements électromagnétiques au CST et également responsable du volet relatif aux cyberopérations étrangères du mandat du CST. Mon pronom est « elle ».

Comme mon collègue l'a souligné, la gravité des cybercrimes et des cyberincidents qui ciblent les Canadiens et les infrastructures essentielles du pays connaissent une croissance exponentielle. Derrière les cybercriminels se cachent toutefois des États et des cyberacteurs parrainés par des États qui constituent une menace constante pour le Canada. Dans le cadre du mandat en matière de renseignement étranger du CST, nous continuons de fournir des renseignements sur les cybermenaces étrangères, notamment sur les activités et les intentions des États et des acteurs non étatiques. Les clients gouvernementaux, dont le centre de cybersécurité, utilisent ces renseignements pour défendre le Canada.

Comme la menace est en constante évolution, la Loi sur le Centre de la sécurité des télécommunications est entrée en vigueur en août 2019, permettant au CST d'élargir son arsenal afin de mener des opérations actives et défensives, réunies sous le nom de cyberopérations étrangères.

● (1545)

[*Français*]

Depuis qu'on lui a accordé ces nouveaux pouvoirs, le CST a tiré parti de ses capacités liées aux cyberopérations pour nuire aux efforts extrémistes basés à l'étranger visant à recruter des Canadiens, à mener des opérations en ligne et à diffuser du contenu violent et extrémiste.

[*Traduction*]

Nous avons également utilisé ces pouvoirs pour perturber les activités de cybercriminels planifiant des attaques au moyen de rançongiciels.

Admettant qu'il importe d'investir dans la cyberrésilience et de renforcer la capacité du Canada, le gouvernement a effectué, dans le cadre du budget de 2022, le premier investissement autonome du pays dans la capacité de cyberopérations, réservant au CST des sommes de 273,7 millions de dollars sur cinq ans et de 96,5 millions de dollars par année pour renforcer ses capacités de cyberopérations étrangères et mener un éventail de cyberopérations visant à lutter contre les cybercriminels et à protéger les infrastructures essentielles du Canada contre les cyberattaques.

[*Français*]

En vertu de son mandat d'assistance, le CST a aussi utilisé ses capacités pour appuyer la mission des Forces armées canadiennes.

Nos alliés, nos partenaires internationaux et nos adversaires investissent tous massivement dans ces capacités et développent leurs capacités de cyberopérations à grande échelle. Il va sans dire que le CST surveille attentivement le cyberespace et adapte régulièrement ses efforts pour protéger le Canada et défendre ses intérêts.

[*Traduction*]

À mesure que les cybermenaces continuent d'évoluer au Canada, le CST est déterminé à améliorer la cybersécurité et à renforcer la confiance des Canadiens à l'égard des systèmes dont ils dépendent au quotidien.

Sur ce, je vous remercie de nous avoir offert l'occasion de témoigner devant vous aujourd'hui. Je me ferai un plaisir de répondre à vos questions.

Le vice-président (M. James Bezan): Je vous remercie de vos allocutions d'ouverture.

Nous entamerons maintenant notre premier tour de questions, avec des interventions de six minutes.

Madame Gallant, vous avez la parole.

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

Je voudrais d'abord présenter un avis de motion. Je pense que la motion a été distribuée. Voici ce qu'elle indique:

> Que le Comité permanent de la défense nationale invite le ministre de la Défense nationale, l'honorable Anita Anand, et le commandant adjoint du NORAD, le lieutenant général Alain Pelletier, à donner une séance d'information d'au moins deux heures sur le navire étranger de la République populaire de Chine qui a récemment violé l'espace aérien canadien, et que cette séance d'information soit tenue en public dans les quatre prochains jours.

Le vice-président (M. James Bezan): D'accord. La motion est inscrite au programme.

Vous avez la parole. Il vous reste cinq minutes et demie.

Mme Cheryl Gallant: Monsieur le président, je demanderais au CST comment et quand il a été informé de la présence du ballon chinois dans notre espace aérien.

Mme Alia Tayyeb: Comme la ministre l'a indiqué pendant la fin de semaine, nous collaborons très étroitement avec nos alliés américains, particulièrement dans le cadre du NORAD, lequel surveille ce ballon en haute altitude et en suit les activités depuis la fin de semaine dernière, il me semble.

Je pense toutefois que les Forces armées canadiennes seraient mieux placées pour répondre à cette question en détail.

Mme Cheryl Gallant: Le CST sait-il si des incidents ou des incursions semblables se sont produits au cours des 10 dernières années?

Mme Alia Tayyeb: En ce qui concerne les ballons...?

Mme Cheryl Gallant: Oui.

Mme Alia Tayyeb: Je ne suis pas certaine de savoir comment répondre à cette question pour l'instant sans examiner les renseignements ou des détails opérationnels. Je vous renverrais donc à mes collègues des Forces armées canadiennes à ce sujet.

Je vous remercie.

Mme Cheryl Gallant: Le CST a-t-il joué un rôle dans la guerre électronique ou le blocage des dispositifs attachés au ballon espion?

Mme Alia Tayyeb: Ici encore, je m'excuse de ne pas pouvoir répondre à votre question. J'espère que vous comprenez que, sur le plan du renseignement et des opérations, je ne peux fournir de détails sur la question.

Je vous remercie.

Mme Cheryl Gallant: D'accord. Permettez-moi de revenir à la première question à laquelle vous avez répondu. Quand exactement le CST a-t-il appris que le ballon chinois se trouvait dans l'espace aérien du Canada?

Mme Alia Tayyeb: Je ne voudrais pas vous donner une réponse inexacte. Si vous le permettez, je pourrais vérifier ce qu'il en est exactement et vous répondre à une date ultérieure.

Mme Cheryl Gallant: Je ne veux pas savoir quand les forces armées... Ce que je veux savoir, c'est quand le CST a appris l'existence du ballon.

Mme Alia Tayyeb: D'après ce que je comprends, c'est quelque part au cours des derniers... c'est il y a deux fins de semaine. Je devrai vous trouver la date exacte, car je préférerais être précise et vous fournir ultérieurement une réponse plus détaillée.

● (1550)

Le vice-président (M. James Bezan): Si vous vouliez bien fournir une réponse par écrit, nous vous en saurions gré.

Je vous remercie.

Mme Alia Tayyeb: C'est ce que je ferai.

Mme Cheryl Gallant: Comment le CST a-t-il été informé de la présence de ce ballon? L'a-t-il découvert avec son propre équipement ou a-t-il été avisé par un autre organisme du gouvernement, la Défense nationale ou le NORAD?

Mme Alia Tayyeb: Ici encore, juste pour être absolument sûre et ne pas induire des membres du Comité en erreur, j'aimerais vous fournir cette réponse par écrit.

Mme Cheryl Gallant: D'accord.

Vu la nature inconnue des dispositifs que transporte le ballon chinois, existe-il, sur le plan de la cybersécurité ou de la cyberguerre, un risque supplémentaire dont le CST s'est ou ne s'est pas occupé?

Mme Alia Tayyeb: Je peux vous dire que nous collaborons très étroitement avec nos alliés américains, les Forces armées canadiennes et tous les autres organismes canadiens qui surveillent ce ballon. En partenariat avec des organismes, nous surveillons tous les risques qui pèsent sur les renseignements, les actifs ou les infrastructures du Canada.

Mme Cheryl Gallant: Vous n'avez pas précisé comment le CST a appris la présence du ballon, mais s'il l'a fait comme la plupart des Canadiens, c'est-à-dire aux nouvelles, comment proposeriez-vous de modifier les protocoles relatifs aux incursions dans l'espace aérien du Canada?

Mme Alia Tayyeb: Je vous remercie beaucoup de cette question, que je considère extrêmement importante.

Je ne pense pas être la mieux placée pour y répondre, considérant que les Forces armées canadiennes seraient mieux habilitées à répondre à des questions de cette nature.

Mme Cheryl Gallant: Le CST se préoccupe-t-il des partenariats de recherche entre les universités canadiennes et l'Université nationale de technologie de défense de la Chine, récemment dévoilés par le *Globe and Mail*?

Mme Alia Tayyeb: De fait, dans le cadre de notre mandat en matière de renseignement étranger, nous faisons rapport sur les activités de nos adversaires étrangers qui visent les Canadiens, y compris sur les approches faites à l'égard de notre travail de recherche, de notre propriété intellectuelle ou de nos investissements économiques. Nous surveillons donc certainement ces activités et les signalons à nos clients gouvernementaux.

Mme Cheryl Gallant: Comment avez-vous été informés de la panne générale du réseau de Rogers, survenue le 8 juillet?

Mme Alia Tayyeb: Je pense qu'il vaut mieux que je laisse à mon collègue, M. Khouri, répondre à cette question.

M. Sami Khoury: Je vous remercie de la question.

Nous avons surveillé la situation. Nous avons de bons partenariats avec toutes les entreprises de télécommunications, et peu après le début de la panne, nous étions en contact avec Rogers pour connaître la nature de l'incident.

Mme Cheryl Gallant: Avez-vous appelé l'entreprise pour vous informer ou est-ce elle qui a communiqué avec vous pour vous dire ce qui se passait?

M. Sami Khoury: Je l'ai appelée pour m'informer.

Mme Cheryl Gallant: D'accord.

Le vice-président (M. James Bezan): Madame Lambropoulos, vous avez la parole.

Mme Emmanuella Lambropoulos (Saint-Laurent, Lib.): Je vous remercie, monsieur le président.

Je remercie les témoins de comparaître aujourd'hui pour répondre à d'importantes questions.

Je crois comprendre que le CST travaille avec ses partenaires en Ukraine afin de déterminer s'il existe des cybermenaces, si la cybersécurité...

Le vice-président (M. James Bezan): Excusez-moi, mais nous ne recevons pas l'interprétation. J'ai arrêté le chronomètre.

[*Français*]

Mme Christine Normandin (Saint-Jean, BQ): Monsieur le président, pourriez-vous demander à la députée si elle a le bon casque d'écoute?

Nous venons de recevoir une directive de la Chambre des communes nous demandant de nous assurer d'utiliser le bon casque d'écoute pour protéger la santé des interprètes.

[*Traduction*]

Le vice-président (M. James Bezan): Madame Lambropoulos, est-ce le casque d'écoute fourni par la Chambre des communes? Oui.

Pouvez-vous le disposer naturellement devant votre visage? Essayez cette solution, je vous prie.

Mme Emmanuella Lambropoulos: Le son est-il mieux et plus clair?

Le vice-président (M. James Bezan): Non. Les interprètes me font signe que non.

Mme Emmanuella Lambropoulos: Pouvez-vous passer à un autre collègue? J'essaierai de trouver un endroit d'où il est un peu plus facile d'entendre.

Le vice-président (M. James Bezan): D'accord. Je vous remercie.

Madame O'Connell, vous avez la parole pour six minutes.

● (1555)

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

Je remercie les témoins de comparaître.

Je pense que le CST accomplit un travail extrêmement important et que la plupart des Canadiens n'ont même pas conscience de la qualité de nos services et de notre technologie. Je me réjouis d'avoir l'occasion d'en apprendre un peu plus et de permettre aux Canadiens d'en savoir un peu plus sur le travail que vous faites.

On entend beaucoup parler dans les médias des attaques par rançongiciel ciblant le secteur privé. Dans ma région, à l'extérieur du Grand Toronto, l'attaque menée contre l'hôpital pour enfants malades a certainement fait les manchettes, et l'affaire a fait l'objet de nombreux reportages. Pourriez-vous parler du processus ou du rôle que le CST peut jouer quand survient une attaque par rançongiciel contre le secteur privé et non gouvernemental, et nous expliquer comment vous tentez de travailler avec les clients? Qu'est-ce que vous pouvez faire et ne pas faire dans le cadre de votre mandat en cas d'attaques contre le secteur privé?

M. Sami Khoury: Je vous remercie de la question, à laquelle je répondrai avec plaisir.

En ce qui concerne les rançongiciels, quand nous avons publié notre troisième évaluation des cybermenaces nationales, nous avons continué de mettre l'accent sur la menace que ces logiciels représentent pour les Canadiens et les organisations canadiennes. Il s'agit d'une menace sérieuse, comme nous pouvons le constater dans le secteur des soins de santé, dans les infrastructures essentielles, dans les entreprises et ailleurs.

Nous travaillons de diverses manières avec le secteur privé pour atténuer ou contrer la menace des rançongiciels. Nous publions constamment des alertes et des bulletins cybernétiques pour attirer l'attention sur ce qui pourrait être de nouveaux vecteurs de rançongiciel ou de nouvelles techniques que les cybercriminels utilisent avec des rançongiciels.

Chaque fois que l'occasion se présente de parler à une communauté d'affaires, nous traitons de la menace des rançongiciels. Parfois, des partenaires nous alertent s'ils ont détecté des signes précurseurs de rançongiciels déployés au Canada. Nous aviserons alors l'organisation visée pour lui conseiller de faire attention, car des informations nous indiquent qu'elle pourrait être la cible d'un rançongiciel.

Malheureusement, nous apprenons parfois par les médias qu'une certaine organisation a été victime d'un rançongiciel...

Mme Jennifer O'Connell: Je suis désolée. Je ne veux pas vous interrompre, mais mon temps est limité.

Toujours sur le même sujet, le secteur est-il tenu d'aviser le gouvernement du Canada de quelque chose? Je peux voir que certaines entreprises ne veulent peut-être pas révéler qu'elles sont vulnérables. Existe-t-il des exigences à cet égard? Que fait-on en cas d'incident? Que recommanderiez-vous au Comité alors qu'il amorce son étude dans le domaine?

Je m'excuse encore de vous avoir interrompu. C'est juste que mon temps est limité.

M. Sami Khoury: Je vous remercie. Le secteur privé n'est pas tenu de signaler des incidents de rançongiciel, et bien des entreprises ne les signalent pas. En fait, en 2021, le centre de cybersécurité n'a été informé que de 300 incidents de rançongiciel environ. Des incidents ne sont probablement pas signalés pour un certain nombre de raisons.

Dès que nous sommes informés d'un incident, nous proposons notre aide. Parfois, elle est acceptée, mais elle est plus souvent rejetée.

Mme Jennifer O'Connell: Je vous remercie.

Poursuivons sur le même sujet. Les infrastructures essentielles sont particulièrement importantes. Mes collègues savent que j'ai déjà travaillé dans le secteur municipal, et d'après ce que je me souviens de mon rôle d'alors, nous n'étions vraiment pas informés. Les municipalités ou les municipalités régionales assument souvent de nombreuses responsabilités concernant les réseaux de distribution d'eau et les infrastructures essentielles, comme les ponts, selon la région.

Que faites-vous pour veiller à ce que tous les ordres de gouvernement aient une formation adéquate ou les outils nécessaires pour connaître les menaces, puisqu'ils sont souvent responsables des infrastructures essentielles?

M. Sami Khoury: Je vous remercie de la question.

Nous communiquons régulièrement avec les divers secteurs responsables d'infrastructures essentielles, y compris les municipalités, et nous leur proposons un certain nombre de programmes. Nous les appelons régulièrement. J'ai personnellement été invité à prendre la parole lors d'activités annuelles ou de conférences afin de parler des dernières menaces que nous connaissons, que nous observons ou qui les touchent.

Notre équipe de partenariat met en œuvre un programme de sensibilisation, s'adressant continuellement aux municipalités, aux exploitants d'infrastructures essentielles, aux secteurs des soins de santé et à d'autres intervenants pour tenter de les informer le plus possible au sujet des services que propose le centre de cybersécurité.

● (1600)

Mme Jennifer O'Connell: Je vous remercie.

Dites-nous brièvement si le CST fait concurrence aux experts de la cybersécurité et de la technologie sur le plan de la rétention du talent...

Le vice-président (M. James Bezan): Je ferai une brève pause pendant une minute, car nous recevons l'interprétation française sur le canal anglais.

Bien. Essayez de nouveau, s'il vous plaît.

Mme Jennifer O'Connell: Je vous remercie.

Au chapitre de la rétention ou du recrutement, je présume que nous faisons concurrence à Silicon Valley et à d'autres concurrents. Quelle stratégie avez-vous pour vous assurer que nous continuons de former et de recruter la crème du talent dans le domaine?

M. Sami Khoury: Je vous remercie encore de poser cette question importante.

Le recrutement n'est pas chose facile, d'autant plus qu'il s'agit d'un domaine où la concurrence est féroce. Nous essayons d'embaucher des employés en vue de pourvoir un certain nombre de postes, dans une gamme de secteurs d'activité, et nous nous assurons d'embaucher des Canadiens qui représentent la richesse et la diversité de la société dans laquelle nous vivons.

À l'heure actuelle, nous modernisons notre effort de recrutement multidisciplinaire pour attirer les meilleurs talents. À cet égard, nous investissons dans un programme d'emplois pour étudiants et un programme d'alternance travail-études afin d'assurer la richesse de notre bassin de talents. Nous collaborons de près avec des collectivités pour sensibiliser les étudiants à la cybersécurité en leur faisant des exposés afin de les intéresser aux domaines des sciences, de la technologie, de l'ingénierie et des mathématiques. Nous investissons également dans le maintien en poste de notre personnel actuel. D'ailleurs, nous avons été désignés comme l'un des meilleurs employeurs pendant trois années consécutives.

Le vice-président (M. James Bezan): Votre temps est écoulé.

[*Français*]

Madame Normandin, vous avez la parole pour six minutes.

Mme Christine Normandin: Merci beaucoup, monsieur le président.

Madame Tayyeb et monsieur Khoury, je vous remercie de votre présence.

Mes questions vont dans le même sens que celles de ma collègue Mme O'Connell.

J'aimerais que vous nous parliez des similarités entre ce que vous faites et ce qui se passe dans les Forces armées canadiennes. Des témoins nous ont déjà parlé de certains problèmes.

Ma question porte sur la main-d'œuvre.

La difficulté de recruter de la main d'œuvre et le fait que le secteur privé soit très compétitif posent-ils des risques en lien avec la sécurité?

M. Sami Khoury: Nous sommes très conscients des défis actuels que crée la situation de l'emploi. Nous essayons d'attirer les talents de diverses parties du Canada. Nous ne concentrons pas seulement sur ceux de la région de la capitale nationale. Nous essayons d'engager des gens de partout au Canada, qui ont différentes expertises. Nous essayons aussi d'engager des étudiants et des stagiaires de programmes coop. Ce ne sont pas seulement des professionnels qui se joignent à nous. Il y a donc des employés qui apportent beaucoup de talent à l'organisation. C'est ce sur quoi nous concentrons nos efforts.

Nous sommes aussi en train d'explorer la possibilité d'embaucher des gens qui sont prêts à demeurer en région pour fournir du soutien en matière de cybersécurité. Il ne s'agit donc pas seulement d'embaucher des gens qui sont prêts à déménager à Ottawa. Il faut offrir du soutien à l'échelle locale.

Mme Christine Normandin: Je vous remercie.

Je ne peux pas passer sous silence la question du jour, à savoir McKinsey & Company, dont nous avons beaucoup parlé au cours des dernières semaines. Nous avons aussi beaucoup parlé du recours à différentes firmes privées pour de la sous-traitance, notamment pour des services informatiques.

Est-ce le type de sous-traitance auquel le Centre de la sécurité des télécommunications a recours?

Le cas échéant, de quelle façon peut-on s'assurer de la sécurité, sachant que ces firmes ont plusieurs clients?

M. Sami Khoury: Je vous remercie de votre question.

À ce que je sache, nous n'avons pas de contrat avec ladite firme. Si vous le voulez, je peux vous envoyer une réponse écrite après la réunion.

Pour ce qui est de la sécurité des contrats, chaque ministère a la responsabilité de sauvegarder son information. Notre travail, c'est d'établir les normes de sécurité pour différents contrats, pas de façon individuelle. C'est aux ministères de respecter ces normes.

J'espère que j'ai bien répondu à votre question.

Mme Christine Normandin: Si j'ai bien compris, votre organisation n'a pas de contrat avec la firme McKinsey & Company spécifiquement.

Cela dit, en a-t-elle avec d'autres firmes?

M. Sami Khoury: À ma connaissance, nous n'avons pas de contrat avec d'autres firmes. Encore une fois, je peux vous fournir une réponse à cet égard ultérieurement.

● (1605)

Mme Christine Normandin: Je vous en serais reconnaissante. Je vous remercie.

Vous dirigez, à l'occasion, des cyberopérations défensives, lesquelles requièrent une autorisation ministérielle. J'aimerais que vous nous parliez de la rapidité à laquelle vous obtenez ces autorisations.

Y a-t-il des éléments qui vous permettraient d'être un peu plus efficaces et de réagir plus rapidement, par exemple quand vous vous penchez sur des dossiers en lien avec une situation donnée?

Mme Alia Tayyeb: Je vous remercie beaucoup de votre question.

Nous sommes toujours à la recherche de méthodes pour améliorer nos processus. Nous avons récemment investi dans notre programme, ce qui nous a surtout permis d'améliorer notre capacité à travailler avec nos collègues du ministère des Affaires étrangères, qui jouent un rôle très important dans notre processus d'approbation.

[*Traduction*]

Je crois que l'important, c'est que nous travaillons très étroitement avec nos collègues, tant au centre de cybersécurité qu'à Affaires mondiales Canada. Ils sont chargés, avec nous, de fournir de l'aide et des conseils en ce qui concerne notre planification opérationnelle. Nous avons toutefois été en mesure de réagir très rapidement aux menaces à mesure qu'elles sont apparues.

[*Français*]

Mme Christine Normandin: Merci beaucoup.

Un autre défi auquel les Forces armées canadiennes sont confrontées concerne les difficultés d'approvisionnement et l'obtention d'autorisations de sécurité. Cela prend trop de temps pour obtenir du matériel de pointe pour un projet quelconque ou des autorisations de sécurité pour des employés potentiels, par exemple. J'aimerais vous entendre sur ces deux aspects.

M. Sami Khoury: Je peux répondre à cette question. Merci.

La chaîne d'approvisionnement a certainement été touchée par la pandémie, et nous avons autant de difficulté que les autres ministères à acquérir de l'équipement électronique ou de l'équipement de réseautage pour augmenter nos capacités. Nous sommes conscients de cela. Nous essayons de travailler avec les entreprises pour accélérer la livraison de certains de ces produits, mais nous sommes tout aussi touchés que tous leurs autres clients, effectivement.

[*Traduction*]

Le vice-président (M. James Bezan): Madame Mathyssen, vous avez droit aux six dernières minutes de ce premier tour.

Mme Lindsay Mathyssen (London—Fanshawe, NPD): Merci, monsieur le président.

Je remercie les témoins d'être des nôtres aujourd'hui.

Je voulais revenir sur ce que disait Mme Normandin au sujet de ces contrats. C'est certainement un thème qui occupe l'esprit de bon nombre d'entre nous ces derniers temps.

Monsieur Khoury, au regard des recommandations que vous faites à un grand nombre de ministères, en ce qui concerne ces renseignements, ces infrastructures essentielles et ces entrepreneurs qui traitent des renseignements précis, des renseignements de nature délicate, des renseignements personnels et des données sensibles au nom du gouvernement, comment leur communiquez-vous ces pratiques exemplaires? Comment vous y prenez-vous pour surveiller la conformité au sein de chaque ministère?

Vous avez dit que les ministères doivent le faire eux-mêmes, mais jouez-vous un rôle dans ces activités de communication et de surveillance?

M. Sami Khoury: Je vous remercie de la question.

Nous déterminons les différentes normes de sécurité de l'information qui sont en vigueur: protégé A, protégé B, protégé C. Nous communiquons ces normes. Elles sont en quelque sorte instaurées par l'entremise du Conseil du Trésor. Grâce à chacun de ces niveaux de classification, les ministères savent quels renseignements sont classés dans la catégorie « protégé B » ou « protégé C », ou ce qui est secret et ce qui est très secret. Les ministères eux-mêmes doivent respecter ces normes. Nous n'en faisons pas une vérification proprement dite.

Parfois, nous sommes amenés à participer à des projets précis. En pareil cas, nous fournissons des conseils en matière de sécurité dans le cadre du projet et nous nous assurons que la sécurité des renseignements liés au projet est proportionnelle à leur classification. Nous n'examinons pas, contrat par contrat, quels renseignements sont fournis à l'entrepreneur. J'en parle du point de vue informatique, car ma principale préoccupation est la cybersécurité et la sécurité informatique.

Mme Lindsay Mathyssen: En ce qui a trait à ces contrats privés, les entrepreneurs auraient accès à des renseignements de nature délicate. Mis à part le fait que chaque ministère assure sa propre surveillance, n'envisagez-vous pas — vous ou le CST — des problèmes potentiels à cet égard au sein des ministères? N'ont-ils pas l'obligation ou la responsabilité de vous faire rapport?

● (1610)

M. Sami Khoury: Chaque ministère est doté d'un agent de sécurité organisationnel. Nous avons un groupe d'agents qui se rencontrent régulièrement. Le Conseil du Trésor en est la branche stratégique. Nous travaillons avec lui pour nous assurer que l'information est diffusée autant que possible, mais nous ne menons pas de vérification auprès des ministères pour comprendre comment ils traitent les renseignements selon le niveau de classification.

Mme Lindsay Mathyssen: Oui, mais n'estimez-vous pas que cela pourrait créer des problèmes? C'est peut-être une recommandation que nous pourrions faire à l'avenir pour qu'il y ait davantage de communication entre ces ministères et le CST ou votre centre en particulier, afin de mieux nous renseigner sur les problèmes qui pourraient survenir au sein des ministères en ce qui a trait aux renseignements de nature délicate.

M. Sami Khoury: Je vous remercie à nouveau de votre question.

Je pense que les ministères savent comment demander de l'aide, que ce soit au Conseil du Trésor ou à notre centre, s'ils cherchent à obtenir des précisions sur la bonne classification des renseignements. J'ai personnellement participé à un certain nombre de discussions sur le niveau de classification des renseignements en question et le profil de sécurité qui correspond au système informatique afin de protéger ces renseignements. Ce genre de tribunes et de voies de communication existent déjà.

Mme Lindsay Mathyssen: C'est littéralement indiqué dans le nom de votre organisme. Vous êtes le centre. Vous êtes censés rassembler bon nombre de ces renseignements. Voici ce qui me préoccupe: dans le cas de certains de ces entrepreneurs, si vous deviez constater des tendances, ce serait plus utile, je suppose, mais lorsqu'il s'agit de contrevenants récidivistes, c'est-à-dire des entreprises qui pourraient avoir l'habitude de ne pas suivre les pratiques exemplaires en matière de cybersécurité au sein des ministères, seriez-vous en mesure de déceler ces comportements?

En outre, nous avons vu qu'aux États-Unis, par exemple, une entreprise comme Deloitte a effectivement divulgué des renseignements de nature très délicate. Cette fuite massive de données, qui a eu lieu en 2017, a touché le département de la Défense, le département de la Sécurité intérieure, le département d'État et les instituts nationaux de la santé des États-Unis, mettant en cause des mots de passe, des adresses IP et des renseignements de nature délicate.

Lorsque vous constatez qu'un tel incident se produit à l'échelle internationale et que les services de ces mêmes entreprises sont retenus ici, au Canada, au sein de notre propre gouvernement, offrez-vous des commentaires ou des avertissements? Recommandez-vous au gouvernement de ne pas recourir aux entreprises qui ont eu ces problèmes? Surveillez-vous la situation? En faites-vous un suivi? Formulez-vous de telles recommandations?

M. Sami Khoury: Je vous remercie encore une fois de la question.

Je m'en remettrais à Services publics et Approvisionnement Canada pour tout ce qui a trait aux contrats. Notre rôle consiste surtout à examiner parfois l'architecture de sécurité, auquel cas nous collaborerions avec nos collègues.

Les ministères ont la responsabilité d'évaluer et d'autoriser la sécurité de leurs systèmes. Ils examinent l'accréditation de sécurité de leurs systèmes, et nous intervenons dans ce processus. Avant l'étape de la mise en service, si le système contient des renseignements de nature délicate, le ministère doit s'assurer qu'il respecte les normes de sécurité établies par le centre de cybersécurité. Parfois, nous participons directement au projet et nous intervenons donc là-dedans.

Pour ce qui est des contrevenants récidivistes et des questions de contrats, je vous invite respectueusement à vous en enquérir auprès de Services publics et Approvisionnement Canada.

Le vice-président (M. James Bezan): Nous allons devoir nous arrêter là. Nous avons légèrement dépassé le temps alloué.

Madame Kramp-Neuman, vous avez la parole pour cinq minutes.

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

Je remercie les témoins de leur présence.

Voici ma première question. En raison de la nature concurrentielle des possibilités d'emploi dans le domaine de la cybersécurité, peut-on supposer sans risque de se tromper que le centre de la sécurité du Canada a du mal à recruter des employés possédant les compétences requises pour la cybersécurité et la lutte contre la cyberguerre?

Mme Alia Tayyeb: Je pourrais peut-être commencer par le début. C'est une excellente question. Nous en parlons beaucoup au CST et au centre de cybersécurité.

Nous avons de la chance, d'une certaine manière. À en juger par les statistiques, notre organisation suscite beaucoup d'intérêt. Nous avons une mission intéressante. C'est un sujet qui intéresse bien des gens. Depuis que la visibilité de notre centre de cybersécurité a augmenté, nous avons certainement fait d'importants progrès en matière de sensibilisation du public, d'où le grand nombre de personnes qui souhaitent travailler ici.

Nous embauchons une variété de personnes issues de différents domaines techniques; il ne s'agit pas d'un seul type de profession. Nous avons des ingénieurs, des mathématiciens, des experts en cybersécurité, et j'en passe. Nous offrons également une gamme d'emplois.

Cela dit, comme M. Khoury l'a dit tout à l'heure, il s'agit d'un domaine où la concurrence est féroce. Nous devons donc innover et nous assurer de rester à la hauteur de nos concurrents. C'est pourquoi certaines de nos initiatives visent à faire du CST un excellent lieu de travail, et nous prenons toutes les mesures qui s'imposent pour devenir un employeur de premier plan au Canada. Il s'agit notamment d'offrir un environnement propice à l'innovation et de favoriser un milieu inclusif afin de pouvoir attirer continuellement, dans le secteur, de nouvelles personnes qui n'y auraient peut-être pas songé auparavant, en particulier des femmes ou des gens de différentes origines ethniques...

● (1615)

Mme Shelby Kramp-Neuman: Je vous remercie. Comme je n'ai pas beaucoup de temps, je vais devoir passer à une autre question.

Mme Alia Tayyeb: Très bien.

Mme Shelby Kramp-Neuman: Nous savons qu'il reste beaucoup de défis à relever sur le plan de la compensation financière, entre autres, mais je vais passer à autre chose.

À mesure que les organismes continuent de modifier leurs mandats, comment entrevoyez-vous l'évolution de la relation entre le commandement de cyberdéfense et les Forces armées canadiennes? Comment pouvons-nous faire en sorte d'optimiser leurs domaines d'expertise et leurs ressources?

Mme Alia Tayyeb: Merci beaucoup. C'est une question fantastique.

Les Forces armées canadiennes se sont avérées un excellent partenaire pour ce que nous appelons la « mise sur pied d'une force », c'est-à-dire la constitution d'une nouvelle main-d'œuvre qui s'intéresse au domaine cybernétique.

À cet égard, le CST travaille également en étroite collaboration avec le commandement de cyberdéfense des États-Unis. Nous discutons de stratégies relatives à l'effectif pour acquérir l'expertise dont nous avons besoin afin de mettre au point des outils efficaces qui nous permettront de relever les défis de demain.

Mme Shelby Kramp-Neuman: Je vous remercie.

Nous reconnaissons que l'un des principaux objectifs du CST est de mener des cyberopérations actives. Compte tenu de l'intervention de différentes entités, comme les ministères des Affaires étrangères et de la Défense nationale, le CST agirait-il de façon indépendante ou en collaboration avec ces différents intervenants?

Mme Alia Tayyeb: Je vous remercie de la question.

En effet, nous ne travaillons certainement pas de façon indépendante. Nous collaborons très étroitement avec les Forces armées canadiennes et le ministère des Affaires étrangères.

D'ailleurs, la participation du ministère des Affaires étrangères est requise pour les cyberopérations actives. La ministre des Affaires étrangères est tenue de donner son consentement pour ces opérations. Nous travaillons en très étroite collaboration à la planification et à la conception de ces opérations, ainsi qu'à l'évaluation des risques.

En ce qui concerne les Forces armées canadiennes, nous avons essentiellement un effectif combiné. Autrement dit, nous avons rassemblé les agents des deux secteurs afin de continuer à travailler efficacement sur ce volet de notre mandat.

Mme Shelby Kramp-Neuman: Je vous remercie.

On a dit tout à l'heure que le recrutement est très difficile, de même que le maintien en poste du personnel actuel. Je vais peut-être vous laisser le soin d'ajouter d'autres observations à ce sujet.

C'est peut-être votre collègue qui a parlé des difficultés liées au maintien en poste.

M. Sami Khoury: Je vous remercie.

Non, en fait, je voulais dire que nous investissons dans le maintien en poste du personnel et nous nous assurons de demeurer un employeur de choix: nous offrons à nos employés un endroit où ils peuvent s'épanouir, en ayant accès aux possibilités de formation dont ils ont besoin. En ce qui concerne le maintien en poste, nous sommes également...

Mme Shelby Kramp-Neuman: Je suis désolée de vous interrompre. J'ai une dernière question à poser.

Je ne veux pas que vous vous répétiez, mais avons-nous actuellement assez de personnel pour répondre pleinement aux exigences opérationnelles?

M. Sami Khoury: Je vous remercie encore une fois.

Nous embauchons constamment. La demande pour nos services ne cesse de croître. Nous sommes occupés à embaucher autant que nous le pouvons.

Mme Shelby Kramp-Neuman: Je vous remercie.

Le vice-président (M. James Bezan): Très bien.

Madame Lambropoulos, essayons à nouveau. Vous avez cinq minutes.

Mme Emmanuella Lambropoulos: Je remercie les témoins d'être des nôtres aujourd'hui pour répondre à certaines de nos questions.

Comme je m'apprêtais à le dire tout à l'heure, le CST travaille avec des partenaires en Ukraine pour surveiller et détecter toute cybermenace potentielle et, le cas échéant, mener des enquêtes. Il aide également ses partenaires à prendre les mesures qui s'imposent pour contrer ces menaces.

D'après ce que vous avez observé, la Russie a-t-elle mené des cyberopérations pour nuire à l'Ukraine pendant cette guerre? Pouvez-vous nous dire si cela a eu une incidence sur la capacité de l'Ukraine à se défendre? Par ailleurs, en tant que Canadiens, pouvons-nous tirer des leçons?

M. Sami Khoury: Je vous remercie de la question. Je vais y répondre en premier, et je demanderai peut-être à ma collègue, Mme Tayyeb, de compléter ma réponse.

Avant le début de l'invasion de l'Ukraine, nous avions signalé à nos partenaires la menace des cyberactivités russes. La Russie est un cyberacteur redoutable, et nous avons communiqué des renseignements autant que possible afin que les gens prennent cette menace au sérieux.

Du point de vue des Ukrainiens, ils sont victimes de la cyberagression russe depuis 2015 et 2016, lorsque leur réseau électrique a fait l'objet d'une attaque. Au fil des ans, l'Ukraine a renforcé sa résilience. Grâce aux renseignements fournis par l'Occident, les Ukrainiens ont repoussé un certain nombre de cyberattaques que la Russie a déclenchées sur leur pays au début de la guerre.

Nous avons beaucoup appris des cyberattaques que la Russie a lancées contre l'Ukraine. Nous avons réagi sans tarder et publié ou émis des bulletins cybernétiques. Ainsi, au cas où il y aurait des répercussions en Amérique du Nord ou, du moins, au Canada, nous serions prêts à communiquer le plus d'information possible aux infrastructures essentielles et aux entreprises au sujet de certains de ces indicateurs.

● (1620)

Mme Emmanuella Lambropoulos: Voulez-vous ajouter quelque chose, madame Tayyeb?

Mme Alia Tayyeb: Oui, en effet. Je voudrais peut-être faire quelques observations supplémentaires en réponse à votre question sur ce que nous avons observé concernant les tactiques utilisées par la Russie en Ukraine. Selon moi, il y a une quantité considérable de renseignements — y compris dans des sources ouvertes — qui mettent en évidence l'utilisation de cyberoutils par la Russie dans son dernier conflit avec l'Ukraine et le recours à des cyberattaques et à des cybermenaces contre l'Ukraine, parallèlement aux attaques cinétiques russes. L'exemple le plus frappant est la désactivation des communications satellitaires en Ukraine dans la période précédant la guerre.

De notre point de vue, la « guerre hybride », comme nous l'appelons — c'est-à-dire l'utilisation d'outils tant cinétiques que cybernétiques — a été bien documentée dans ce conflit, à la fois par le centre de cybersécurité et, en fait, par Microsoft, qui a fait une excellente étude sur la cartographie de ces deux capacités et la façon dont elles ont été utilisées en parallèle dans ce conflit.

Mme Emmanuella Lambropoulos: Je vous remercie.

D'après ce que vous me dites, la Russie est bien sûr un acteur redoutable à cet égard. Vous avez dit, dans votre déclaration liminaire, que la cybercriminalité est la menace la plus susceptible de toucher les Canadiens et qu'il y a beaucoup d'acteurs qui présentent une menace, notamment la Chine, la Russie, la Corée du Nord et l'Iran. Voilà les pays qui constituent les plus grandes menaces. En quoi ces acteurs diffèrent-ils sur le plan de leurs objectifs et de leurs capacités?

M. Sami Khoury: Je vous remercie de votre question.

Nous avons désigné ces quatre États-nations dans notre troisième évaluation des cybermenaces nationales. Ils ont diverses raisons de s'en prendre au Canada, que ce soit pour cibler des Canadiens, compromettre certaines technologies dans le cadre de campagnes mondiales, s'attaquer à la valeur économique du Canada ou rechercher des gains financiers.

Par exemple, nous savons que l'Iran utilise des outils cybercriminels pour éviter toute attribution. C'est l'une de ses techniques. La Chine, pour sa part, s'attaque à la recherche, aux données techniques, à la propriété intellectuelle des entreprises et aux capacités militaires. La Corée du Nord cherche à accroître sa valeur économique en volant des données d'authentification, ainsi que des fonds.

Chacun d'eux est animé d'une motivation: mener ce genre d'activités ou, du moins, s'attaquer à un certain aspect de la société canadienne pour faire avancer ses propres intérêts.

Mme Emmanuella Lambropoulos: Madame Tayyeb, voulez-vous ajouter quelque chose? Vous avez 30 secondes.

Mme Alia Tayyeb: Je crois que M. Khoury a bien décrit la situation.

Nous surveillons constamment le cyberespace, à la recherche de nouvelles tactiques et techniques utilisées par les auteurs de rançongiciels qui ciblent les Canadiens. Il s'agit d'un domaine en constante évolution, et il faut déployer des efforts soutenus en matière de suivi pour nous assurer de protéger en permanence les infrastructures canadiennes.

Mme Emmanuella Lambropoulos: Merci à vous deux.

Le vice-président (M. James Bezan): Je vous remercie.

Nous passons maintenant aux interventions de deux minutes et demie.

Allez-y, madame Normandin.

[*Français*]

Mme Christine Normandin: Merci, monsieur le président.

J'aimerais que vous nous parliez de la collaboration entre les États et le partage de l'information. On sait que le Canada fait partie du Groupe des cinq. Il y a une politique internationale en matière de cyberespace où le Canada demande aux États de rendre des comptes sur les activités malveillantes.

Cela se passe-t-il relativement bien avec les autres États ou y a-t-il plutôt une dynamique donnant-donnant qui s'installe? Par exemple, si le Canada donne de l'information, il en reçoit. À défaut d'en recevoir, on est un peu frileux à échanger de l'information.

À quoi ressemble la collaboration entre les autres pays?

● (1625)

Mme Alia Tayyeb: Il y a un système de partage de l'information très efficace et très ouvert, surtout entre les pays du Groupe des cinq. Nous sommes partenaires pour combattre toutes les menaces dont nous avons parlé aujourd'hui.

Nous avons des relations très étroites avec nos partenaires de ces organisations. En plus, nous avons d'autres alliés partout au monde avec qui nous partageons de l'information. Ce sont des menaces qui nous affectent tous. Je dirais que nous avons de très bonnes relations dans ce domaine.

Je vais laisser M. Khoury continuer.

M. Sami Khoury: J'aimerais ajouter quelques mots.

Dans le domaine de la cybersécurité, nous faisons partie de plusieurs communautés d'échange d'information. Dans le Groupe des cinq, nous échangeons beaucoup d'information.

Plus globalement, nous échangeons de l'information avec les équipes d'intervention en cas d'urgence informatique partout au monde. Lorsque nous sommes informés d'activités malveillantes, nous leur envoyons une note afin qu'elles prennent des mesures localement pour neutraliser la menace.

Mme Christine Normandin: Lorsqu'il y a un échange d'information, celle-ci est-elle transmise à l'ensemble des pays membres du Groupe des cinq ou y a-t-il à l'intérieur de ce groupe des échanges plus bipartites?

Mme Alia Tayyeb: Je dirais, dans les grandes lignes, que les deux scénarios sont possibles et que cela dépend du type de menace qui touche les partenaires. Cela dit, M. Khoury a peut-être quelque chose de différent à dire à ce sujet.

[*Traduction*]

Le vice-président (M. James Bezan): Le temps est écoulé. Il faut passer à la prochaine intervention de deux minutes et demie. J'en suis désolé.

La parole est à vous, madame Mathyssen.

Mme Lindsay Mathyssen: Je vous remercie.

Madame Tayyeb, vous avez évoqué, dans votre déclaration liminaire, les pouvoirs accrus qui vous ont été conférés. Cet élargissement des pouvoirs a, bien sûr, inquiété beaucoup de gens. En effet, votre ministère peut recueillir des renseignements sur des Canadiens à des fins de recherche, sans qu'il soit tenu de les divulguer. C'est là pour toujours.

Bien entendu, beaucoup d'organisations de défense des droits de la personne et des droits civils étaient préoccupées par l'utilisation de ces données et le risque qu'elles soient utilisées contre des personnes qui exercent leurs droits. D'autres inquiétudes ont également été exprimées en ce qui concerne la surveillance et la reddition de comptes, ainsi que la façon dont les gens se font surveiller en permanence, maintenant que ces lois sont en vigueur depuis plusieurs années.

Qu'en pensez-vous?

Mme Alia Tayyeb: Merci beaucoup.

Permettez-moi de clarifier un point, si je me suis mal exprimée tout à l'heure. Soyons clairs: le CST n'a pas le droit, de quelque façon que ce soit, de cibler des Canadiens ou toute personne au Canada. C'est une interdiction fondamentale. Cela s'applique à notre mandat de renseignement étranger et à notre mandat de cyberopération.

Ce à quoi je faisais sans doute allusion, c'est que, dans ce domaine, l'intérêt serait porté sur l'acteur étranger. Si un acteur étranger devait cibler des Canadiens, nous nous intéresserions à ses agissements qui pourraient nuire au Canada. C'est une interdiction très précise.

Pour ce qui est de la surveillance, nos activités font absolument l'objet d'examens. Nous avons deux organismes de surveillance: l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, ou OSSNR, et le Comité des parlementaires sur la sécurité nationale et le renseignement, ou CPSNR. Nous avons également un commissaire au renseignement qui approuve les autorisations ministérielles liées au renseignement étranger pour s'assurer qu'elles sont conformes à nos obligations en vertu de la Charte, et pour maintenir et assurer la protection de la vie privée des Canadiens si jamais des renseignements sur des Canadiens sont recueillis par inadvertance.

Tous les volets de notre mandat font l'objet d'une surveillance et d'un examen constants.

Mme Lindsay Mathyssen: Aux termes de la Loi sur le Centre de la sécurité des télécommunications, vous êtes autorisés à effectuer des recherches sur les activités des Canadiens à l'échelle nationale, n'est-ce pas?

Mme Alia Tayyeb: Non, nous n'avons pas cette capacité.

Le vice-président (M. James Bezan): Je vous remercie beaucoup.

Monsieur Kelly, vous avez la parole pour cinq minutes.

M. Pat Kelly (Calgary Rocky Ridge, PCC): Je vous remercie.

Monsieur Khoury, vous avez dit au Comité il y a moins d'un an que « les cyberprogrammes parrainés par la Chine, la Russie, la Corée du Nord et l'Iran constituent la plus grande menace stratégique pour le Canada ».

Tout d'abord, est-ce toujours le cas? Pouvez-vous nous parler des acteurs non étatiques?

M. Sami Khoury: Je vous remercie de la question.

Selon notre plus récente évaluation de la cybermenace, ces quatre pays — la Russie, la Chine, la Corée du Nord et l'Iran — demeurent la principale menace stratégique à laquelle fait face le Canada.

Pour ce qui est des acteurs non étatiques, les cybercriminels sont bien sûr une menace qu'il nous faut neutraliser. Dans le cadre du conflit entre la Russie et l'Ukraine, différents groupes de cybermilitants cherchant à appuyer les acteurs étatiques ont aussi vu le jour. Ces cybercriminels ont choisi leur camp, en quelque sorte. Certains groupes se servent de logiciels de rançon pour favoriser la Russie et constituent une préoccupation constante.

● (1630)

M. Pat Kelly: Dites-vous que des acteurs étatiques recourent aux services de ces mercenaires, issus d'organisations criminelles internationales?

M. Sami Khoury: Dans certains cas, il existe une relation étroite entre l'appareil étatique et certaines organisations criminelles de pirates informatiques.

M. Pat Kelly: D'accord.

Dans le rapport que nous avons produit à la suite de votre dernière comparution, la recommandation 10 se lit comme suit:

> Que le gouvernement du Canada investisse dans des capacités défensives et actives de cyberopérations. De plus, il devrait accélérer le recrutement et l'instruction de cyberspécialistes des Forces armées canadiennes et du Centre de la sécurité des télécommunications, et veiller à la protection adéquate de tous les systèmes fédéraux contre les cybermenaces.

Quelles mesures votre centre a-t-il prises relativement à la recommandation 10?

M. Sami Khoury: Mme Tayyeb pourrait répondre à la première partie de la question.

Mme Alia Tayyeb: Je n'ai pas le rapport sous les yeux, mais je répète, à propos de la première recommandation sur l'investissement dans les capacités défensives et actives de cyberopérations, que le budget annoncé en 2022 prévoit [*difficultés techniques*].

Le vice-président (M. James Bezan): Nous sommes victimes d'une cyberattaque.

Des voix: Ah, ah!

M. Sami Khoury: Entretemps, je peux répondre à la deuxième partie de la question sur la défense des systèmes gouvernementaux.

Le vice-président (M. James Bezan): Allez-y, monsieur Khoury.

M. Sami Khoury: Nous surveillons les systèmes gouvernementaux en permanence et nous les mettons à jour en fonction des derniers indicateurs de menace. Nous collaborons étroitement avec Services partagés et le Conseil du Trésor pour assurer la protection des technologies de l'information au sein du gouvernement.

Dans la foulée de la recommandation du Comité des parlementaires sur la sécurité nationale et le renseignement, nous épaulons les petits ministères, les organismes gouvernementaux et les sociétés d'État afin qu'ils contribuent à nos capacités de défense.

M. Pat Kelly: D'accord, je vous remercie.

Qu'en est-il du Commissariat à la protection de la vie privée? En réponse à une question précédente, vous avez indiqué que les entreprises n'ont pas l'obligation de signaler les logiciels de rançon, le piratage ou les pertes de données, mais elles doivent faire une déclaration à ce sujet au commissariat. Recevez-vous des informations de cette institution ou travaillez-vous avec elle pour évaluer la menace?

M. Sami Khoury: Je vous remercie de la question.

Non, nous ne recevons pas de renseignements du Commissariat à la protection de la vie privée. Les entreprises ont l'obligation de rendre des comptes à divers organismes. Il s'agit parfois du Commissariat et parfois des organismes de réglementation. Nous prêtons main forte dès qu'un incident nous est signalé. Nous communiquons toujours avec les victimes et leur offrons notre aide.

M. Pat Kelly: De votre côté, vous ne faites que surveiller les médias. Il doit y avoir une meilleure façon de se tenir au fait des attaques, des demandes de rançon et de ce genre de menaces lorsqu'elles surviennent.

M. Sami Khoury: Nous recueillons des renseignements sur les incidents par divers moyens, notamment par les médias, mais nous recevons également de l'information venant de nos partenaires. Parfois, les victimes vont se manifester elles-mêmes. Nous sommes mis au courant de différentes manières, mais nous ne sommes évidemment pas informés de tous les cyberincidents.

Le vice-président (M. James Bezan): Je vous remercie; votre temps est écoulé.

Je signale simplement que l'image à l'écran ne fige jamais quand vous participez en personne. Vous êtes à l'abri des cyberattaques à ce moment-là.

M. May va poser les dernières questions.

● (1635)

M. Bryan May (Cambridge, Lib.): Je vous remercie bien, monsieur le président. Je prends bonne note de votre remarque, car le Comité a du mal à m'entendre aujourd'hui.

Tout d'abord, je tiens à remercier les experts qui témoignent aujourd'hui; grâce à eux, notre étude part du bon pied. Mes questions porteront sur la Russie et l'Ukraine.

Depuis l'invasion de la Russie en Ukraine et en particulier depuis que le Canada et nombre d'alliés de l'OTAN fournissent énormément de matériel, la Russie a averti qu'elle pourrait riposter en lançant des cyberattaques contre l'OTAN. À votre avis, cette menace s'est-elle concrétisée?

M. Sami Khoury: Je vous remercie de cette question.

La menace ne s'est pas matérialisée directement, mais par des conséquences indirectes.

Dans l'affaire soulevée par ma collègue Mme Tayyeb, la Russie a perturbé les communications satellitaires en s'en prenant à Viasat. Or, certaines entités occidentales faisant affaire avec Viasat ont aussi été touchées. Cette attaque russe visait à nuire aux communications ukrainiennes, mais elle a entraîné un contrecoup à plus grande échelle. Ce type de menace s'est donc bel et bien matérialisé.

Or, des groupes de pirates aux visées semblables ont joint les efforts de la Russie pour cibler les gouvernements occidentaux. Les attaques les plus connues ont pris la forme de dénis de service distribué en Allemagne et ailleurs dans le monde.

Le vice-président (M. James Bezan): Monsieur May, nous ne vous entendons pas.

M. Bryan May: Pour une raison ou une autre, mon petit appareil ne fonctionne pas très bien, ici. M'entendez-vous, monsieur?

Le vice-président (M. James Bezan): Nous allons reprendre du début.

Allez-y.

M. Bryan May: Je vous remercie.

Dans ce contexte, pouvez-vous prendre un instant pour nous dire quelles stratégies la Russie met en oeuvre dans sa cyberguerre contre le Canada? Ces stratégies ont-elles changé depuis l'an dernier?

M. Sami Khoury: Je vous remercie de la question.

Je répète que la Russie est un acteur majeur, qui a déployé des capacités cybernétiques destructives en Europe ou du moins en Ukraine. La Russie a utilisé ces capacités à deux reprises pour rendre le réseau électrique ukrainien inopérant.

Nous sommes très inquiets, et nous aidons les fournisseurs des infrastructures essentielles au Canada à prendre toutes précautions et toutes les mesures nécessaires pour protéger leurs réseaux contre ce genre de cybermenaces. Les communications ponctuelles et les bulletins d'information que nous envoyons à l'intention des entreprises canadiennes servent à transmettre les enseignements que nous tirons de toute activité cybernétique, de ce qui se déroule en Ukraine et de tout ce que fait la Russie dans le monde.

M. Bryan May: Comment le Centre de la sécurité des télécommunications soutient-il les Forces armées canadiennes, surtout en matière de collecte de renseignement et de contre-espionnage?

Mme Alia Tayyeb: Je peux répondre à cette question.

Nous travaillons en collaboration de manière très étroite avec les Forces armées canadiennes en matière de communication de renseignements. Nous leur transmettons tous les renseignements que nous recueillons, qu'il s'agisse de menaces pour le déploiement de forces armées à l'étranger ou de menaces internes au Canada qui pourraient affecter le ministère de la Défense nationale, avec lequel nous entretenons également une relation de travail très étroite.

En ce qui a trait aux autres formes de coopération, j'ai parlé des cyberopérations étrangères et de la manière dont nous travaillons en étroite collaboration avec le ministère de la Défense sur ce dossier.

J'ajouterais que, selon notre loi habilitante, nous avons également un mandat d'assistance. Ce mandat nous demande explicitement de fournir de l'aide aux Forces armées canadiennes et, ce faisant, de suivre leurs directives. Toutefois, nous pouvons utiliser nos compétences techniques, nos aptitudes et nos capacités pour aider les Forces canadiennes dans leurs opérations si elles en faisaient la demande.

Je vous remercie.

M. Bryan May: Merci.

Je pense que mon temps de parole est écoulé, monsieur le président.

Le vice-président (M. James Bezan): Je vous remercie, monsieur May.

Pour poursuivre sur le même sujet et exercer quelque peu ma prérogative à titre de président, j'aimerais vous poser une question. Depuis que le CST appuie les Forces armées canadiennes dans le cadre de son nouveau mandat formulé en 2019, cette aide s'applique-t-elle à la fois aux opérations défensives et offensives?

● (1640)

Mme Alia Tayyeb: Le volet de demande d'assistance de notre mandat précise que nous agirions sous l'autorité des Forces armées canadiennes, dans la mesure où elles reçoivent le feu vert pour mener des opérations. Que ce soit pour des opérations de nature défensive ou offensive, nous serions habilités à aider les forces dans la mesure où leurs prérogatives le permettent.

Le vice-président (M. James Bezan): J'aimerais également approfondir l'enjeu de la protection des infrastructures canadiennes.

Dans quelle mesure travaillez-vous avec nos partenaires du secteur public et du secteur privé, tels que les institutions financières, les centres de transport, les systèmes de soins de santé et d'autres éléments de ce type qui pourraient être considérés comme des cibles vulnérables par nos adversaires?

M. Sami Khoury: Merci de cette question.

Nous travaillons beaucoup avec le secteur privé et le secteur public. Nous intervenons sur plusieurs forums d'engagement pour offrir des renseignements à nos partenaires de manière régulière. Par exemple, nous organisons un forum toutes les deux semaines pour tenir le secteur des soins de santé informé des menaces les plus récentes. Dans la plupart des cas, nous disposons de plus de 500 employés prêts à répondre à une demande d'aide.

Nous entretenons des liens de collaboration plus intime, par exemple, avec des partenaires du secteur bancaire et du secteur de l'électricité, ainsi qu'avec des fournisseurs de gaz naturel. Nous adaptons nos engagements aux collectivités qui ont des infrastructures, des technologies ou des capacités similaires, mais nous offrons nos services à la quasi-totalité des 10 centres d'infrastructures essentielles au Canada.

Le vice-président (M. James Bezan): Merci beaucoup.

Je tiens à remercier M. Khoury et Mme Tayyeb d'avoir été des nôtres aujourd'hui. Vos déclarations ont été très intéressantes, et c'était une excellente façon d'amorcer notre étude sur la cybersécurité.

Sur ce, nous allons suspendre la séance.

Je demanderais aux prochains témoins de se présenter à la table et de se connecter en ligne, afin que nous puissions poursuivre la séance dans les plus brefs délais.

● (1640)

_____(Pause)_____

● (1640)

Le vice-président (M. James Bezan): Nous reprenons la séance. C'est parti.

Pour la deuxième heure, nous accueillons deux membres du Centre pour l'innovation dans la gouvernance internationale. Nous recevons par vidéoconférence Aaron Shull, directeur général et avocat général, ainsi que M. Wesley Wark, agrégé supérieur, qui est avec nous en présentiel, ce qui nous fait beaucoup plaisir.

Vous avez droit à cinq minutes chacun pour nous présenter vos observations préliminaires. Monsieur Shull, vous allez commencer.

● (1645)

M. Aaron Shull (directeur général et avocat général, Centre for International Governance Innovation): Merci beaucoup, monsieur le président.

Je tiens à remercier sincèrement les membres du Comité de m'avoir invité à comparaître aujourd'hui. C'est un honneur pour moi d'avoir l'occasion de discuter d'un enjeu crucial, soit la cybersécurité et les capacités des acteurs étrangers.

Pour aborder ce problème de manière efficace, je pense que le gouvernement doit adopter une stratégie à plusieurs volets. Je suis conscient qu'il y a urgence, alors plutôt que de décrire l'état actuel de la cybersécurité — les deux témoins précédents ont abordé les diverses menaces auxquelles notre pays est confronté —, je vais commencer par la fin et proposer quelques pistes de réflexion sur les solutions que le gouvernement pourrait mettre en œuvre.

J'ai eu l'occasion de me familiariser avec les observations de mon collègue, M. Wark, et je dois dire que j'approuve les solutions qu'il s'apprête à vous présenter. Je vais donc me concentrer sur mes propres propositions.

Premièrement, je pense que le gouvernement devrait inciter les entreprises à adopter les mesures de sécurité les plus récentes, telles que le programme CyberSécuritaire Canada mis sur pied par ISDE et par le CST, qui s'adresse aux petites et moyennes organisations. La norme offre un niveau de protection élevé. Le problème, c'est que son adoption demeure limitée jusqu'à présent.

Une autre solution est la mise en place d'un système de crédit d'impôt. Une telle mesure incitative contribuerait à accroître le niveau général de cybersécurité au pays et à réduire le risque de cyberattaques visant nos entreprises. Ce type d'attaques entraîne des pertes financières importantes, la perturbation des opérations, ainsi qu'une atteinte à notre réputation. La mise en œuvre d'un système de crédit d'impôt nous permettrait d'attirer des investisseurs et d'augmenter la productivité et la rentabilité de nos entreprises. Les normes en matière de cybersécurité existent déjà, mais trop peu d'entreprises les appliquent. Un vieux dicton dit que l'on ne peut pas obliger les abeilles à se rassembler, mais que l'on peut en revanche choisir l'endroit où l'on pose le pot de miel. Je propose donc d'encourager nos entreprises à adopter les normes en leur accordant un crédit d'impôt.

Deuxièmement, je pense que le gouvernement doit établir un cadre juridique clair et concis pour faire face aux cyberattaques, un cadre comprenant des lignes directrices en matière d'attribution, d'intervention et de responsabilité. La structure de gouvernance de ce cadre devrait toutefois demeurer souple et être en mesure de s'adapter à un contexte qui évolue rapidement. Les règlements devraient être élaborés par des experts en fonction de bonnes pratiques, et non de stratagèmes politiques. Le gouverneur en conseil devrait être en mesure d'approuver les normes, les codes de pratique et les programmes de certification, agissant comme un mécanisme de conformité intégré.

Troisièmement, le gouvernement devrait mettre en place une plateforme annuelle multilatérale pour assurer la participation et la collaboration des acteurs concernés par la question de la cybersécurité. Une telle plateforme devrait rassembler des participants de tous les ordres du gouvernement, du secteur privé, de l'industrie, des communautés autochtones, du milieu universitaire, des organismes à but non lucratif, et des chefs de file en matière de maintien de l'ordre. À mon avis, la cybersécurité devrait être une préoccupation pour l'ensemble de la société canadienne. Tout le monde, y compris les groupes de réflexion, doit faire davantage d'efforts pour s'attaquer à ce problème.

Ainsi, mon organisation, le CIGI, prévoit d'organiser en juin le premier dialogue de Waterloo sur la sécurité. Ce sommet, qui va réunir divers intervenants, vise à mettre en place des discussions et des simulations pour mieux comprendre les répercussions des cyberincidents, les mesures d'intervention et de rétablissement, de même que les rôles et les responsabilités de chacun.

Parlons à présent des différents types de menaces. Comme les témoins précédents l'ont mentionné, il existe des menaces persistantes actives, c'est-à-dire des cyberattaques coordonnées et ciblées souvent menées par des acteurs étatiques, et qui visent à voler des renseignements sensibles ou à perturber des infrastructures essentielles sur une longue période.

Il y a d'abord les rançongiciels, dont nous avons déjà parlé. Il s'agit de logiciels malveillants qui cryptent les fichiers de la victime, à qui ils exigent un paiement pour obtenir une clé de décryptage. Nous sommes aussi maintenant confrontés à ce qu'on appelle la double extorsion, qui consiste à menacer un internaute de divulguer des renseignements très sensibles à son sujet. Non seulement les renseignements de la victime se retrouvent verrouillés, mais le pirate peut alors exiger un paiement en la menaçant de divulguer des renseignements sensibles pouvant la mettre dans l'embarras.

Il y a ensuite les attaques visant la chaîne d'approvisionnement. Ce type d'attaque se produit lorsqu'un individu arrive à compromettre le logiciel ou le matériel d'un fournisseur pour transmettre un code malveillant à ses clients. De mémoire d'homme, la plus connue de ce type d'attaques est probablement l'incident SolarWinds de 2020. Le populaire logiciel de gestion SolarWinds avait été piraté pour compromettre des milliers d'organisations.

Un autre type de menace est l'ingérence dans les élections. Cela se produit lorsque des acteurs étrangers se servent de moyens cybernétiques pour pirater les bases de données sur les électeurs, diffuser de la désinformation et manipuler les médias sociaux, le tout dans le but d'influencer l'opinion publique.

Enfin, il y a aussi parfois des attaques contre les infrastructures essentielles d'un pays. On en a déjà parlé dans le contexte du réseau électrique de l'Ukraine. Il s'agit d'un exemple particulièrement frappant d'attaques contre des infrastructures essentielles qui ont eu des répercussions réelles. En 2015, 225 000 personnes ont été privées d'électricité.

Il est évident que les capacités totales des États varient. Dans le contexte des tendances géopolitiques actuelles, je crois que l'hypothèse la plus sûre pour le Canada est que nous allons évoluer dans une « zone grise » dans un avenir prévisible.

Concernant ce que j'entends par « zone grise », je me permets d'adopter la définition de la politique de défense du Canada, qui m'a semblé être la meilleure définition que j'aie vue.

● (1650)

Voici cette définition:

> Les acteurs étatiques et non étatiques poursuivent de plus en plus leurs objectifs à l'aide de méthodes hybrides dans la « zone grise », juste sous le seuil du conflit armé. Les méthodes hybrides consistent à exploiter de manière coordonnée divers instruments diplomatiques, d'information, cybernétiques, militaires et économiques pour atteindre des objectifs stratégiques ou opérationnels. Elles reposent souvent sur la diffusion délibérée de renseignements erronés afin de semer la confusion et la discorde dans la communauté internationale, de créer de l'ambiguïté et de maintenir un déni plausible.

En conclusion, je suis personnellement d'avis qu'il s'agit d'une préoccupation pour l'ensemble de la société canadienne. Cela ne concerne pas uniquement le gouvernement. C'est plutôt une affaire de gouvernance.

J'estime qu'il est de notre devoir de mieux préparer le pays à naviguer dans cette zone grise.

Merci, monsieur le président.

Le vice-président (M. James Bezan): Merci pour ces observations préliminaires.

À vous la parole, monsieur Wark.

M. Wesley Wark (agrégé supérieur, Centre for International Governance Innovation): Merci, monsieur le président.

Je vous suis reconnaissant, monsieur le président, et mesdames et messieurs les membres du Comité, de me donner l'occasion de comparaître devant vous aujourd'hui.

Votre étude porte sur différentes facettes de la cybermenace, mais je vais traiter d'un seul de ces aspects dans les cinq minutes mises à ma disposition pour vous présenter mes observations préliminaires. Je vais ainsi vous entretenir de l'invasion de l'Ukraine par la Russie, une situation qui nous offre d'importantes indications bien concrètes quant à la manière dont les cyberarmes peuvent et vont dorénavant être utilisées en temps de guerre, de concert avec des attaques militaires plus conventionnelles.

Cette façon de faire a d'abord été illustrée par le piratage de Viasat, l'entreprise offrant les services de communication par satellite en Ukraine, dès le premier matin de l'invasion russe. Des représentants du Centre de la sécurité des télécommunications vous ont d'ailleurs déjà parlé de cette attaque.

Que savons-nous des événements survenus depuis le 24 février 2022? Permettez-moi de vous parler de deux études de sources publiques. J'ai d'ailleurs transmis à votre greffier les liens pour avoir accès à ces études.

En juin 2022, le Centre pour la sécurité des télécommunications, l'instance canadienne responsable de la cybersécurité, a publié un bulletin sur les cybermenaces qui faisait état d'importantes cyberactivités de la Russie parallèlement à ses attaques militaires contre l'Ukraine pendant la période de février 2022 à mai 2022.

Parmi les principaux avis exprimés dans ce bulletin, notons que le CST considérait que les cyberopérations russes étaient plus sophistiquées et étendues que le laissaient entendre les sources d'information publiques et que, au-delà du théâtre ukrainien, les auteurs de cybermenaces parrainés par la Russie se livraient à de vastes campagnes de cyberespionnage visant les pays de l'OTAN. On notait en outre que la Russie était en train de se donner de nouvelles cybercapacités pour s'attaquer à ces cibles, et notamment au Canada.

En janvier 2003, l'agence ukrainienne de cybersécurité a rendu public un rapport — heureusement traduit en anglais —, fruit d'une méthodologie assez semblable à celle utilisée par le CST, où l'on documentait la portée des cyberattaques russes et leur déploiement de concert avec les bombardements conventionnels de février jusqu'à novembre 2022.

Une des constatations importantes du rapport ukrainien concerne la façon dont les cyberattaques russes ciblent les infrastructures énergétiques de l'Ukraine dans le cadre d'une intensification des efforts menés par la Russie pour détruire les sources civiles d'alimentation électrique et saper du même coup le moral des Ukrainiens. Selon le SBU, le service de sécurité ukrainien, les Russes lançaient en novembre 2022 une moyenne de 10 cyberattaques par jour à l'encontre des infrastructures énergétiques essentielles de l'Ukraine.

Les responsables ukrainiens de la cybersécurité souhaitent que le reste du monde soit conscient de la cyberguerre qu'ils doivent livrer. Ils réclament l'adoption d'une démarche commune pour contrer les cyberagressions, le recours à des sanctions pour miner les cybercapacités d'un agresseur, un meilleur partage de l'information au sujet des cybermenaces et une dénonciation claire des cyberattaques à l'encontre des infrastructures civiles essentielles comme étant des crimes de guerre, en même temps qu'une volonté de demander des comptes aux auteurs de ces crimes.

Comment le Canada devrait-il répondre à toutes ces revendications? Voici ce que je recommande.

Premièrement, il faut s'assurer que le CST est en mesure d'offrir la meilleure aide possible à l'Ukraine en matière de cybersécurité et de renseignement sur les transmissions.

Deuxièmement, le gouvernement du Canada doit continuer à offrir un soutien financier suffisant pour assurer la résilience des cybersystèmes ukrainiens.

Troisièmement, nous devons avoir recours, de concert avec nos alliés, à des sanctions ciblées afin de miner les cybercapacités de l'État russe et de ses mandataires. Je pense que nous devons également continuer de documenter et de dénoncer publiquement les cyberagressions de la Russie à l'encontre de l'Ukraine et de l'OTAN. Nous devrions selon moi être aux avant-postes des efforts consentis pour donner suite à la requête de l'Ukraine qui veut que les cyberattaques contre les infrastructures essentielles soient désignées comme étant des crimes de guerre en droit international et aider les Ukrainiens à demander des comptes aux coupables.

Enfin, nous devons nous assurer de pouvoir toujours compter sur des moyens efficaces de surveiller les cyberattaques russes contre l'Ukraine afin de pouvoir en tirer des enseignements. Il faut pour ce faire appuyer les travaux de recherche menés par les universitaires et les ONG du Canada en plus de faire appel à l'expertise du secteur privé.

La cyberguerre que la Russie mène à l'Ukraine nous a appris trois choses. Premièrement, les civils sont une cible de choix. Deuxièmement, les cyberarmes ne sont pas des munitions de précision. Troisièmement, les cyberagressions ne connaissent ni règles ni limites.

Mais le pire se pointe peut-être à l'horizon. Je parle de la menace d'une autre attaque au moyen d'un logiciel malveillant, comme NotPetya, avec des ramifications mondiales. NotPetya a servi à une opération de cyberpiratage de la GRU — l'agence de renseignement militaire de la Russie — lancée en juin 2017 contre l'Ukraine. L'opération est devenue hors de contrôle, comme cela arrive souvent avec ces attaques faisant intervenir des logiciels malveillants, pour finir par paralyser le transport de conteneurs à l'échelle planétaire. Un conseiller à la sécurité intérieure du président des États-Unis a dit de cette attaque que c'était l'équivalent d'utiliser une bombe nucléaire pour réaliser un gain tactique de faible importance.

● (1655)

Nous devons nous efforcer de contrer les menaces cybernucléaires de la même manière que nous devons éviter que le conflit en Ukraine dégénère en guerre nucléaire.

Monsieur le président, je vais conclure en espérant ne pas vous avoir trop donné l'impression d'entendre un savant un peu fou.

Merci.

Le vice-président (M. James Bezan): Merci beaucoup.

J'ai trouvé vos deux déclarations préliminaires fort intéressantes.

Nous allons maintenant passer au premier tour de questions.

Madame Kramp-Neuman, vous avez six minutes.

Mme Shelby Kramp-Neuman: Merci, monsieur le président.

Monsieur Wark, merci de votre témoignage. Mes premières questions seront pour vous.

Dans quelle mesure les tensions du côté de la Russie exigent-elles un apport supplémentaire en ressources et en soutien militaire de telle sorte que le Canada puisse vraiment être à la hauteur sur la scène internationale?

M. Wesley Wark: Merci pour la question.

Je ne suis pas certain de l'avoir bien saisie, mais je crois que cela concernait nos capacités de défense ou les capacités de nos forces armées. Je pense qu'il faudrait… Je suis certes d'accord avec vous.

Il y a sans doute une façon conventionnelle de voir les choses… Nous verrons ce que le gouvernement décidera dans sa prochaine mise à jour de l'examen de sa politique de défense. Je crois toutefois que l'on déterminera que nos forces armées ont besoin de nouveaux équipements en grande quantité pour pouvoir jouer un rôle efficace dans tout conflit à venir, notamment à l'appui de notre propre souveraineté aux côtés de nos alliés. Nous en avons beaucoup à faire à ce chapitre.

Je pense que nous sommes tous conscients qu'il manque différentes choses à nos Forces armées canadiennes, en commençant par des effectifs suffisants pour aller jusqu'à des capacités militaires de pointe. Bon nombre de ces besoins criants ont déjà été signalés.

En tant que simple citoyen, je dois dire que le fait que nous avons pu seulement fournir quatre chars d'assaut Leopard 2 à l'Ukraine témoigne on ne peut mieux de la mesure dans laquelle nous avons laissé nos capacités militaires se dégrader de façon catastrophique au fil des ans.

Merci.

Mme Shelby Kramp-Neuman: Merci. Je passe à ma question suivante.

Il y a un manque de main-d'œuvre et le moral est à son plus bas. En outre, on craint de plus en plus que le Canada soit laissé pour compte dans le contexte du Groupe des cinq pendant que le Royaume-Uni, les États-Unis et l'Australie continuent d'aller de l'avant.

Dans quelle mesure la situation s'est-elle détériorée au cours des 10 dernières années et que doit faire le Canada pour rétablir des liens à ce niveau?

M. Wesley Wark: Merci pour cette question.

Ma réponse va aller dans une direction un peu différente, car je ne suis pas certain d'être totalement d'accord avec vous. Je pense qu'il convient peut-être de faire une distinction entre nos capacités militaires et la manière dont elles se sont dégradées, et nos capacités de renseignement, particulièrement sur les transmissions, et notre contribution au Groupe des cinq.

J'estime que le Canada est, grâce au travail de son Centre pour la sécurité des télécommunications, considéré comme un acteur clé au sein du Groupe des cinq, et a droit au respect de ses partenaires. On m'a indiqué que ceux-ci considèrent que nous figurons parmi les meilleurs pays au monde quand il s'agit d'assurer la cybersécurité des communications et des infrastructures de données fédérales. Notre travail en la matière nous a valu le respect des autres.

Selon moi, le défi va consister pour le Canada à demeurer tout aussi efficace alors que la menace ne cesse de se diversifier.

Nous sommes considérés comme étant un joueur important parmi le Groupe des cinq. Il y aura toujours des choses que ce groupe souhaiterait nous voir faire davantage. À titre d'exemple, on fait pression sur le Canada depuis des décennies pour que nous mettions en place un service de renseignement étranger et une agence pour le renseignement d'origine humaine, mais nous avons toujours résisté. Du point de vue du renseignement sur les transmissions et de la cybersécurité, je pense que nous remplissons bien notre mandat.

Mme Shelby Kramp-Neuman: Merci.

Ma prochaine question sera pour M. Shull.

On s'inquiète de plus en plus de l'utilisation des médias sociaux et de l'information sur notre cybersécurité que les Canadiens acceptent ainsi de communiquer à des entreprises étrangères. En quoi cette utilisation des médias sociaux fait-elle de nous des cibles plus faciles pour les cybermenaces internationales?

M. Aaron Shull: Il y a la cybersécurité conventionnelle qui consiste généralement en un accès non autorisé à des systèmes et à des données. Le sujet que vous abordez — et j'ai vraiment aimé votre question — nous permet d'aller plus loin en nous penchant sur la résilience sociétale. Nous parlons ici des gens et de leurs façons de voir le monde.

Qu'il soit question de désinformation, de mésinformation ou de malinformation, le fait est que les gens sont influençables. Des campagnes perfectionnées sont sans cesse menées pour essayer de changer notre discours, de semer la discorde au sein de la société et d'amener les gens dans des directions différentes alors même qu'il nous faut être unis. Il faut savoir que bon nombre de ces outils sont facilement accessibles sur le marché. L'exemple le plus connu à ce titre est celui de l'ingérence russe dans les élections de 2016 aux États-Unis.

Il ne s'agit pas en fait d'un mauvais fonctionnement du système. Celui-ci fonctionne conformément à la manière dont il a été conçu. Nous devons composer avec les intermédiaires sociaux que sont les plateformes se retrouvant au cœur de notre discours sociétal. Leur but est d'engranger des profits et d'avoir l'auditoire le plus large possible. C'est nous-mêmes qui sommes à l'origine de ce système.

C'est un sujet plus vaste que la cybersécurité à proprement parler, mais c'est une excellente question.

● (1700)

Mme Shelby Kramp-Neuman: Merci.

Dans le même ordre d'idées, quel genre de pouvoir les consommateurs mettent-ils entre les mains des entreprises lorsqu'ils acceptent leurs différentes modalités d'utilisation?

M. Aaron Shull: Ce serait un beau sujet pour une thèse de doctorat.

Je vous dirais que, suivant une estimation qui a été faite, il faudrait quelque chose comme 200 jours à une personne pour lire toutes les modalités de service auxquelles elle donne son assentiment pendant une année.

Je pense qu'il faut surtout considérer que nous avons conçu l'ensemble de notre système en fonction du consentement, ce qui est totalement erroné. C'est un mensonge. En fait, nous ne savons pas ce à quoi nous consentons. Pour illustrer le tout, une entreprise a glissé dans ses modalités de service qu'en acceptant les modalités proposées, le consommateur lui fait cadeau de son âme à jamais. Il y a donc maintenant une entreprise à San Francisco qui ne sait tout simplement pas quoi faire de toutes ces âmes qui lui appartiennent.

Mme Shelby Kramp-Neuman: Je reviens à vous, monsieur Wark, étant donné que vous êtes avec nous dans la salle. Comment évaluez-vous les investissements actuels du Canada dans ses infrastructures comparativement à ceux d'autres pays comme les États-Unis, par exemple?

M. Wesley Wark: Je suis désolé, mais vous parlez bien des investissements dans les infrastructures...?

Mme Shelby Kramp-Neuman: Oui, en comparaison avec ceux consentis par d'autres pays comme les États-Unis.

M. Wesley Wark: Je dirais que nous avons un grand pas à franchir pour décider ce que nous souhaitons faire du point de vue de nos infrastructures essentielles.

Nous sommes en attente d'une stratégie en matière d'infrastructures essentielles, une considération toujours à l'étude par le gouvernement fédéral. Il en est question dans le projet de loi C-26 qui traite justement de ces infrastructures. Notre liste d'infrastructures essentielles remonte à 2009. Autrement dit, elle n'a pas été mise à jour depuis cette date qui correspond au lancement de notre dernière stratégie touchant les infrastructures essentielles.

Il faudra d'abord et avant tout déterminer ce que l'on entend exactement par « infrastructures essentielles ». Une fois que cette étape — importante, mais pas facile — aura été franchie, nous devrons réfléchir à la façon dont nous voulons régir le fonctionnement de ces infrastructures essentielles et quelles sont nos attentes à leur égard, surtout aux fins des stratégies de cybersécurité.

Une partie de ce travail est en cours, bien sûr de façon informelle. Des niveaux de cybersécurité très élevés ont pu être atteints à l'égard de certains éléments de nos infrastructures essentielles. Les grandes banques en sont sans doute un excellent exemple. Il existe une grande diversité au sein de ce système.

Mme Shelby Kramp-Neuman: Excellent. Merci beaucoup.

Le vice-président (M. James Bezan): Monsieur Sousa, vous avez la parole.

M. Charles Sousa (Mississauga—Lakeshore, Lib.): Merci beaucoup.

Merci à vous deux pour vos exposés que j'ai trouvé très intéressants. Je vous suis reconnaissant de mettre ainsi en lumière certaines de ces questions dans le contexte de la guerre menée en Ukraine par la Russie et des différents acteurs étrangers qui font peser une menace sur nous tous.

Vous avez traité brièvement de la guerre cognitive, de la mésinformation et de différents phénomènes tout aussi prévalents qui ne manquent pas de causer certains torts. Il ne s'agit pas tant de tactiques visant à nous forcer à faire quoi que ce soit, que de moyens utilisés pour nous faire avaler de fausses informations.

Pouvez-vous me dire, en ne tenant pas compte des influences étrangères, dans quelle mesure de tels agissements sont fréquents au Canada?

M. Wesley Wark: Merci pour cette question.

Il faut préciser d'entrée de jeu que nous comprenons mieux comment les choses se passent dans toute la sphère de l'information. Il est ainsi important de pouvoir établir des distinctions entre les trois catégories d'informations en circulation qui sont susceptibles de nous causer des difficultés.

Il y a d'abord la mésinformation que le CST, entre autres, définit comme étant de la fausse information diffusée sans qu'il y ait de mauvaises intentions. Autrement dit, quelqu'un y croit même si ce n'est pas la vérité. Il y a bien sûr une grande quantité de mésinformation en circulation, en grande partie par l'entremise des médias sociaux. Nous avons par exemple pu en constater les répercussions l'an dernier lors des événements liés au « convoi de la liberté » à Ottawa et ailleurs au pays.

Il y a ensuite la désinformation, soit de l'information fausse et trompeuse souvent diffusée délibérément par des adversaires étrangers ayant comme objectif, pour diverses raisons, de perturber le bon fonctionnement d'une société. Certains pays, comme la Russie et la Chine, sont de véritables experts de la désinformation. La Russie semble vouloir se démarquer à ce chapitre, comme nous avons pu amplement l'observer lors de sa guerre en Ukraine.

On en arrive à la troisième catégorie à laquelle, selon moi, nous devrions nous intéresser de près. C'est ce que le CST et son pendant américain ont qualifié de malinformation. Il s'agit d'une zone grise entre la désinformation et la mésinformation, c'est-à-dire de la manipulation d'informations partiellement vraies et partiellement fausses dans le but d'atteindre certains objectifs.

Nous comprenons de mieux en mieux les impacts de ces différentes formes de diffusion d'informations fausses et trompeuses, même si nous commençons à peine à étudier ce phénomène. En toute franchise, il est très difficile de savoir exactement comment s'en prémunir autrement qu'en essayant de contrer les agissements de certains acteurs étrangers.

● (1705)

M. Charles Sousa: Tout indique que le phénomène se manifeste surtout à partir de l'étranger. Ne vous intéressez-vous pas également à ce qui peut se faire au pays?

M. Wesley Wark: Toute intervention à l'intérieur du pays dans le contexte du débat politique risque de soulever d'importantes préoccupations du point de vue de la Charte des droits.

Il est beaucoup plus simple, malgré que cela demeure très complexe du point de vue technologique, de s'en prendre à des actes de toute évidence inappropriés et illégaux, comme ceux perpétrés par d'autres pays. C'est d'ailleurs la raison pour laquelle le CST et d'autres ministères fédéraux ont notamment pour mandat de contrer la désinformation émanant d'États étrangers.

M. Charles Sousa: Dans quelle mesure l'intelligence artificielle et la technologie quantique sont-elles efficaces? Est-ce que ces éléments font partie des mesures de cybersécurité prises pour contrer les agissements étrangers?

M. Wesley Wark: L'intelligence artificielle a certes un rôle à jouer et on l'utilise d'ores et déjà de différentes manières. L'informatique quantique et les applications qui en découleront sont des pistes de solution pour l'avenir, et je ne suis pas un expert en la matière. En toute franchise, j'espère ne plus être là lorsqu'on finira par mettre ces solutions en place. On peut formuler bien des hypothèses sur la forme que prendront ces applications, mais nous n'en sommes pas encore rendus là.

M. Charles Sousa: Comment nous en tirons-nous face aux cybermenaces en provenance de la Russie et de la Chine?

M. Wesley Wark: C'est une bonne question.

Je pense que nous nous en tirons plutôt bien. Je pense qu'il est particulièrement important de prêter attention à la guerre en Ukraine parce que c'est un laboratoire pour la cyberguerre. C'est véritablement le premier laboratoire important que nous ayons vu à cet égard. Il est donc très important que nous étudiions tout ce qui a été utilisé par la Russie contre l'Ukraine, et la façon dont l'Ukraine a répondu. Nous sommes dans une position privilégiée pour pouvoir étudier cela.

M. Charles Sousa: Les contre-attaques de l'Ukraine sont-elles efficaces dans ce domaine?

M. Wesley Wark: Oui, elles le sont. Je dirais que c'est en partie parce que ce pays a une longue expérience en la matière qui remonte à 2014 et à l'incursion initiale des Russes en Crimée et ailleurs. Les Ukrainiens n'ont cessé de renforcer leurs capacités depuis ce moment-là. Ils ont non seulement renforcé leurs capacités nationales et profité du soutien populaire pour y arriver, mais ils ont également reçu beaucoup d'aide d'alliés importants de l'Ouest et de tous les partenaires du Groupe des cinq.

M. Charles Sousa: Dans le cadre de l'infrastructure mobilisée par le Canada face à certains des efforts déployés par des acteurs étrangers, avons-nous établi un partenariat avec l'OTAN et avec d'autres intervenants pour lutter collectivement contre les atteintes à la cybersécurité? Lorsque nous faisons cela, est-ce que nous nous exposons à d'autres acteurs?

M. Wesley Wark: Je pense que c'est une question intéressante.

Je pense que le réseau d'alliances important auquel le Canada participe et dans lequel il est en mesure de faire un travail important est le partenariat du Groupe des cinq. En effet, un grand nombre des membres de ce partenariat, ou du moins certains d'entre eux, sont également membres de l'OTAN — le Canada, les États-Unis et le Royaume-Uni —, ce qui a des répercussions sur l'OTAN. Le Groupe des cinq est le partenariat le plus important pour renforcer la cybersécurité. Je pense que des efforts considérables sont déployés dans les coulisses.

Très rapidement, j'aimerais attirer l'attention du Comité sur l'un des problèmes auxquels fait face le Canada. Le Centre de la sécurité des télécommunications a un certain mandat qu'on peut voir à l'œuvre dans son évaluation des cybermenaces, qui a été mentionnée plus tôt par des représentants de l'organisme. Ils veulent parler de menaces stratégiques à l'encontre du Canada, c'est-à-dire des menaces actives provenant d'États étrangers, parce que cela fait partie de leur mandat. Il existe cependant toute une gamme de menaces à l'encontre du Canada et des Canadiens, notamment par l'entremise de la cybercriminalité, qui n'entre pas dans le mandat du Centre de la sécurité des télécommunications. En effet, ce type de menaces relève plutôt de la GRC.

Je ne fais que prier les membres du Comité de se pencher — dans le cadre de cette étude, s'ils ont le temps, ou plus tard — sur la façon dont la GRC peut faire face au vaste monde de la cybercriminalité et à ses répercussions.

Le vice-président (M. James Bezan): Je vous remercie.

[*Français*]

Monsieur Desilets, soyez le bienvenu au Comité permanent de la défense nationale.

Vous avez la parole pour 16 minutes, s'il vous plaît.

M. Luc Desilets (Rivière-des-Mille-Îles, BQ): Avez-vous bien dit « 16 minutes », monsieur le président?

● (1710)

[*Traduction*]

Le vice-président (M. James Bezan): Je veux dire six minutes. Vous avez six minutes.

[*Français*]

M. Luc Desilets: Merci, monsieur le président.

Je remercie nos invités.

Je siège occasionnellement au Comité, et je trouve le sujet vraiment fascinant et passionnant. Par contre, c'est un sujet inquiétant, mais aussi plein d'avenir.

Mes premières questions s'adresseraient à M. Shull.

Selon vous, les cyberattaques que l'on subit à petites doses, mais qu'on subira probablement de plus en plus, pourraient-elles être, à la limite, considérées comme des crimes de guerre?

[*Traduction*]

M. Aaron Shull: C'est une très bonne question. En effet, des hauts représentants du gouvernement ukrainien ont demandé que les cyberactivités offensives en Ukraine soient considérées comme des crimes de guerre. À l'heure actuelle, ce n'est probablement pas le cas, mais ce n'est certainement pas quelque chose qui…

[*Français*]

M. Luc Desilets: Excusez-moi, monsieur Shull.

Monsieur le président, la qualité du son ne semble pas adéquate pour l'interprète.

[*Traduction*]

Le vice-président (M. James Bezan): Pouvez-vous vous assurer que votre microphone est au bon endroit? Veuillez parler plus fort et essayer de nouveau, s'il vous plaît.

M. Aaron Shull: Est-il possible d'interpréter mes interventions si je parle lentement?

Le vice-président (M. James Bezan): Malheureusement, nous ne pouvons pas accepter d'autres interventions de votre part, monsieur Shull, car la qualité du son n'est pas assez bonne pour l'interprétation. Vous pouvez peut-être vous déconnecter, quitter l'écran, vous reconnecter et tenter d'améliorer votre son pour que nous puissions vous entendre suffisamment pour que le service d'interprétation puisse faire son travail.

J'ai arrêté le chronomètre, monsieur Desilets. Vous pouvez adresser vos questions à M. Wark, si vous le souhaitez.

[*Français*]

Monsieur Desilets, vous avez la parole.

M. Luc Desilets: Reprenons-nous avec le même témoin?

Il semble que non. Puisque les difficultés techniques ne sont pas résolues, nous allons poursuivre avec un autre témoin.

[*Traduction*]

Le vice-président (M. James Bezan): Vous devez poursuivre la discussion avec M. Wark.

[*Français*]

M. Luc Desilets: Monsieur Wark, on a beaucoup parlé de la firme McKinsey & Company, dernièrement. Étant donné que cette firme a aussi des liens avec la Chine, croyez-vous que cela pourrait avoir un impact en matière de sécurité nationale du Canada?

[*Traduction*]

M. Wesley Wark: Je vous remercie.

Je ne suis pas un expert en matière de contrats et j'hésite donc à répondre. Je pense que la réponse que vous avez eue des intervenants du Centre de la sécurité des télécommunications est probablement la plus appropriée, c'est-à-dire que la sécurité des contrats est une question qui relève de Services publics et Approvisionnement Canada. D'après mon expérience à titre de sous-traitant occasionnel — mais pas à l'échelle de McKinsey —, c'est une question que cet organisme prend très au sérieux.

[*Français*]

M. Luc Desilets: Vos travaux ne se comparent pas à ceux de la firme McKinsey & Company. C'est ce que je comprends.

Plus tôt, vous avez fait allusion au Groupe des cinq. En ce qui concerne la position et la participation du Canada actuellement, quels seraient vos commentaires ou critiques?

La participation canadienne est-elle suffisante et adéquate?

Quelles sont les failles?

[*Traduction*]

M. Wesley Wark: C'est une question très intéressante, mais à laquelle il est très difficile de répondre pour quelqu'un de l'extérieur, comme moi, qui n'a pas participé aux réunions ou aux communications du Groupe des cinq.

Je crois savoir que le Canada est membre du Groupe des cinq et qu'il a joué un rôle important dans l'élargissement du système de ce groupe. Notre pays est membre depuis 1949, et nous faisons donc partie de ce regroupement depuis très longtemps.

Notre principal investissement dans le Groupe des cinq a toujours été lié aux domaines du renseignement d'origine électromagnétique et de la cybersécurité, mais nous sommes allés plus loin au fil des ans et de l'essor du Groupe de cinq. Je pense que le Canada pourrait apporter une plus grande contribution au Groupe des cinq dans un éventail de domaines. Cela soulève l'éternelle question, par exemple, d'un service de renseignement étranger et des renseignements supplémentaires qu'il pourrait fournir au Canada.

Les autres partenaires du Groupe des cinq s'attendent également à ce que le Canada joue un autre rôle et le Canada est en mesure de le jouer à l'occasion, mais probablement pas avec toute la force nécessaire; il s'agit de l'évaluation des menaces à la sécurité mondiale. L'évaluation des menaces est un élément important pour le Groupe des cinq, et les partenaires de ce groupe aiment obtenir des perspectives multiples sur des questions complexes et changeantes liées aux menaces mondiales. Nous disposons de certaines capacités à cet égard, mais je pense que nous pourrions investir davantage dans l'aspect analytique du renseignement, qui reçoit souvent beaucoup moins d'attention que l'aspect de la collecte. Je parle du renseignement d'origine électromagnétique ou l'agent sur le terrain.

● (1715)

[*Français*]

M. Luc Desilets: Ce que vous dites est intéressant.

Vous avez parlé des trois types de fausses informations qui circulaient. J'ai beaucoup aimé la catégorisation que vous en avez faite. Vous avez parlé, entre autres, en deuxième lieu, de la désinformation délibérée. C'est un sujet assez nouveau, je crois. Nous avons probablement vécu à une autre échelle un tel type de désinformation.

Selon vous, pouvons-nous faire quelque chose pour contrer ce genre de désinformation délibérée véhiculée par les Russes, par les Chinois, et possiblement par des pays alliés, à certains moments?

[*Traduction*]

M. Wesley Wark: Je vous remercie de votre question.

Nous devrions probablement nous inquiéter davantage des adversaires qui envisagent de mener des campagnes de désinformation et de s'ingérer dans les pratiques démocratiques. Depuis 2016, nous avons consacré une grande partie de notre attention à la possibilité d'une ingérence dans les élections, car c'est un processus fondamental pour la pratique de la démocratie. Nous nous intéressons aussi beaucoup à la façon dont nos adversaires étatiques peuvent utiliser des cyberoutils pour tenter d'avoir un impact sur les communautés de la diaspora au Canada et chez nos alliés.

Je crois que nous pouvons prendre trois mesures efficaces à cet égard.

La première, et sans doute la plus importante, consiste à surveiller et à dénoncer publiquement ces activités. Cette dénonciation peut servir de moyen de dissuasion contre les acteurs étatiques étrangers qui tentent d'utiliser ces outils, mais elle peut aussi permettre à la population canadienne de comprendre ce qui se passe. Nous le faisons à l'occasion et nous le faisons plus souvent qu'auparavant. Les dénonciations sont toujours délicates, car elles peuvent avoir des répercussions diplomatiques. Mais même si elles peuvent compliquer la situation, je pense que les dénonciations sont importantes.

La sensibilisation de la population est un élément essentiel, mais je dirais qu'un autre élément important qu'on sous-estime souvent est la capacité des Canadiens à prendre des décisions éclairées, au bout du compte, au sujet des renseignements qui sont visiblement faux et des renseignements qui sont diffusés pour le compte d'un État étranger. Je suis peut-être un peu optimiste, mais je continue à faire confiance au bon jugement des Canadiens.

J'aime toujours citer l'exemple de ce que le gouvernement français a fait en réponse à ses préoccupations concernant l'ingérence électorale lors de l'élection nationale de 2016 dans ce pays. En effet, le gouvernement a créé un bureau spécial dans le bureau du président afin de formuler des commentaires satiriques sur les campagnes de désinformation russes mal menées et pour se moquer de ces campagnes. Je pense que c'est une excellente tactique.

Le vice-président (M. James Bezan): Madame Mathyssen, vous avez la parole. Vous avez six minutes.

Mme Lindsay Mathyssen: Je vous remercie, monsieur le président.

Je suis heureuse de voir que M. Shull est de retour en ligne. Je pense que les deux témoins peuvent tenter de répondre à mes questions.

Monsieur Shull, j'aimerais poursuivre la discussion entamée par Mme Kramp-Neuman. Je crois que vous avez abordé l'aspect lucratif des médias sociaux et les dangers qui en découlent, et bien entendu la question des algorithmes qui sont expressément conçus et utilisés pour accroître ces profits, mais qui favorisent au bout du compte la désinformation et parfois la haine en ligne. Nous avons pu observer directement ce phénomène.

Pourriez-vous nous dire quel rôle le gouvernement doit jouer en ce qui concerne la réglementation et la responsabilisation de ces sociétés privées pour qu'elles n'utilisent pas autant ces algorithmes ou qu'elles n'en tirent pas autant de profits?

M. Aaron Shull: Certainement. Je vais seulement vérifier si les interprètes peuvent m'entendre maintenant. Ils ne m'entendent pas du tout?

Le vice-président (M. James Bezan): Malheureusement, nous n'avons pas le feu vert.

Mme Lindsay Mathyssen: Il pourrait peut-être nous envoyer ses réponses.

Le vice-président (M. James Bezan): C'est une bonne idée.

Vous pourriez envoyer votre réponse par écrit au Comité. Vous n'avez qu'à la faire parvenir au greffier, et nous aurons ainsi accès à vos commentaires.

Madame Mathyssen, vous avez la parole.

Mme Lindsay Mathyssen: J'aimerais poser la même question à M. Wark.

M. Wesley Wark: Je vous remercie de votre question.

Le fait que le Centre pour l'innovation dans la gouvernance internationale, qui est au premier plan de la recherche dans le cyberunivers canadien, semble parfois avoir de la difficulté à se connecter est souvent un sujet de plaisanterie entre M. Shull et moi-même, mais…

Des voix: Ha, ha!

M. Wesley Wark: Je dirais que l'une des choses dont M. Shull et moi avons discuté et sur lesquelles nous nous sommes penchés — et je vous offre donc une réponse partielle —, c'est que l'univers des communications dans les médias sociaux est de plus en plus touché par les robots automatisés. Il s'agit simplement de machines qui amplifient, selon divers algorithmes, certains types de messages et qui peuvent être utilisées à des fins de désinformation par des acteurs étatiques étrangers. C'est ce qu'a fait la Russie lors de la campagne électorale de 2016 aux États-Unis. Ces robots peuvent être utilisés par les entreprises de médias sociaux pour accroître l'indice d'utilisation.

Je pense que la conclusion à laquelle nous sommes arrivés — sans disposer des outils nécessaires et sans suggérer la méthode à employer —, c'est que nous devons nous attaquer à la question des robots automatisés d'une manière ou d'une autre, afin de réduire leur impact et la portée de leur utilisation.

● (1720)

Mme Lindsay Mathyssen: J'ai été informée — et j'ai reçu un mémoire à cet égard — sur la façon dont nous envisageons la question des renseignements personnels à l'avenir et sur la façon dont les gens ont le droit d'utiliser ces renseignements personnels. Il a été suggéré que les gens soient payés pour céder leurs renseignements personnels à Facebook, aux médias sociaux ou à toute autre plateforme. L'idée d'une compensation est-elle une solution possible à l'avenir, afin que les gens sachent mieux ce qu'ils obtiennent et qu'un contrat soit essentiellement établi?

M. Wesley Wark: Je vous remercie de votre question.

Je dirais qu'il s'agit d'une question sur laquelle les différents commissaires à la protection de la vie privée se sont successivement penchés avec enthousiasme — non seulement les commissaires fédéraux, mais aussi les commissaires provinciaux, y compris l'ancien commissaire à la protection de la vie privée de l'Ontario — pour essayer d'élaborer un meilleur modèle de consentement qui ne nous oblige pas, comme l'a dit M. Shull, à lire des centaines de pages de langage technique abscons, ce qu'aucun d'entre nous ne fait.

Nous avons visiblement besoin d'un meilleur modèle de consentement, et nous avons certainement besoin de restrictions qui encouragent davantage les entreprises de médias sociaux à utiliser le consentement. Je pense que le gouvernement du Canada a un rôle à jouer à cet égard en établissant des lignes directrices — aussi difficile que cela puisse être, car les plateformes géantes de médias sociaux n'aimeront pas cela —, mais selon moi, c'est un enjeu auquel nous devons nous attaquer.

Mme Lindsay Mathyssen: Si je peux me permettre de changer un peu le sujet, dans le cadre d'une discussion précédente — monsieur Shull, je sais que vous ne pouvez pas contribuer, mais nous pouvons parler de ce qui se trouve dans votre mémoire écrit —, on a parlé d'inciter davantage les petites entreprises à améliorer leurs dispositions en matière de cybersécurité. Mme O'Connell a demandé aux témoins du groupe précédent ce que les municipalités pouvaient faire sur le plan fiscal en ce qui concerne cette infrastructure et ce qu'elles reçoivent en matière de soutien, de conseils, etc.

Monsieur Wark, à votre avis, ce soutien doit-il également être fourni aux municipalités et aux autres ordres de gouvernement?

M. Wesley Wark: Je suis désolé que M. Shull ne puisse pas répondre à cette question. Je vais tenter de répondre pour nous deux au mieux de mes connaissances.

Je pense que la suggestion de M. Shull au sujet des encouragements fiscaux représente certainement une solution possible. La réglementation, du moins sur ce que nous pourrions considérer comme des infrastructures de données et des communications essentielles, en est une autre. Le projet de loi C-26 pourrait avoir des répercussions intéressantes à cet égard, selon ce qu'en fera le Parlement. Cela mérite certainement d'être étudié.

Je pense que la conclusion à laquelle nous sommes arrivés — et les intervenants du Centre de la sécurité des télécommunications ont aussi abordé le sujet —, c'est que même si les principaux intervenants du secteur privé au Canada, y compris le secteur financier et d'autres éléments de l'infrastructure essentielle, ont des niveaux assez élevés de capacités, de sensibilisation et de mise en œuvre en matière de cybersécurité, le véritable problème se situe au niveau des petites et moyennes entreprises. En effet, elles n'ont pas les ressources nécessaires et ne comprennent peut-être même pas la mesure dans laquelle elles sont vulnérables aux cyberattaques.

Je pense qu'il faut se concentrer sur les petites et moyennes entreprises et trouver des moyens de les aider à améliorer leurs niveaux de cybersécurité d'une manière abordable et accessible. C'est le défi à relever.

Le vice-président (M. James Bezan): Je vous remercie encore une fois. Votre temps est écoulé.

Nous entamons maintenant la série de questions de cinq minutes.

Mme Jennifer O'Connell: Monsieur le président, je suis désolée.

Avant de continuer, pourrions-nous demander à M. Shull s'il peut envoyer ses réponses par écrit au Comité? Je pense que ce sont des questions importantes.

● (1725)

Le vice-président (M. James Bezan): Il n'est plus en ligne. Est-ce qu'il est toujours là?

Le greffier du Comité (M. Andrew Wilson): Il est là, il a seulement fermé sa caméra.

Le vice-président (M. James Bezan): Il est à l'écoute.

Monsieur Shull, si vous pouviez répondre à toutes ces questions par écrit, nous vous en serions très reconnaissants.

Mme Jennifer O'Connell: Oui, s'il le souhaite.

Le vice-président (M. James Bezan): Je sais que cela représente un peu plus de travail, mais nous aimerions beaucoup avoir votre contribution.

Nous poursuivons maintenant les délibérations. Monsieur Kelly, vous avez cinq minutes.

M. Pat Kelly: D'accord.

En plus de ce que vous avez dit dans votre déclaration préliminaire, pouvez-vous nous décrire les répercussions d'une possible cyberattaque réussie sur la vie civile au Canada?

M. Wesley Wark: Je vous remercie de la question.

Il y a eu quelques exemples d'attaques contre des détenteurs canadiens de données et de renseignements personnels au fil des ans, monsieur Kelly. Cela dit, aucune attaque n'a été paralysante jusqu'à présent. Les pires attaques remontent probablement à quelques années. Le Conseil national de la recherche a entre autres été la cible d'un piratage, et la reconstruction des systèmes à la suite de cette attaque a pris beaucoup de temps.

Nous apprenons au fur et à mesure, alors je n'ai pas d'autres exemples à vous donner au-delà de ces incidents isolés.

M. Pat Kelly: Lors de l'étude que nous avons menée au cours de la dernière année — c'était une étude plus vaste, mais nous nous sommes penchés sur l'enjeu de la cybersécurité —, nous avons abordé les écarts qui existent entre les Forces armées canadiennes et le Centre de la sécurité des télécommunications.

Diriez-vous que ces écarts existent encore? Les a-t-on comblés? Quels sont les écarts entre nos institutions?

M. Wesley Wark: Monsieur le président, je vous dirais qu'il serait particulièrement intéressant d'entendre le COMRENSFC à ce sujet, car c'est l'organisation au sein du ministère de la Défense nationale qui est la plus affectée par les développements.

Les Forces armées canadiennes ont récemment statué qu'elles avaient nettement besoin d'accroître leur capacité en matière de cybersécurité et de cybercapacités pour leurs opérations offensives et défensives, ce qui a été souligné dans la stratégie de défense « Protection, Sécurité, Engagement » en 2017 — et ce sera peut-être renforcé dans une mise à jour ultérieure. Les FAC cherchent à développer une capacité indépendante et autonome à cet égard dans le cadre de leur mandat, et le CST a été en mesure de les aider à cet effet.

Il ne s'agit pas tant que cela des écarts entre le CST et le COMRENSFC, selon moi. Il s'agit plutôt de savoir dans quelle mesure les Forces armées canadiennes, et le COMRENSFC, surtout, ont su créer le groupe de cyberguerriers dont ils ont besoin.

M. Pat Kelly: Vous avez également effleuré l'aspect des ressources dans vos remarques liminaires. Nous savons à quel point les navires, les jets, les chars d'assaut, etc. coûtent cher.

Le budget est-il insuffisant? Faudrait-il déposer de nouvelles demandes budgétaires pour établir un système de cybersécurité réussi? S'agit-il plutôt d'embaucher le bon personnel? Y a-t-il des lacunes en matière de matériel ou de postes budgétaires onéreux? Si oui, devrait-on prévoir un budget à cet égard à l'avenir?

M. Wesley Wark: Merci.

Je dirais que tout entre en ligne de compte. Selon moi, les principaux défis du COMRENSFC en matière de renforcement des capacités sont en partie d'ordre technologique. Il y a non seulement l'enjeu de l'accès aux meilleurs types de systèmes nécessaires, mais aussi de la capacité en ressources humaines. Il s'agit de trouver un bassin de candidats talentueux qui pourront contribuer à une sorte de cybercadre au sein du ministère de la Défense nationale, que ce soit des civils ou des membres des forces armées. Le COMRENSFC est confronté aux mêmes défis que le CST, bien que peut-être amplifiés, en matière de rétention de la main-d'œuvre, qui a fait l'objet de questions au Comité auxquelles les représentants du CST ont répondu.

Je crois que la situation est particulièrement difficile pour le COMRENSFC. On sait notamment que la culture de l'institution des forces armées n'a pas nécessairement tendance à changer rapidement. On l'a constaté à maints égards.

M. Pat Kelly: Merci. Il me reste moins d'une minute.

Vous avez parlé de systèmes auxquels il faudrait avoir accès; à combien devrait s'élever le budget pour veiller à avoir des systèmes adéquats en place?

M. Wesley Wark: Je ne peux pas vraiment répondre à cette question, pour être franc. Je ne crois pas que le budget serait faramineux, mais il s'agit de dénicher les systèmes et de les obtenir. C'est probablement le plus grand défi.

● (1730)

M. Pat Kelly: La rapidité du processus d'approvisionnement est un facteur, donc.

M. Wesley Wark: Oui.

Le vice-président (M. James Bezan): Le temps file. Nous devrons en faire un usage judicieux d'ici la fin de la séance.

Allez-y, monsieur Fisher.

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

J'aimerais remercier nos témoins d'être ici.

Nous avons beaucoup entendu parler d'infrastructures essentielles aujourd'hui. Mme O'Connell en a parlé avec les autres témoins, tout comme Mme Kramp-Neuman, si je ne m'abuse. Je me questionne tout particulièrement sur la possibilité que certains secteurs soient la cible de cyberattaques financées par un État, qui seraient un moyen d'attaquer le Canada sans avoir recours aux moyens militaires conventionnels.

J'aimerais vous entendre tous deux à ce sujet, mais peut-être pourrions-nous entendre M. Wark maintenant et obtenir l'autre réponse par écrit. Quels sont les secteurs les plus à risque, selon vous? Je pense à la panne de Rogers et à ses répercussions sur les Canadiens un peu partout au pays. Je pense aussi à des catastrophes naturelles telles que la tempête Fiona. Ce type d'événements a démontré notre dépendance en matière d'électricité, de télécommunications, d'essence et de guichets automatiques. Autrefois, Internet était un luxe. Aujourd'hui, cela semble être une nécessité. Il n'y a rien à faire lors d'un tel événement.

J'aimerais vous entendre à ce sujet, monsieur Wark. Quels secteurs sont les plus à risque, selon vous?

M. Wesley Wark: Je vous remercie de la question.

Je vais peut-être vous surprendre, mais je dirais l'espace. On n'a pas tendance à le considérer dans la liste des infrastructures essentielles, mais il faudra le faire à l'avenir. On va s'appuyer de plus en plus sur des plateformes spatiales pour les infrastructures essentielles, les communications, le suivi des répercussions des changements climatiques et bien d'autres choses.

Le gouvernement travaille sur une stratégie en matière d'infrastructures essentielles, et j'espère qu'il y inclura l'espace comme nouveau secteur. Selon moi, il s'agit du milieu le plus vulnérable, non seulement parce que tout y est si nouveau, mais aussi parce qu'il évolue et se développe si rapidement. Le Canada a un rôle à jouer à cet égard. L'espace est un secteur très important.

J'ajouterais autre chose; les agences de renseignement, le CST, le Groupe des cinq et d'autres ont dit que nous sommes présentement la cible d'attaques d'exploration perpétrées par des États étrangers adverses qui tentent de comprendre comment nos systèmes d'infrastructures essentielles fonctionnent et où se trouvent les vulnérabilités. Préféreront-ils attaquer ces systèmes plutôt que de mener une guerre? C'est très difficile à prédire. C'est sans doute peu probable, parce que de telles attaques pourraient mener à toute une escalade, mais certains éléments peuvent être vulnérables, surtout en matière de pratiques démocratiques et d'infrastructure électorale, par exemple.

Je dirais que l'espace et ces systèmes d'infrastructures essentielles qui alimentent nos besoins démocratiques autour des élections en particulier sont deux éléments clés.

M. Darren Fisher: Je pense à ce qui s'est passé dans le Canada atlantique avec la tempête Fiona. Une catastrophe naturelle peut-elle donner lieu à une cyberattaque, étant donné notre dépendance envers le secteur énergétique, le système bancaire, etc.?

M. Wesley Wark: Votre question est intéressante, mais je ne saurais trop y répondre.

Je crois que des adversaires pourraient observer la réponse d'un pays à un tel événement pour voir à quel point il peut se rétablir ou quelles sont les vulnérabilités en matière d'infrastructures essentielles, de communications, de services, etc. Je dirais que de tels événements serviraient probablement davantage à des missions d'observation.

M. Darren Fisher: D'accord.

Nous avons effleuré le sujet des guerres conventionnelles. On entend continuellement que la guerre de l'avenir ne ressemblera pas à ce qu'on voit sur le terrain en Ukraine. Je ne veux pas parler pour vous, mais vous avez entre autres utilisé les termes « de concert » et « hybride ». Je crois que c'est vous qui avez dit que la portée des cyberattaques russes était très « sophistiquée ». Or, la Russie n'a pas le dessus dans la guerre en Ukraine.

Que pensez-vous de la guerre hybride? On entend depuis des années que les guerres futures ne se dérouleront pas sur les champs de bataille d'autrefois. Or, la guerre actuelle est tout de même un peu hybride; il y a des cyberattaques, de la désinformation, et certains moyens militaires conventionnels et traditionnels.

M. Wesley Wark: Votre question est fascinante.

La guerre actuelle en Ukraine nous rappelle grandement la Première Guerre mondiale. Il y a toujours cet élément de force brute, machine contre machine, homme contre homme et femme contre femme dans les combats de nos jours, et il ne faut pas l'oublier.

Je crois qu'au début de la guerre en Ukraine, on s'attendait à ce que les Russes soient nettement plus sophistiqués, tant en matière de capacités militaires conventionnelles qu'en cybercapacités. Cela ne s'est heureusement pas avéré. Cela ne veut pas dire pour autant qu'ils ne tentent pas d'apprendre et de s'améliorer. De toute évidence, la guerre en Ukraine est loin d'être gagnée pour qui que ce soit en ce moment.

On a tendance à trop s'inquiéter entre autres de l'avenir de la guerre et des changements technologiques, mais il est important de tenir compte de cet élément.

● (1735)

M. Darren Fisher: Merci.

Le vice-président (M. James Bezan): Merci. Votre temps est écoulé, monsieur Fisher.

Il nous reste cinq minutes, que se sépareront M. Desilets et Mme Mathyssen.

[*Français*]

M. Luc Desilets: Merci, monsieur le président. Tout à l'heure, votre français était excellent.

Compte tenu de la magnifique idée de ma collègue, j'aimerais que M. Shull puisse retenir trois questions auxquelles nous aimerions avoir des réponses écrites.

Premièrement, une cyberattaque pourrait-elle être considérée comme un crime de guerre?

Deuxièmement, s'il y avait une cyberattaque majeure contre un des pays de l'OTAN, à quel genre de réaction pourrait-on s'attendre? Serait-ce perçu comme une attaque contre l'OTAN, et l'OTAN serait-elle en guerre?

Ma troisième question est assez large. Vous avez fait allusion plus tôt, monsieur Wark, à certaines recommandations que vous souhaiteriez voir apparaître dans le rapport.

Monsieur Shull, de votre côté, aimeriez-vous que le Comité inclue dans son rapport certaines recommandations?

Monsieur Wark, je me tourne vers vous. Je reviens à ma dernière question en lien avec la désinformation, que je trouve extrêmement dangereuse et qui, en ce moment, est partout. Pour ma part, je suis un ancien directeur d'école, et je pense aux jeunes, à l'éducation, et je pense aussi à la prévention qui devrait être faite dans le milieu scolaire pour permettre aux jeunes de savoir distinguer le vrai du faux.

Si on met cet aspect préventif de côté, quelle responsabilité revient aux médias, et quelle responsabilité nous revient, à nous, les élus?

[*Traduction*]

Le vice-président (M. James Bezan): Vous disposez d'une minute pour répondre à la question.

M. Wesley Wark: Merci, monsieur le président.

Je dirais que les médias jouent un rôle très important. Bien sûr, les institutions médiatiques ont évolué au cours des dernières décennies. Il y a les médias traditionnels, mais aussi toutes sortes d'autres médias, désormais. Selon moi, les médias traditionnels ont un code de pratique et d'éthique bien ancré afin de tenter de veiller à rapporter la vérité telle qu'ils la voient et de rendre des comptes. La situation est bien sûr tout autre sur les médias sociaux, où il n'y a pas de code de conduite.

En fin de compte, je crois que cela dépend vraiment de la capacité des Canadiens ordinaires à décider de l'origine de leurs sources d'information. On espère que ces sources ne proviendront pas de chambres d'écho, qui offrent des informations qui confirment des croyances préexistantes. J'espère que de nombreux Canadiens seront finalement en mesure de décider d'une telle chose.

Le vice-président (M. James Bezan): La dernière question vous revient, madame Mathyssen.

Mme Lindsay Mathyssen: Merci.

Il est intéressant de noter, monsieur Wark, que nous avons abordé le sujet de la sécurité de l'Arctique dans une étude précédente.

Nous avons reçu le professeur Byers, qui a dit que nous — le gouvernement y compris — devrions entre autres prioriser le remplacement du système de Constellation RADARSAT en entier. C'était l'une de ses principales revendications. Pourriez-vous nous dire ce que vous en pensez? Êtes-vous du même avis? Il s'agit d'un enjeu majeur.

M. Wesley Wark: Je serai très bref et me référerai à un récent rapport de la vérificatrice générale sur la surveillance dans l'Arctique. On y soulevait un point très important, selon moi, à savoir que le processus d'approvisionnement canadien en matière de nouvelles capacités satellitaires est très lent, surtout pour celles qui nous permettraient de surveiller l'espace arctique, tant à des fins militaires que civiles. Les systèmes satellitaires actuels tels que RADARSAT et le trio de satellites pourraient cesser de fonctionner avant que nous soyons en mesure de les remplacer.

Il y a un écart entre la planification à long terme du ministère de la Défense nationale et de l'Agence spatiale canadienne pour le remplacement de ces systèmes et le moment où leur capacité pourrait devenir insuffisante, et il faut y remédier. La Constellation RADARSAT est très importante pour le Canada. Somme toute, j'estime qu'il nous faut investir beaucoup plus dans les capacités satellitaires pour nos propres besoins.

● (1740)

Mme Lindsay Mathyssen: Je passe un peu du coq à l'âne, mais nous avons beaucoup parlé des besoins en matière de personnel. Il faut avoir les bonnes personnes en poste en matière de cybersécurité. Le Canada en fait-il assez à cet égard? Le gouvernement du Canada pourrait-il en faire plus pour former ces personnes?

Je sais qu'il y a un certain rattrapage à faire, mais que pourrait faire le gouvernement pour attirer ces travailleurs?

M. Wesley Wark: Je crois que ce serait une question de suivi intéressante pour les représentants du CST, qui disposent de leurs propres systèmes de formation au sein de l'organisation. Vous pourriez leur demander s'il serait possible de transposer ces systèmes de formation dans d'autres ministères et organismes fédéraux et le secteur privé.

Je ne connais pas la réponse. Je présume que les lacunes auxquelles vous faites référence sont majeures.

Le vice-président (M. James Bezan): Merci. Le temps est écoulé.

Je m'excuse auprès de Mmes Gallant et O'Connell qui n'ont pas pu poser leurs questions.

Monsieur Wark, en tant que Canadien fier de son héritage ukrainien, je vous remercie de ce que vous avez dit sur l'invasion russe en Ukraine. J'ai trouvé intéressant que vous disiez qu'une cyberattaque en Ukraine devrait être considérée comme un crime de guerre.

Très rapidement, une cyberattaque contre une nation étrangère est-elle un acte de guerre? Oui ou non?

M. Wesley Wark: Je crois que la réponse la plus simple est que ce n'est pas clair dans le droit international, mais j'estime que le Canada pourrait faire preuve d'initiative à cet égard.

Nous avons toujours pris les devants — ou nous aimons le penser, du moins — en matière de développement du droit international, surtout à la Cour pénale internationale, et j'aimerais que le Canada se tienne debout et soutienne la position de l'Ukraine à cet égard en statuant que les cyberattaques contre les infrastructures civiles constituent un crime de guerre.

Le vice-président (M. James Bezan): Merci beaucoup, monsieur Wark.

Je vous remercie aussi, monsieur Shull.

J'aimerais rappeler aux membres du Comité que notre réunion de vendredi portera à nouveau sur la cybersécurité et la cyberguerre. Nous accueillerons des universitaires. Quant aux représentants du ministère de la Défense nationale et des Forces armées canadiennes, nous les rencontrerons la semaine prochaine.

Sur ce, la séance est levée.