CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

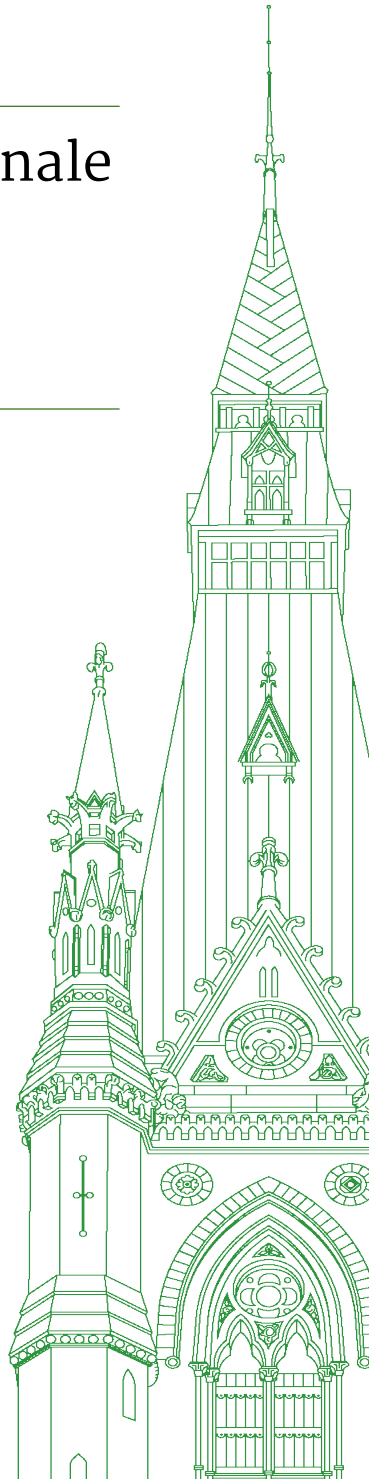
44e LÉGISLATURE, 1re SESSION

Comité permanent de la défense nationale

TÉMOIGNAGES

NUMÉRO 049

Le vendredi 10 février 2023



Président : L'honorable John McKay

Comité permanent de la défense nationale

Le vendredi 10 février 2023

● (0845)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): La séance est ouverte, chers collègues.

J'aimerais d'abord que nous discutions de la motion sur le ballon.

Est-ce que cette motion est toujours dans les airs ou est-ce que vous souhaitez qu'elle atterrisse?

Une députée: Nous allons la présenter.

Le président: Qui veut la proposer?

Mme Cheryl Gallant (Renfrew—Nipissing—Pembroke, PCC): Je propose:

> Que le Comité permanent de la défense nationale invite la 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 président: Souhaitez-vous en débattre?

Mme Shelby Kramp-Neuman (Hastings—Lennox and Addington, PCC): J'aimerais proposer un amendement, afin que la motion se lise comme suit:

> Que le Comité permanent de la défense nationale invite la ministre de la Défense nationale, l'honorable Anita Anand, à comparaître avant le 11 mars 2023 et que le commandant adjoint du NORAD, le lieutenant-général Alain Pelletier, et le commandant de l'ARC, le lieutenant-général Eri Kenny, témoignent au cours de la semaine suivante afin de 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.

Le président: D'accord. Y a-t-il d'autres...?

Est-ce que vous voulez discuter de l'amendement?

M. Bryan May (Cambridge, Lib.): J'aimerais proposer un autre amendement, mais je peux parler de celui-ci.

Le président: Oui, s'il vous plaît.

M. Bryan May: Nous voulons évidemment tenir ces réunions. Tout ce que j'aimerais, c'est que nous ajoutions, au sujet de la participation des représentants, les mots « et tous les autres représentants appropriés ».

Le président: Ou « représentants pertinents »...?

M. Bryan May: Oui, ce serait bien.

La date du 11 mars nous convient. Nous préférerions que ce soit « le plus tôt possible », mais il faudrait en débattre.

J'apporterais aussi un autre changement mineur; je ferais plutôt référence à un « ballon de surveillance en haute altitude », qui est le terme le plus souvent utilisé.

Le président: D'accord. Je crois que notre ballon n'atterrira pas de si tôt.

Nous allons procéder à l'inverse et voir si nous avons un consensus.

La dernière proposition visait à parler d'un « ballon de surveillance en haute altitude ».

Est-ce que cela vous convient?

Un député: Oui.

Mme Shelby Kramp-Neuman: Monsieur le président, nous acceptons les amendements favorables.

Le président: Acceptez-vous les trois?

Mme Shelby Kramp-Neuman: Oui.

Le président: D'accord. Vous acceptez les trois amendements favorables.

(Le sous-amendement est adopté.)

Le président: Nous avons accepté ces amendements. Est-ce que les membres de l'autre côté ont accepté l'amendement de Mme Kramp-Neuman à la motion originale de Mme Gallant?

M. Bryan May: Oui.

(L'amendement est adopté.)

Le président: Nous avons donc une motion claire.

Monsieur le greffier, est-ce bien le cas?

Le greffier du Comité (M. Andrew Wilson): Plus ou moins, oui.

Le président: D'accord.

M. Blaine Calkins (Red Deer—Lacombe, PCC): Est-ce que c'est plus ou c'est moins?

Le président: Je dirais que c'est plus.

Nous savons donc sur quoi porte le vote.

(La motion modifiée est adoptée.)

Le président: Merci, chers collègues. Je ne ferai plus de blagues boiteuses au sujet de l'atterrissage du ballon.

Sur ce, nous pouvons maintenant passer à l'objet principal de la réunion. Nous recevons pour commencer deux témoins: M. Thomas Keenan, qui est professeur à l'Université de Calgary et M. Alex Rudolph, qui est doctorant à l'Université Carleton.

Comme M. Keenan s'est levé le plus tôt ce matin pour pouvoir témoigner devant nous, nous allons lui céder la parole.

Nous vous souhaitons la bienvenue au Comité, monsieur. Vous disposez de cinq minutes.

M. Thomas Keenan (professeur, School of Architecture, Planning and Landscape, University of Calgary, à titre personnel): Merci beaucoup.

Monsieur le président, mesdames et messieurs les membres du Comité, je vous remercie de m'avoir invité à témoigner devant vous aujourd'hui.

J'aimerais vous parler d'un sujet que j'étudie depuis plusieurs années en tant que chercheur, professeur à l'Université de Calgary et boursier de l'Institut canadien des affaires mondiales: l'intelligence artificielle. Je crois qu'elle révolutionnera notre monde, notamment dans les domaines de la cybersécurité et de la cyberguerre, et ce beaucoup plus rapidement que l'on pourrait le croire.

On parle beaucoup de l'intelligence artificielle dans les médias à l'heure actuelle, en raison de la sortie de ChatGPT, entre autres. J'enseignais l'intelligence artificielle il y a 30 ans et bon nombre de mes étudiants qui avaient intégré la rétropropagation à des réseaux neuronaux ont par la suite accompli de grandes choses. De nos jours, l'intelligence artificielle peut tout faire: elle peut détecter de minuscules tumeurs sur l'IRM comme elle peut aider les villes à optimiser leurs feux de circulation.

Il y a toutefois un côté sombre à l'intelligence artificielle: ce qu'on appelle l'intelligence artificielle antagoniste. Ma crainte, c'est que de nombreux secteurs, notamment celui de la défense, adoptent cette technologie sans pleinement comprendre la façon dont elle peut être utilisée contre nous.

Vous avez probablement entendu parler de ces kiosques d'information des centres commerciaux de Cadillac Fairview. La société a été réprimandée par le commissaire à la protection de la vie privée parce qu'elle avait secrètement recueilli des données sur cinq millions de personnes, notamment leur âge approximatif et leur sexe. Comment a-t-elle pu connaître le sexe de gens? En utilisant l'intelligence artificielle et la reconnaissance faciale pour faire une estimation éclairée.

Pendant 25 ans, j'ai offert un programme pour les étudiants très doués du secondaire, qui s'appelait Shad Valley Calgary. Il se terminait par une exposition scientifique où les étudiants pouvaient montrer le fruit de leur travail. Une année, mes étudiants avaient créé un réseau neuronal pour déterminer le sexe d'une personne en fonction des mensurations, comme le rapport taille-hanches. Le représentant de l'un de nos commanditaires est passé par le kiosque; il était plutôt corpulent. Mes étudiants l'ont mesuré et lui ont dit que selon une probabilité de 84 %, il était une femme. Cette erreur s'est avérée une bonne chose parce que mes étudiants ont compris que l'intelligence artificielle ne faisait que des suppositions éclairées.

Les programmes comme ChatGPT ou d'autres vous donnent des réponses qui ne sont associées à aucun pourcentage ou degré d'incertitude. Ils se lisent comme des énoncés de faits. Ils peuvent être dans l'erreur totale. J'ai demandé à ChatGPT: « Est-ce que Danielle Smith est intelligente? » Il m'a répondu: « Je ne peux pas déterminer avec certitude à qui vous faites référence lorsque vous parlez de Danielle Smith. » Le programme dit toutefois que Justin Trudeau est généralement considéré comme étant intelligent. Qu'est-ce qui se passe ici?

J'ai regardé sous le capot de l'actuelle version gratuite de ChatGPT. Sa base de connaissances va jusqu'en 2021. À ce moment-là, Danielle Smith était une animatrice de radio sans emploi. Elle n'est apparue sur la scène politique qu'en 2022. Je suis certain que la base de données de ChatGPT sera mise à jour et que sa réponse ne sera plus la même.

C'est un autre problème. On peut poser une même question deux fois et obtenir des réponses complètement différentes. L'intelligence artificielle ne vous dira pas pourquoi.

Comprenez-moi bien, j'adore l'intelligence artificielle et ses avantages possibles. De nombreuses entreprises vous feront valoir ces avantages, parce qu'elles ont des produits à vendre. Ma mission est de veiller à ce que nous connaissions les risques et à ce que nous utilisions cet outil de façon intelligente.

J'aimerais vous faire part de trois préoccupations relatives à l'intelligence artificielle utilisée dans le cadre de la défense nationale.

Premièrement, la source des données d'apprentissage. L'intelligence artificielle se fonde principalement sur des données du domaine public qui peuvent être inadéquates. Nous avons constaté que les programmes de reconnaissance faciale avaient de la difficulté à reconnaître les personnes de couleur, parce qu'ils avaient été exposés principalement à des visages de personnes blanches. Dans l'industrie de la défense, la plupart — si ce n'est la totalité — des données les plus importantes ne sont pas du domaine public.

Deuxièmement, le manque d'éthique de l'intelligence artificielle. Comment peut-on oublier Tay, le robot conversationnel de Microsoft, qui avait complètement déraillé et avait lancé des idées nazies, proféré des jurons et qualifié le féminisme de culte. Tay ne faisait qu'apprendre des gens qui interagissait avec elle. Malheureusement, c'est ce qu'on lui disait.

Troisièmement, les acteurs malveillants peuvent tenter d'empoisonner la base de données. Une femme a tenté de réécrire l'article de Wikipédia sur les nazis afin de les montrer sous un jour favorable. En 2003, les partisans du Parti démocrate ont associé, dans Google, le terme « échec lamentable » à la biographie officielle de George Bush de la Maison-Blanche. Lorsqu'on recherchait le terme sur Google, une photo du président apparaissait.

● (0850)

Si vous ne voulez pas que votre profil politique soit associé à un échec lamentable ou pire encore, vous devriez prendre bonne note de ce que dit ChatGPT à propos de votre comité:

> Le Comité de la Défense, fort et vigilant,
> Veille sur la sécurité de notre pays,
> Ses membres travaillent avec acharnement,
> Pour défendre nos valeurs avec défi
> Ses membres travaillent avec détermination
> Pour protéger notre nation jour après jour

Mais qu'est-ce que tout cela signifie? Seul ChatGPT le sait, et il ne nous le dit pas.

Merci beaucoup.

● (0855)

Le président: Merci, monsieur Keenan. Il est rare que l'on fasse de la poésie au sujet du Comité.

M. Blaine Calkins: C'est déjà arrivé, mais ce n'était pas aussi gentil.

Le président: Ce n'est pas comparable. Je ne crois pas que nous devrions mettre au vote l'intelligence de l'un ou l'autre des politiciens nommés, ou de ceux qui sont ici aujourd'hui.

Je constate qu'il y a une carte très intéressante derrière vous: les câbles sous-marins du monde.

M. Thomas Keenan: Oui, monsieur.

Le président: Cette carte à elle seule pourrait donner lieu à des discussions très intéressantes. Nous devons toutefois passer à notre prochain témoin.

Monsieur Rudolph, vous disposez de cinq minutes. Allez-y.

M. Alexander Rudolph (doctorant, Department of Political Science, Carleton University, à titre personnel): Monsieur le président, mesdames et messieurs les membres du Comité, je vous remercie de m'avoir invité à témoigner devant vous aujourd'hui.

Je m'appelle Alexander Rudolph. Je suis doctorant à l'Université Carleton et boursier de l'Institut canadien des affaires mondiales. Mes recherches portent sur la façon dont les pays développent des outils institutionnels pour réaliser des cyberopérations et les raisons qui les poussent à le faire. Je m'intéresse grandement au Canada dans le cadre de ma recherche.

Mes commentaires porteront sur deux thèmes aujourd'hui: la cybermenace et les tendances relatives aux cyberconflits, et la cyberdéfense canadienne.

La cybermenace peut être décrite comme étant un état de conflit et de tension perpétuel. Elle est le résultat d'une architecture de longue date qui, malgré les améliorations apportées au fil des années, est toujours bien présente. Elle peut entraîner des vulnérabilités et des exploits, qui sont le fondement des logiciels malveillants utilisés dans le cadre de cyberopérations que nous considérons à titre de cyberconflits ou de cyberguerres.

À l'heure actuelle, il faut garder en tête quelques grandes tendances.

Premièrement, aucune norme ou loi internationale n'est actuellement en place pour lutter contre les cyberconflits et les cyberguerres. Pour être clair, ce n'est pas la position du Canada et de nombreux alliés de l'OTAN. Actuellement, il n'y a aucun régime international ou consensus sur la façon d'aborder la loi internationale en matière de cyberconflits.

Deuxièmement, les rançongiciels ont complètement révolutionné la façon dont les États adverses et les acteurs non étatiques perçoivent le cyberespace. Par exemple, la Corée du Nord a très bien réussi à utiliser les cyberopérations, surtout les rançongiciels, pour trouver des façons d'éviter les sanctions internationales, mais il ne faut pas oublier la façon dont la Russie et bon nombre d'autres acteurs utilisent les rançongiciels dans le cadre de leurs cyberopérations, également.

Il y a la marchandisation des « jours zéro ». Il s'agit des vulnérabilités inconnues d'un système, d'un ordinateur ou d'une partie d'un logiciel. La marchandisation des jours zéro et des exploits a largement contribué à la prolifération des cybercapacités et aux cyberopérations. De façon particulière, la Chine exige que toute nouvelle vulnérabilité ou tout jour zéro soit déclaré au gouvernement dans un délai de deux jours. C'est la première loi en son genre, qui tend à aller à l'encontre des normes d'une industrie qui favorisent habituellement une protection maximale des utilisateurs.

Je m'en voudrais de ne pas évoquer l'invasion non provoquée de l'Ukraine par la Russie et le recours aux cyberopérations associées à des opérations militaires cinétiques interarmées quasi simultanées. Je veux faire écho aux commentaires entendus dans le cadre de la réunion précédente, mais je veux aussi vous faire part des opérations les plus nombreuses. Bien que l'attaque de ViaSat soit bien connue, il y a également eu au moins 16 maliciels de nettoyage déployés en Ukraine, qui ciblaient le pays. Ce sont des virus qui détruisent complètement les données et empêchent toute récupération. Il s'agit d'un nouveau type d'attaque, puisqu'elle ne représente pas une pratique criminelle habituelle. En règle générale, les criminels prennent les données en otage et demandent une rançon pour extorquer de l'argent à certaines personnes. Les maliciels de nettoyage ont pour seul objectif de détruire les données des systèmes. Il s'agit du plus important nombre de maliciels déployés au cours des 20 dernières années.

Je vais maintenant passer à la cyberdéfense canadienne et à ce que signifient ces tendances pour le Canada.

De façon particulière, le Canada a besoin d'une intervention pangouvernementale en matière de cybersécurité et d'une intervention très ciblée en matière de cyberdéfense. La cyberdéfense comprend le CST et les Forces armées canadiennes. Je vais me centrer sur les Forces armées canadiennes aujourd'hui.

Les Forces armées canadiennes ne sont aucunement préparées à une cyberguerre en cas de conflit. Je me demande même dans quelle mesure elles sont capables de coopérer et d'échanger avec les alliés, notamment avec les États-Unis.

● (0900)

Les raisons en ce sens sont nombreuses, mais je vais en aborder quelques-unes aujourd'hui.

La politique de cyberdéfense du Canada est à tout le moins incomplète et ponctuelle. Sa stratégie et sa définition ne s'harmonisent pas à celles des alliés du Canada, notamment les États-Unis. Je vais utiliser la définition d'une cyberopération de défense du CST en guise d'exemple, qui fait référence à une contre-attaque ou à une réponse à une menace active contre le Canada. Ce n'est habituellement pas la façon dont on parle des cyberopérations de défense ou la façon de les expliquer. En règle générale, elles ne visent pas une réponse active.

Bien qu'il ne s'agisse que d'un langage juridique, il devient difficile de parler avec les alliés d'un même sujet lorsqu'il est question de cyberopérations de défense, qui visent habituellement les propres réseaux des pays, de façon similaire à la cybersécurité. Lorsqu'il est question de manoeuvres offensives, il y a un grand écart entre la façon dont les penseurs canadiens et les alliés perçoivent et réalisent les cyberopérations.

Le président: Monsieur Rudolph, je vais devoir vous demander de terminer votre exposé dans le cadre de vos réponses à nos questions. Vous avez dépassé les cinq minutes qui vous étaient accordées. Je suis désolé, mais il en est ainsi.

Madame Gallant, vous disposez de six minutes.

Mme Cheryl Gallant: Merci.

Ma première question s'adresse à M. Keenan.

Est-ce qu'il devrait y avoir une discussion ouverte et un accord du Parlement sur les limites de l'utilisation de l'intelligence artificielle dans l'armée?

M. Thomas Keenan: Je crois que oui. Il existe une politique sur l'utilisation responsable de l'intelligence artificielle sur le site Web Canada.ca. Je l'ai lue et elle est correcte, mais elle date de 2021.

La première chose que je dirais, c'est qu'il faut une mise à jour continue. Ces politiques ne peuvent être figées. Oui, il faut absolument avoir une politique en place. J'ai consulté mes amis de l'industrie, surtout ceux qui travaillent pour Microsoft, parce que la société a investi des millions de dollars dans ChatGPT. On passe à l'intelligence artificielle éthique.

À mon avis, il faut le faire, en consultation avec l'industrie et les universitaires.

Mme Cheryl Gallant: Comment le Parlement peut-il atteindre un équilibre entre nous protéger contre le côté sombre et encourager les découvertes positives?

M. Thomas Keenan: C'est la grande question. Nous recevrions un prix Nobel si nous le savions.

Il faut assurer un suivi. Permettez-moi de vous donner un exemple.

Google est doté d'un moteur de recherche, comme nous le savons tous. Une personne a réussi, en utilisant Google, à trouver le nom d'un jeune délinquant en Ontario, alors que celui-ci était protégé par une interdiction de publication. Comme de nombreuses personnes avaient dit que Johnny Smith était un mauvais garçon, lorsqu'on effectuait une recherche avec son nom et le crime odieux qui avait été commis, Google faisait une association. Les représentants de Google ont fait valoir qu'aucun membre de leur équipe n'avait contrevenu à l'interdiction de publication... mais l'algorithme de Google, oui.

Ce que je veux souligner avec cette histoire, c'est qu'il faut toujours surveiller. Il faut être à l'affût d'exemples de ce genre. C'est arrivé il y a plusieurs années. Je ne sais pas si Google a pris des mesures pour se protéger — vous pourriez demander à leurs représentants — lorsque la société contrevient à une interdiction de publication ordonnée par un juge.

Il faut assurer une vigilance continue.

● (0905)

Mme Cheryl Gallant: Monsieur Rudolph, comment la Russie utilise-t-elle les maliciels ou les rançongiciels dans le cadre des opérations cinétiques, par opposition à du simple chantage dans le but d'obtenir de l'argent?

M. Alexander Rudolph: Je vais vous donner l'exemple d'une invasion récente. La Russie a déployé ce qui s'apparente à un rançongiciel capable de chiffrer un système. Ainsi, le système était bloqué et les données étaient chiffrées. On demandait ensuite de l'argent. En fait, la Russie déployait en arrière-plan un maliciel de nettoyage pour détruire toutes les données.

C'est toujours du cas par cas. La Russie, de façon particulière, utilise ces tactiques pour cibler des systèmes et des organisations précis dans le cadre de ses invasions, alors que par le passé, elles étaient utilisées avec les services de renseignement de diverses façons afin extorquer de l'argent.

Mme Cheryl Gallant: À quel moment une entreprise du secteur privé doit-elle communiquer avec le gouvernement? Quand devrait-on aviser l'armée qu'elle doit accroître ses mesures de cybersécurité parce qu'une attaque est en cours, et tenir compte de la possibilité que ce ne soit que le début d'une escalade vers une interaction cinétique?

M. Alexander Rudolph: Il est toujours assez difficile de savoir si une attaque donnera lieu à une intervention cinétique, puisque les cyberopérations peuvent donner lieu à une escalade. C'est souvent dans la façon dont elles sont associées à d'autres efforts. Une cyberopération en soi n'entraînera pas nécessairement de dommages cinétiques, mais la façon dont les États répondent à cette opération ou l'utilisent en association avec des opérations cinétiques est très préoccupante. C'est ce qu'a tenté de faire la Russie en Ukraine.

Mme Cheryl Gallant: Un nouveau projet de loi sur la cybersécurité a été proposé, mais il vise plus les civils. Est-ce qu'on devrait rédiger un autre projet de loi qui répondrait de manière précise à vos préoccupations relatives à l'armée? Est-ce qu'il devrait s'harmoniser au projet de loi sur la cybersécurité civile? À quel point une attaque civile interagit-elle avec les infrastructures militaires? Comment est-ce possible? Est-ce que c'est déjà arrivé?

M. Alexander Rudolph: Je ne peux pas vous dire si c'est arrivé au Canada ou non. Il faudrait demander à l'armée s'il y a eu des attaques contre les infrastructures militaires. C'est souvent difficile à déterminer. Une grande partie des infrastructures essentielles est à double usage. Si l'attaque vise les infrastructures militaires de manière explicite, je dirais qu'il s'agit d'une attaque contre l'armée. À mon avis, il faut un autre projet de loi pour aborder la cyberdéfense des forces armées et du CST. Il faut surtout une structure officielle de force et de commandement qui organise le CST et l'armée, ce qui n'existe pas à l'heure actuelle. Tout est fait de façon ponctuelle.

Mme Cheryl Gallant: Merci, monsieur Rudolph.

Le président: Merci, madame Gallant.

Monsieur Fisher, vous disposez de six minutes. Allez-y.

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

Je vous remercie, messieurs, pour votre présence.

Lorsque le système de Rogers est tombé en panne, j'étais au Cap-Breton, en Nouvelle-Écosse, pour des réunions de travail. Toutes nos infrastructures essentielles sont tombées. On ne pouvait pas faire le plein d'essence; on ne pouvait pas utiliser les guichets automatiques. Rien ne fonctionnait. Je pense aussi à la tempête Fiona, qui a frappé le Canada atlantique. Nous ne recevons plus, depuis longtemps, le journal à la maison. On n'avait pas accès aux nouvelles. On ne pouvait pas payer nos factures. On ne pouvait rien faire lorsque les infrastructures essentielles ont été touchées par Fiona.

Je vous donne ces exemples pour souligner notre dépendance aux infrastructures essentielles et aussi leur importance pour les membres de notre communauté, les habitants du pays et les gens de partout dans le monde.

Monsieur Rudolph, j'aimerais vous entendre en premier.

Comment le gouvernement fédéral, les provinces et les territoires peuvent-ils mieux protéger et défendre ces infrastructures qui sont essentielles à la vie des Canadiens?

M. Alexander Rudolph: C'est une grande question. Je dirais tout d'abord qu'il faut mieux financer le Centre canadien pour la cybersécurité, et assurer une meilleure communication entre le Centre et le reste du gouvernement. Il faut aussi que le gouvernement tienne compte de la différence entre les besoins des provinces et ceux du fédéral en vue de l'offre des services et de la protection contre les menaces.

L'intervention holistique en matière de cybersécurité dont j'ai parlé plus tôt permettrait de tenir compte des besoins en matière d'infrastructures essentielles, mais les Forces armées canadiennes dépendent encore largement de nombreux systèmes publics, notamment parce que leurs systèmes internes sont insuffisants. Il faut un meilleur financement et il faut aborder la façon d'intervenir en cas d'incidents importants de ce genre. Il faut également déterminer le rôle du Centre canadien pour la cybersécurité à cet égard, de façon similaire à ce qui est fait avec l'Agence de cybersécurité et de sécurité des infrastructures aux États-Unis.

● (0910)

M. Darren Fisher: Lorsqu'on pense aux nouvelles technologies, aux mesures que peuvent adopter les Canadiens à grande échelle, comme dans le cas des téléphones cellulaires ou autres, quelles tendances représentent le plus grand risque en matière de cybersécurité? Quelles initiatives le gouvernement fédéral pourrait-il prendre pour atténuer ces risques associés aux téléphones intelligents et aux autres technologies du genre?

M. Alexander Rudolph: Je dirais que l'utilisation des rançongiciels touche les cellulaires tout autant que nos ordinateurs ordinaires, en raison principalement de la prolifération des logiciels de surveillance, dont beaucoup d'entre vous ont sans doute entendu parler, comme Pegasus ou Groupe NSO. La grande prolifération de ces logiciels malveillants ou menaces du jour zéro fait de tout outil technologique une cible pour réaliser potentiellement des profits ou cibler des États ennemis.

Cela fait partie de la tension perpétuelle dont j'ai parlé, et le gouvernement a notamment la responsabilité de faire face à ces menaces et de prendre des mesures contre les criminels en travaillant avec ses alliés pour cibler et arrêter certains des acteurs ayant recours aux rançongiciels qui ont été mentionnés hier, si je me souviens bien, où le jour précédent.

Je dirais que le Canada est actuellement un joueur de niveau inférieur dans ce domaine. Il aide... Le Centre de la sécurité des télécommunications, le CST, a bonne réputation dans le monde, mais... Les Forces armées canadiennes, les FAC, pourraient en faire plus, mais elles ne le peuvent pas. On pourrait examiner l'apport réel de beaucoup d'autres initiatives gouvernementales à la cybersécurité des ministères ou des citoyens.

M. Darren Fisher: Monsieur Keenan, aimeriez-vous nous donner votre point de vue?

M. Thomas Keenan: Vous me demandez mon avis?

M. Darren Fisher: Oui, monsieur.

M. Thomas Keenan: Excellent. J'aimerais parler tout d'abord de ce que j'ai baptisé « les rançongiciels de l'enfer ». C'est un scénario que j'ai inventé, et je pense qu'il faut en parler ici.

Disons que vous êtes un directeur d'hôpital et que vous venez de recevoir un courriel d'un inconnu qui dit qu'un de vos employés vient de cliquer sur le courriel d'hameçonnage d'un prince saoudien et qu'il a pénétré dans votre système, mais qu'il ne va pas exiger une rançon ou effacer vos données. Il a une bien meilleure idée. Il a parcouru votre réseau et il sait que vous possédez 75 appareils de radiographie Picker, 4 appareils d'imagerie par résonnance magnétique, ou IRM, Siemens et 2 000 pompes à perfusion BD, et qu'ils ont tous des vulnérabilités.

De nombreux appareils technologiques ont des vulnérabilités du jour zéro dont les fabricants ne sont pas au courant.

Il dit qu'ils étaient à vendre sur le Web clandestin. Il les a achetés et il doit maintenant récupérer son argent, alors vous avez jusqu'à demain pour lui verser 10 millions de dollars en bitcoins, et si vous ne le faites pas, il ne va pas chiffrer vos données — parce que c'est tellement dépassé —, mais plutôt tuer un patient par jour.

J'ai lu un article paru en Israël intitulé « Sept façons de tuer un patient avec un appareil de radiographie Picker », qui vont de le frapper avec l'appareil à le bombarder de radiation.

En fait, j'ai soumis le problème à un groupe de directeurs d'hôpital aux États-Unis, et ils m'ont dit soit qu'ils paieraient la rançon, soit qu'ils n'en tiendraient pas compte. Je leur ai répondu que, dans le premier cas, le type serait de retour le lendemain en demandant 20 millions de dollars, et dans le deuxième, qu'un article titrant « Décès d'une grand-mère dans un hôpital qui a refusé de verser une rançon » serait à la une du *New York Times* .

Ils ont mentionné aussi qu'ils tenteraient l'isolement — et c'est ici qu'on entre dans les détails techniques — en séparant tous les systèmes dans l'hôpital pour que cela ne puisse pas se produire. Mes collègues en médecine m'ont dit que c'était irréaliste, car le médecin, l'ordinateur du laboratoire et l'appareil IRM peropératoire doivent être reliés à l'appareil de radiographie Picker pour avoir accès aux résultats. Je veux donc en venir au fait qu'il s'agit d'un réseau très interrelié.

J'ai présenté ce scénario à tous les gens intelligents que je connais, et la réponse est qu'il n'y a pas de réponse.

● (0915)

Le président: Je vous remercie, monsieur Fisher.

Il n'y a pas de réponse.

[*Français*]

Monsieur Garon, je vous souhaite la bienvenue au Comité. Vous disposez de six minutes de temps de parole.

M. Jean-Denis Garon (Mirabel, BQ): Merci, monsieur le président.

Je vous remercie d'être parmi nous, monsieur Rudolph.

J'ai une question à vous poser.

On a appris récemment que le gouvernement fédéral faisait affaire de façon substantielle avec des firmes privées. On a beaucoup parlé de McKinsey, et il y en a d'autres. Des ministères aux activités extrêmement sensibles font affaire avec ces firmes, dont le ministère de la Défense nationale et le ministère de l'Immigration et de la Citoyenneté. On a appris que certaines de ces firmes, dont McKinsey, avaient traité de façon substantielle avec des sociétés contrôlées par le régime chinois.

Pensez-vous qu'on devrait porter une attention particulière à cette question et qu'on devrait faire très attention aux firmes avec lesquelles on fait affaire au Canada? Est-ce tout à fait normal que le ministère de la Défense nationale passe des contrats très importants avec des firmes qui traitent avec le gouvernement chinois?

[*Traduction*]

M. Alexander Rudolph: Je conviens qu'il s'agit d'un risque grave, en particulier avec... Je ne me souviens pas du nom de l'entreprise de communication qui a été suspendue récemment en raison de ses liens avec des firmes chinoises.

Je dirais que c'est un problème constant, permanent. Nous avons vu des preuves que la Chine peut corrompre activement des chaînes d'approvisionnement pour tenter d'y implanter des dispositifs de surveillance. Je crois que l'exemple le plus récent est celui d'un parc de voitures presque en entier au Royaume-Uni qui a été parasité de cette façon.

Dans le cas de certaines autres firmes... Je veux faire la distinction entre, disons, les grandes firmes de consultation et les firmes qui se trouvent à la fin de la chaîne d'approvisionnement, car les risques sont complètement différents. En cyberdéfense et en cybersécurité, McKinsey et les autres grandes firmes de consultation sont, vraiment, les grands noms dans l'industrie et accaparent le marché. Elles sont vraiment incontournables.

Quand on prend en compte la forte inflation et la forte concurrence pour embaucher des gens compétents, on peut difficilement rivaliser avec elles.

[*Français*]

M. Jean-Denis Garon: Si vous me le permettez, monsieur Rudolph, je vais poursuivre.

Il y a le Groupe des cinq, entre autres. Puisque vous dites que certaines de ces firmes sont incontournables, ne pensez-vous pas qu'il soit préférable que le Canada ou le gouvernement fédéral ait un régime de sélection et de transparence beaucoup plus efficace? Ainsi, lorsque les Québécois et les Canadiens verront le gouvernement fédéral faire affaire avec ces organisations, ils pourront au moins avoir une idée de l'information qui a été disséminée ou de l'information à laquelle ces organisations ont eu accès. On sait que la Chine se prive de très peu de moyens pour faire de l'espionnage, de la cyberguerre, et ainsi de suite, et que ces firmes font aussi affaire avec la Chine.

Pensez-vous qu'on a un pas à faire vers la transparence pour que les Québécois et les Canadiens soient moins inquiets, que ces peurs soient rationnelles ou non?

[*Traduction*]

M. Alexander Rudolph: Je suis tout à fait d'accord pour dire qu'il faut plus de transparence, de façon générale, sur la politique de cyberdéfense canadienne. J'effectue principalement mes recherches en examinant les rapports de vérification et les résultats ministériels, et je suis surpris de voir que les gens sont surpris de mes connaissances sur les Forces armées canadiennes.

Je connais les grands thèmes, mais mes connaissances comportent beaucoup de lacunes, et c'est tout simplement parce que les Forces armées canadiennes ne disent pas tout et qu'on les empêche de le faire. C'est donc un problème de politique.

J'insiste sur le fait qu'il y a une différence entre la transparence et le fait d'accroître les exigences pour le Groupe des cinq ou pour ces firmes, car il y en a déjà pas mal.

[*Français*]

M. Jean-Denis Garon: Vous avez dit quelque chose d'intéressant. Vous avez mentionné que le manque de transparence, notamment au sein du ministère de la Défense nationale, est à ce point endémique qu'il peut empêcher les chercheurs canadiens de faire de la recherche sur le sujet.

Est-ce bien ce que vous m'avez dit?

[*Traduction*]

M. Alexander Rudolph: Je suis d'accord. Le problème est endémique partout dans le système.

L'Office de surveillance des activités en matière de sécurité nationale et de renseignement a constaté récemment que les Forces armées canadiennes ont 180 bases de données indépendantes, ce qui veut dire que pour avoir accès à une bonne partie des données, il faut une gestion du personnel, et non une gestion de l'information.

● (0920)

[*Français*]

M. Jean-Denis Garon: En terminant, j'ai une question qui s'adresse au professeur Keenan.

On sait que les médias sociaux jouent un très grand rôle dans la surveillance et l'intelligence artificielle. Beaucoup de Canadiens et de Québécois donnent leurs informations, ce qui nourrit les algorithmes. Ils donnent leurs informations sans savoir à quoi ils ont affaire. Il existe évidemment un capitalisme de surveillance, et on sait que ces images, ces photos qui nourrissent les algorithmes font partie du problème.

Le gouvernement du Canada déploie-t-il assez d'efforts pour soutenir les Canadiens dans la protection de leurs renseignements? Quels outils sont à la disposition du gouvernement du Canada pour améliorer la protection de notre identité numérique? On sait qu'une fois qu'on l'a perdue, il est très difficile de la retrouver.

[*Traduction*]

Le président: M. Garon ne vous a laissé que 20 secondes, malheureusement, pour répondre à cette excellente question, alors soyez bref, s'il vous plaît.

M. Thomas Keenan: Je vous remercie d'avoir mentionné les idées de Shoshana Zuboff sur le capitalisme de surveillance. Mon fils mène des recherches sur la cybersécurité, et il a travaillé avec elle sur son livre.

Il ne fait aucun doute que nous donnons trop d'information sur les médias sociaux. Sur le site *The Onion*, un site satirique, on trouve une excellente vidéo dans laquelle Mark Zuckerberg se voit décerner le titre d'agent de la CIA de l'année pour avoir réussi à obtenir des gens autant de renseignements personnels, sur leurs déplacements, les spectacles auxquels ils vont assister, etc. Si la CIA veut les arrêter, elle n'a qu'à consulter leur emploi du temps.

Il faut plus de sensibilisation, absolument. Le fait est que les gens adorent publier de l'information. Ce n'est pas nécessairement une bonne chose. Il faut, à tout le moins, qu'ils vérifient qui a accès à l'information qu'ils publient. S'agit-il de leurs amis, des amis de leurs amis, ou du monde entier?

Le président: Je vous remercie, monsieur Garon.

Monsieur Boulerice, je vous souhaite la bienvenue au Comité. Vous avez six minutes. Allez-y, s'il vous plaît.

[*Français*]

M. Alexandre Boulerice (Rosemont—La Petite-Patrie, NPD): Merci beaucoup, monsieur le président.

Cela me fait plaisir d'être avec vous ce matin.

Monsieur Keenan, j'ai beaucoup aimé que vous rappeliez le fait que les systèmes d'intelligence artificielle pouvaient être nourris par des idées préconçues, des préjugés, que les concepteurs peuvent installer dans le système d'apprentissage. Vous avez aussi parlé de la capacité d'empoisonner la base de données en changeant la conversation.

Est-ce que je me trompe en disant qu'on pourrait utiliser l'intelligence artificielle pour créer des faux comptes sur les médias sociaux qui vont changer la conversation et qui, par la suite, vont contaminer d'autres systèmes d'intelligence artificielle, qui se servaient de cette base de données dans leur apprentissage? Ce serait donc une guerre d'intelligence artificielle qui viendrait pourrir d'autres systèmes d'intelligence artificielle. Cela commence à être un peu compliqué.

[*Traduction*]

M. Thomas Keenan: J'aimerais mentionner que j'ai une excellente étudiante diplômée, Anika Kale, qui étudie les programmes d'études sur l'intelligence artificielle partout dans le monde, plus spécialement du point de vue du genre. Elle constate que la sensibilisation au genre y est presque absente.

Vous avez tout à fait raison. Une source peut en polluer une autre et il n'y a vraiment aucun contrôle à ce sujet. Ce qu'il faut savoir, c'est que l'intelligence artificielle en général ne s'explique pas. Elle donne une réponse. Mon gros problème avec ChatGPT, c'est que la réponse semble très documentée, alors qu'elle sort de nulle part. Un jour, je lui ai demandé de m'écrire un poème et il a inscrit un avertissement au bas que j'ai trouvé fort intéressant. Il disait qu'il s'agissait d'un travail de création et que cela ne contenait pas vraiment de faits.

Vous avez tout à fait raison. Une source de données peut en empoisonner une autre. Je suis certain que des agences de renseignement partout dans le monde s'activent actuellement à trouver des façons d'empoisonner nos bases de données de sources ouvertes.

[*Français*]

M. Alexandre Boulerice: Est-ce qu'une utilisation malveillante de l'intelligence artificielle, notamment sur les médias sociaux, représente un danger potentiel pour la qualité de notre vie démocratique et la montée de l'extrémisme et du populisme?

[*Traduction*]

M. Thomas Keenan: Il ne fait aucun doute que c'est ce qui s'est passé lors des campagnes présidentielles aux États-Unis et lors d'autres campagnes. Des robots malveillants sont créés dans le but explicite de mettre les gens en colère. On le fait parfois des deux côtés, la gauche et la droite, parce qu'on veut semer la discorde aux États-Unis. Vous pouvez sans doute imaginer quels pays s'y adonnent.

Je veux parler des technologies — parce qu'on en a parlé précédemment — et de l'endroit où se trouvent les risques. L'armée américaine a fait l'essai d'un projet de votes électroniques pour que les soldats stationnés à l'étranger puissent voter. On m'a demandé mon avis sur la sécurité du système. C'était bien fait. Les soldats devaient faire une vidéo d'eux pour prouver leur identité. Toutefois, certains d'entre eux avaient des cellulaires fabriqués par Huawei, Xiaomi, Meizu. Dans ce cas, c'était l'élément final, le cellulaire, qui pouvait être vulnérable. C'est la théorie du maillon faible. Le système de votes électroniques aurait donc pu être corrompu de cette façon.

● (0925)

[*Français*]

M. Alexandre Boulerice: C'est très intéressant. Je vous remercie beaucoup, monsieur Keenan.

Monsieur Rudolph, ma question porte sur les cyberattaques contre les infrastructures.

Dans les années 1970, j'étais tout petit, mais je me rappelle que les touristes ne pouvaient pas prendre de photos des centrales ou des barrages électriques, parce que c'était considéré comme des infrastructures essentielles et on ne voulait pas que l'information se propage.

Évidemment, en 2023, on n'en est plus là. Aujourd'hui, quand on parle de cyberattaque contre les infrastructures essentielles du Canada, de quoi parle-t-on exactement?

[*Traduction*]

M. Alexander Rudolph: Je vais prendre tout d'abord votre exemple de l'interdiction de prendre des photos pour des questions de sécurité. Nous devons composer maintenant avec la vaste prolifération du renseignement de sources ouvertes. On peut utiliser Google Maps pour obtenir les mêmes renseignements et analyses qui étaient illégaux 20 ans plus tôt. On peut aussi se servir de ce genre de renseignement de sources ouvertes pour mener des attaques contre des infrastructures essentielles. Ce sont souvent les gens qui sont la vulnérabilité dans un système.

Toutes les organisations ont des professionnels pour surveiller cela et s'occuper de la cybersécurité. On cherche le maillon faible dans un système. Il peut s'agir d'un détail. Si quelqu'un réussit à pénétrer dans le système, il tentera de le verrouiller pour s'en servir à ses fins. S'il s'agit d'un État, il va attendre qu'un conflit éclate pour s'en servir. S'il s'agit d'un criminel, il va habituellement verrouiller le système pour en empêcher l'utilisation, comme lors de l'attaque contre Colonial Pipeline, et exiger une rançon. S'il ne l'obtient pas, il publiera les données en ligne, même si elles sont secrètes ou de nature délicate.

Le président: Je vous remercie, monsieur Boulerice.

Chers collègues, il nous reste un peu plus de 15 minutes, et la deuxième série de questions en prendrait 25. Le compte n'y est pas, alors je vais retrancher une minute à chaque intervenant. Nous commençons par Mme Kramp-Neuman.

Mme Shelby Kramp-Neuman: Je vous remercie.

Monsieur Keenan et monsieur Alex Rudolph, je vous remercie de vos témoignages aujourd'hui.

Monsieur Rudolph, vous avez dit que nous n'étions absolument pas préparés à une cyberguerre, et je trouve cela très inquiétant.

Je vais commencer par parler d'un article de 2021 de l'Institut canadien des affaires mondiales dans lequel vous avez souligné l'importance et la nécessité pour les FAC d'avoir une force de cybersécurité performante. Vous avez mentionné que, si elles ne peuvent pas répondre à leurs besoins en cybersécurité, elles pourraient devoir s'en remettre au CST.

En avril de la même année, les FAC ont publié un rapport intitulé « Évaluation des cyberforces », dans lequel on parlait de plusieurs problèmes de recrutement et de rétention.

Si ce sont des civils qui s'acquittent de rôles qui autrement seraient dévolus à des membres des forces armées, quelles sortes de problèmes cela pourrait-il entraîner?

M. Alexander Rudolph: Comme sa représentante l'a confirmé mardi dernier, le CST peut prêter main-forte aux FAC pour s'occuper des enjeux liés à la cybersécurité et à la cyberdéfense. Lorsque cela se produit, le CST prend en charge des mandats des FAC, ce qui veut dire que s'il était amené à participer à un conflit, en particulier une guerre, les civils du CST qui aident les FAC seraient considérés comme des combattants dans cette guerre.

Il faut comprendre dans quelle mesure cela s'étend au reste de l'organisation à ce moment et en tenir compte.

● (0930)

Mme Shelby Kramp-Neuman: Monsieur Rudolph, de quelle manière l'ordre de reconstitution des FAC qui est en vigueur touche-t-il le développement des cyberforces?

M. Alexander Rudolph: Je ne peux pas vraiment vous en parler, car j'ai très peu d'information à ce sujet.

Je peux dire que si les FAC ont de la difficulté à garder les gens compétents, c'est principalement, et simplement, parce qu'elles ne disposent pas des infrastructures et des moyens pour faire le travail. Les obstacles bureaucratiques sont nombreux et l'approvisionnent est lent. Les gens se joignent aux forces pour faire ce genre de travail, mais ils ne veulent pas se contenter d'aller installer des radios.

Mme Shelby Kramp-Neuman: Je vous remercie.

Pour revenir à l'article initial dont j'ai parlé, vous avez mentionné que selon de récentes informations, « le CST et le ministère de la Défense/les FAC sont aux [mêmes] étapes de planification en vue d'un type d'organisation similaire, mais qu'on en sait encore peu sur l'échéancier de sa création. »

Pouvez-vous nous parler du manque d'information sur l'initiative et des répercussions graves que cela présente pour les employés civils du CST? Pourriez-vous nous en dire un peu plus à ce sujet?

M. Alexander Rudolph: C'est un plan, et c'est tout ce que je peux vous dire. C'est vraiment tout ce que je sais à ce sujet.

D'après ce que des responsables m'ont dit, il semble que la relation actuelle soit plutôt ponctuelle. Ils ont probablement des employés du CST intégrés au sein des FAC ou vice versa. Je n'ai pas beaucoup d'information à ce sujet, car il n'y en a pas vraiment dans les sources ouvertes.

Mme Shelby Kramp-Neuman: Pour ce qui est de l'urgence de régler le problème des services numériques vieillissants et défaillants, pourquoi, d'après vous, le gouvernement est-il lent à réagir?

M. Alexander Rudolph: C'est un problème qui date et qui...

Parlez-vous seulement des FAC ou de l'ensemble du gouvernement?

Mme Shelby Kramp-Neuman: Je parle plus précisément des FAC.

M. Alexander Rudolph: C'est en partie dû au processus ponctuel dont j'ai parlé. La mise sur pied de Services partagés Canada a essentiellement vidé les forces armées de leurs cybertalents, notamment en cybersécurité. La centralisation était une bonne idée, mais on a oublié l'importance fondamentale de la défense nationale et des capacités numériques nécessaires à cet égard.

On a...

Le président: Nous allons devoir en rester là, malheureusement. Je m'excuse encore, et même si ce n'est pas sincère, je le fais quand même.

Madame Lambropoulos, vous avez quatre minutes. Allez-y, s'il vous plaît.

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

Je veux commencer par remercier M. Rudolph et M. Keenan d'être avec nous pour répondre à nos questions, et les remercier de leur témoignage intéressant.

Je vais commencer par M. Rudolph.

Vous avez dit qu'il n'existait pas de moyens précis actuellement pour lutter contre les cyberconflits. Comme on pourrait procéder à un examen législatif de la Loi sur la sécurité nationale en 2023, croyez-vous que l'on devrait envisager d'y apporter des changements?

Comment pouvons-nous procéder pour renforcer la loi ou en créer une? Que devrions-nous inclure, afin de pouvoir préparer le Canada à faire face à des cybermenaces ou à une cyberguerre?

M. Alexander Rudolph: Je vous remercie de la question.

Je dirais que la grande priorité pour le Canada est de faire connaître sa position à propos d'un engagement continu. La stratégie des États-Unis consiste à lutter constamment contre les éléments ennemis dans le cyberespace. On entend dire que le Cyber Command ou la National Security Agency aux États-Unis procède à des attaques offensives pour cibler ou arrêter les utilisateurs de rançongiciels, et c'est le genre d'action qui témoigne d'un engagement continu.

Le Canada a donné quelques exemples du soutien qu'il apporte, mais ce n'est pas très clair, et le soutien offert n'est pas cohérent.

Mme Emmanuella Lambropoulos: D'accord, il s'agit donc d'être plus clair et plus cohérent dans notre façon de réagir à ces menaces.

Monsieur Keenan, vous dites que nous sommes très vulnérables en raison de notre dépendance à la technologie. Il n'y a pas grand-chose que nous puissions faire à cet égard. Pour revenir à la Loi sur la sécurité nationale et à son examen, j'aimerais savoir si vous avez des suggestions à faire. Y a-t-il des changements à apporter?

M. Thomas Keenan: On pourrait parler explicitement de ce qu'on appelle le « hack back », la contre-attaque, ou les mesures actives.

J'ai interrogé les Forces armées canadiennes à ce sujet, et on m'a renvoyé au document « Protection, sécurité, engagement ». M. Rudolph en sait sans doute plus à ce sujet. On dit à un endroit qu'avec le bon niveau d'autorisation, on peut contre-attaquer. Le fait est que nous allons devoir contre-attaquer. On ne peut plus vraiment faire autrement.

Naturellement, cela devient alors une question de définition. On m'a dit à un certain moment que le gouvernement des États-Unis examinait des installations en Russie qui pourraient être victimes d'une attaque. Nous savons que le gouvernement américain a inséré un virus dans des imprimantes destinées à l'Irak, etc. Cela se passe actuellement.

Je ne pense pas que nous ayons une politique claire à ce sujet, et je pense que nous avons un besoin de savoir. Je suis conscient que, pour des raisons de sécurité, on ne veut pas communiquer le moment où cela se passe, mais il me semble, à partir de ce que j'ai pu récolter d'information comme civil, qu'on ne sache pas clairement quand des mesures actives peuvent être prises.

● (0935)

Mme Emmanuella Lambropoulos: Très bien, merci.

Monsieur Rudolph, ma prochaine question est à nouveau pour vous.

Je ne sais pas si vous pourriez nous éclairer davantage sur la distinction entre cybersécurité et cyberguerre. À partir de quel moment se retrouve-t-on en cyberguerre? Quels sont les chevauchements entre les deux?

Le président: Vous avez environ 10 secondes pour répondre à cette question.

M. Alexander Rudolph: Je vais donc essayer d'être bref, ce qui n'est pas chose facile pour un universitaire.

La cybersécurité s'inscrit en grande partie dans une perspective générique, alors que la cyberdéfense et la cyberguerre sont très ciblées sur les différentes menaces et font intervenir dans la plupart des cas des États, plutôt que des acteurs non étatiques. Dans le domaine de la cybersécurité, on doit composer autant avec des criminels de faible envergure qu'avec les États eux-mêmes, pendant que la cyberdéfense est une activité plus ciblée, à l'instar de la défense nationale

[*Français*]

Le président: Monsieur Garon, vous disposez d'une minute.

M. Jean-Denis Garon: Professeur Keenan, il a été question d'infrastructures critiques. J'ai en tête les grilles électriques et les hôpitaux, notamment, ce qui est évidemment de la compétence des provinces.

Je me demande si, au Canada, les provinces et le Québec sont suffisamment inclus dans les discussions et les protocoles qui viseraient éventuellement à protéger nos infrastructures critiques.

Si ce n'est pas le cas, que devrait-on faire précisément?

[*Traduction*]

M. Thomas Keenan: Nous devons travailler en consultation avec les provinces ainsi qu'avec le secteur privé. Un grand nombre de ces éléments relèvent en effet de la responsabilité d'entreprises privées. Je sais qu'il y a des rencontres à ce sujet et qu'il y a collaboration entre les parties.

Je ne veux pas ressortir l'exemple du ballon, mais le fait est que certains s'inquiètent des risques qu'un tel engin puisse cacher par exemple une arme à impulsion électromagnétique. Il est possible que quelqu'un en vienne à lancer une attaque de haut niveau contre nos infrastructures essentielles. Il faudrait alors que tous mettent la main à la pâte.

Je conviens que l'on devrait tenir de plus vastes consultations et élaborer des plans d'urgence. Il ne fait aucun doute que nous ne tiendrions pas le coup très longtemps sans électricité.

[*Français*]

Le président: Monsieur Boulerice, vous disposez d'une minute.

M. Alexandre Boulerice: Oh, j'ai une minute!

Ma question s'adresse à M. Rudolph.

Vos propos sur notre incapacité à faire face à des cyberattaques sont assez inquiétants. Nous sommes très dépendants des firmes d'experts-conseils du secteur privé, des grandes compagnies de télécommunication et des géants du Web, qui ont beaucoup de contrôle sur nos vies et sur nos renseignements personnels.

Notre incapacité, à l'échelle publique, et notre dépendance envers toutes ces compagnies privées ne vous inquiètent-elles pas un peu?

[*Traduction*]

M. Alexander Rudolph: Je ne suis pas inquiet du tout. J'estime que les professionnels de la cybersécurité jouent un rôle tout aussi important que les membres des forces militaires et policières. Il va de soi que l'on peut, à certains égards, considérer que leur travail n'est pas sans risque, mais ces spécialistes sont essentiels au bon fonctionnement de notre société. Il serait faux de dire que cela ne nous expose pas à certains risques, mais il s'agit de risques que nous devons prendre en compte, au même titre que dans nos relations avec n'importe quelle autre organisation.

Le président: Merci, monsieur Boulerice.

Monsieur Kelly, vous avez quatre minutes.

M. Pat Kelly (Calgary Rocky Ridge, PCC): Je vais vous ramener un instant, monsieur Rudolph, à vos observations préliminaires alors que vous nous disiez que les Forces armées canadiennes ne sont aucunement préparées à livrer une cyberguerre. Comme vous avez manqué de temps pour vos explications à ce sujet, je voudrais vous permettre maintenant, compte tenu de l'importance de ces précisions pour le Comité et le rapport que nous allons produire, de nous faire part de vos différentes recommandations aux fins d'une préparation adéquate de nos forces armées dans ce contexte.

Nous vous écoutons.

M. Alexander Rudolph: Je vous remercie de me permettre de le faire.

J'ai heureusement pu traiter de bon nombre de ces éléments en répondant aux questions du Comité.

Je n'ai cependant pas beaucoup parlé du manque général de cyberinfrastructures au sein de nos forces. Cette situation est en partie attribuable à la lenteur de notre processus d'approvisionnement, comme vous êtes nombreux à le savoir pertinemment, mais aussi à notre difficulté à bien saisir et intégrer les défis particuliers qui distinguent le cyberespace du secteur traditionnel de la défense.

Je dois vous dire d'entrée de jeu que je suis loin d'être un expert de l'approvisionnement en matière de défense. Je peux toutefois vous confirmer que les politiques en vigueur dans ce domaine ne permettent pas, dans bien des cas, de tenir compte des investissements en cybersécurité et en cyberdéfense consentis par de grandes firmes susceptibles de devenir des entrepreneurs principaux. En outre, la lenteur du processus est encore plus pénalisante pour les PME du secteur de la cybersécurité, car elles ne peuvent pas se permettre d'attendre 12 ou 16 mois pour une invitation à se qualifier alors qu'elles ont du financement pour peut-être une année, dans le meilleur des cas, surtout lorsqu'il est question d'intelligence artificielle et de bon nombre de ces capacités offensives de pointe. Ces PME ont besoin de tout le soutien qu'elles peuvent obtenir. Lorsque leur seul client potentiel est le gouvernement et que les choses se passent aussi lentement, elles ne vont pas nécessairement faire des affaires avec le Canada

● (0940)

M. Pat Kelly: Pourrait-on dire que les processus d'approvisionnement de Services publics et Approvisionnement Canada ou du gouvernement sont trop lourds pour les PME? S'il y a trop de complications administratives, elles ne vont même pas se lancer dans l'aventure, n'est-ce pas?

M. Alexander Rudolph: Je ne dirais pas que c'est le cas pour toutes ces entreprises, mais c'est sûrement ce qui arrive pour celles du secteur de la cybernétique.

M. Pat Kelly: Je vais maintenant vous laisser une minute pour nous parler du CST, étant donné que vous avez indiqué que ni les Forces armées canadiennes ni le CST… Vous n'avez pas eu beaucoup de temps pour nous entretenir de la situation du CST, alors dites-nous quelles dispositions ce centre devrait prendre pour être prêt à agir.

M. Alexander Rudolph: Je dirais que le CST est l'organisation la mieux préparée, car ses efforts de planification sont en grande partie efficaces et ses rapports ouverts sont souvent de grande qualité. La difficulté vient surtout du fait que les liens entre le CST et les FAC sont pour ainsi dire inexistants. D'après ce que j'ai pu apprendre, tout se passe de façon très informelle.

Il faut qu'une structure de commande officielle soit en place pour assurer la médiation en cas de conflit. Dans l'état actuel des choses, ce serait sans doute le CST qui serait appelé à intervenir si une cybermenace se concrétisait. Je crois que les liens entre le CST et Affaires mondiales Canada sont plus structurés que ceux qui unissent les Forces armées canadiennes et le CST.

Le président: Merci, monsieur Kelly.

Madame O'Connell, vous avez quatre minutes.

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

Je vais poursuivre un peu dans le même sens en revenant à certaines réponses données par M. Rudolph.

Je veux seulement une précision. Vous avez parlé de transparence, et je ne sais pas trop s'il était question de transparence à l'égard des politiques ou plutôt concernant les détails de ces relations. Vous avez noté que toutes ces bases de données sont séparées. Parlez-vous des politiques régissant ces mécanismes ou des considérations détaillées liées à tout cela?

M. Alexander Rudolph: Je dirais que c'est un peu des deux. Lorsque je parlais de politiques ponctuelles, c'était notamment en référence à ces nouvelles politiques que l'on adopte chaque année en constatant que celles de l'année précédente ne produisent pas les résultats voulus. On manque vraiment de cohérence et de logique au fil des ans.

Mme Jennifer O'Connell: Je peux voir où vous voulez en venir d'un point de vue théorique, mais je pense qu'il faut également reconnaître que le principe du besoin de savoir doit s'appliquer lorsqu'il est question de sécurité nationale et assurément de cybermenaces. Pour garantir la transparence des politiques, je peux tout à fait comprendre la nécessité de rendre l'information accessible en source ouverte, mais pour ce qui est des détails ou des renseignements plus précis, je conçois également qu'il faut disposer de plusieurs bases de données, car ce n'est pas tout le monde qui a une autorisation de sécurité fondée sur son besoin de savoir pour toutes les données accumulées.

Si on pense à l'exemple de M. Keenan concernant les cyberattaques au moyen par exemple d'un maliciel, ne considérez-vous pas qu'il pourrait être avantageux — ce qui n'est pas nécessairement le cas du point de vue d'un chercheur — de travailler en vase clos? Je n'arrive pas à croire que je suis en train de dire cela après toutes ces années passées dans le secteur des finances à m'efforcer d'abattre les cloisons entre les gouvernements ou leurs différents ministères.

Pour ce qui est de la cyberinformation à proprement parler, l'importance du principe du besoin de savoir et la nécessité d'éviter... Il faut trouver le juste équilibre, car en rendant ces informations accessibles en source ouverte, on les met également à la disposition de nos adversaires.

Je peux comprendre votre point de vue de chercheur, mais ne croyez-vous pas qu'il existe des motifs vraiment valables de limiter en partie l'accès aux détails sur les relations entre le CST et les Forces armées canadiennes ainsi qu'entre ces dernières et les différents ministères? Ne voyez-vous pas quel pourrait être le risque pour la sécurité si toutes ces données étaient accessibles en source ouverte?

● (0945)

M. Alexander Rudolph: Je serais d'accord avec vous en principe, mais je préconiserais une approche plus nuancée étant donné que cette problématique va s'articuler à différents niveaux, tout comme c'est le cas pour les autorisations de sécurité. Le problème vient du fait que ces cloisonnements ont vu le jour sans qu'on se demande vraiment au départ s'ils étaient nécessaires et dans quelle mesure ils pouvaient nuire à l'efficacité opérationnelle de nos forces armées.

Mme Jennifer O'Connell: Auriez-vous des exemples à nous donner pour nous permettre de pousser plus loin notre analyse?

M. Alexander Rudolph: Il va de soi qu'il existe des bases de données regroupant des renseignements plus détaillés et d'autres qui portent sur les politiques. Dans un cas comme dans l'autre, des mesures ponctuelles font surface. S'il y a une politique qu'il conviendrait vraiment de tirer davantage au clair, ce serait la position des Forces armées canadiennes relativement à la stratégie d'engagement soutenu.

Mme Jennifer O'Connell: Engagement soutenu par rapport à quoi ?

M. Alexander Rudolph: Il s'agit de la politique des États-Unis pour contrer les États antagonistes dans le cyberespace.

Le président: Je dois malheureusement mettre fin à cette portion de notre séance. Comme nous avons pu le voir avec les trois ou quatre dernières questions, nous commencions à aller au fond des choses, surtout concernant les liens entre le Centre de la sécurité des télécommunications et les Forces armées canadiennes ainsi que les relations du CST avec différentes organisations comme Affaires mondiales Canada et Sécurité publique Canada. Tout cela est cloisonné, mais nous espérons que l'étanchéité ne soit pas totale, car c'est la sécurité qui doit toujours primer.

Par ailleurs, la question sur la stratégie d'engagement soutenu nous amène à nous interroger sur la capacité du CST de mener des opérations semblables au Canada. Au nom du Comité, je vous invite à nous soumettre par écrit vos réflexions à ce sujet afin d'éclairer les recommandations stratégiques qu'il nous faudra formuler.

Je tiens à vous remercier d'avoir bien voulu comparaître aujourd'hui devant le Comité pour prendre part à cette conversation des plus stimulante.

Nous allons maintenant suspendre la séance, le temps d'accueillir nos prochains témoins.

Je veux vous remercier encore une fois, monsieur Rudolph et, surtout vous, monsieur Keenan, car vous avez dû vous lever un peu plus tôt en raison du décalage horaire. Nous vous en sommes très reconnaissants.

● (0945)

_____(Pause)_____

● (0950)

Le président: Nous reprenons nos travaux.

Avant de demander à Mme Csenkey et à M. Rapin de nous présenter leurs exposés de cinq minutes, je veux noter que notre collègue et ami, James Bezan, n'est pas des nôtres aujourd'hui parce qu'il est au chevet de son petit-fils qui a subi une opération à cœur ouvert hier. On m'indique que le bébé se porte bien. Dans la foulée de la tragédie de Laval, nous nous préoccupons plus que jamais du sort de nos enfants et de nos petits-enfants. J'ai moi-même des petits-enfants et je peux vous assurer que c'est mon cas. Je vous prierais donc de ne pas hésiter à envoyer un petit mot à notre collègue.

Sur ce, je vais d'abord donner la parole à Mme Csenkey pour les cinq prochaines minutes, après quoi M. Rapin disposera également de cinq minutes.

Mme Kristen Csenkey (doctorante, Balsillie School of International Affairs, Wilfrid Laurier University, à titre personnel): Bonjour à tous. C'est un honneur pour moi d'avoir été invitée à comparaître et je vous remercie de me donner l'occasion de prendre la parole devant vous aujourd'hui.

Je tiens à souligner que nous nous trouvons sur le territoire traditionnel de la nation des Algonquins-Anishinabe qui l'occupe depuis des temps immémoriaux. À mes yeux, cette déclaration prend toute son importance dans le cadre de notre engagement envers le processus de réconciliation et de notre reconnaissance des liens territoriaux et identitaires.

Je m'appelle Kristen Csenkey et je suis doctorante à l'École d'affaires internationales Balsillie de l'Université Wilfrid-Laurier où il me reste seulement à présenter ma thèse. Mes recherches portent sur la cybergouvernance et la gestion des nouvelles technologies au Canada.

J'ai l'honneur d'avoir été convoquée par le Comité pour parler de cybersécurité et de cyberguerre. Je vais aborder ces deux sujets en ma qualité de chercheure et d'universitaire s'intéressant à l'aspect gouvernance de la cybersécurité. J'ai rédigé des articles sur différentes questions liées aux sujets à l'étude, à savoir notamment les menaces associées à la cybersécurité, les rôles et les responsabilités des différents acteurs, et les recoupements à faire avec les situations de conflit. Je vais donc traiter de ces enjeux à la lumière de mes recherches et de mes publications.

Mes observations préliminaires vont porter sur deux considérations importantes qui sont susceptibles d'éclairer le Comité dans son étude. Il s'agit d'abord du caractère évolutif des menaces liées à la cybersécurité, puis de la nécessité d'une coordination et d'une coopération entre les différents acteurs pour se préparer à contrer ces menaces.

Permettez-moi de vous en dire plus long sur ces deux enjeux.

Je parle d'un caractère évolutif, car la cybersécurité est une notion complexe qui ne cesse de changer en faisant intervenir un grand nombre d'acteurs, de contextes et d'idées. Cela s'explique du fait que la cybersécurité est une opération combinant des considérations sociales, politiques et techniques dans le cadre de laquelle ressources humaines et technologiques s'imbriquent. Nous vivons dans un monde cybermatériel en ce sens que de nombreux aspects de nos existences se déroulent dans des espaces numériques reliés à des composantes physiques. En conséquence, les menaces associées à la cybersécurité exigent une compréhension nuancée des capacités et du potentiel technologiques mis à contribution ainsi que du rôle des acteurs humains, tout particulièrement lorsqu'il s'agit d'interpréter les menaces et d'y réagir.

Cela m'amène à mon second point. Pour être prêt à contrer les menaces associées à la cybersécurité, il faut de la coordination et de la coopération. Si nous devons discuter du caractère évolutif de ces menaces, et notamment du potentiel et des capacités technologiques des différents acteurs, il nous faut aussi parler de la façon dont nous pouvons les neutraliser. Tout cela peut sembler plutôt évident, mais les choses ne se passent pas toujours de cette manière dans les faits.

Voici un exemple que je soumets au Comité. Dans un article que nous avons publié récemment, ma coautrice et moi-même nous sommes penchés sur la perception de différents états alliés relativement à la menace quantique. Je parle ici d'une menace pour la cybersécurité qui découle des capacités offertes par les ordinateurs quantiques. Parmi les partenaires du Groupe des cinq, nous avons décelé des différences dans la manière dont cette menace, ses intentions, la technologie employée, ses utilisateurs et les possibles acteurs malveillants sont pris en compte dans les politiques. Les divergences dans l'interprétation des menaces associées à la cybersécurité ont une incidence sur les rôles et les responsabilités des différents acteurs chargés de les neutraliser.

Il faut qu'il y ait une coordination entre les divers acteurs ayant un rôle à jouer à l'égard des aspects politiques, sociaux et techniques dont la combinaison influe sur la cybersécurité. Une telle coordination peut voir le jour à la faveur d'une mobilisation de l'expertise et des pistes de solutions existantes ne se limitant pas à une compréhension contextuelle unique de la menace. La coopération est nécessaire à cette fin.

La coopération est en effet essentielle pour neutraliser les menaces liées à la cybersécurité et assurer la protection du Canada. Notre pays peut miser sur les partenariats sûrs déjà établis pour coordonner les interventions face aux différentes menaces en tenant compte du caractère évolutif de la cybersécurité. On pourrait à cette fin favoriser une mobilisation formelle ou informelle d'alliés aux vues similaires possédant les capacités techniques voulues afin de définir globalement les menaces et de mieux comprendre les enjeux de capacité et de potentiel technologiques qui y sont associés de même que toute la complexité des aspects humains et techniques de la cybersécurité. En misant en priorité sur des partenariats novateurs, on pourrait mieux assurer notre sécurité tout en protégeant et en faisant valoir les intérêts des Canadiens à l'étranger.

C'est grâce à la coopération et à la coordination que le Canada pourra faire le nécessaire pour veiller ce que nous demeurions en sécurité au sein d'un monde cybermatériel déjà très complexe.

J'espère bien avoir l'occasion de discuter plus à fond des idées et des enjeux que je viens de mettre de l'avant en répondant à vos questions.

Je vous remercie de votre attention.

● (0955)

Le président: Merci, madame Csenkey.

Monsieur Rapin, vous avez cinq minutes.

M. Alexis Rapin (chercheur en residence, Chaire Raoul-Dandurand en études stratégiques et diplomatiques, Université du Québec à Montréal, à titre personnel): Monsieur le président et mesdames et messieurs les membres du Comité, bonjour. Merci de me donner l'occasion de comparaître devant vous aujourd'hui.

Je suis chercheur en résidence à la chaire Raoul-Dandurand en études stratégiques et diplomatiques de l'Université du Québec à Montréal. Mes recherches portent sur les enjeux liés à la cyberstratégie et à la cyberdéfense ainsi que, dans une perspective plus large, sur les impacts des technologies de l'information sur la sécurité internationale.

En 2020, l'équipe de recherche dont je fais partie a créé une base de données ayant pour but de recenser publiquement les cyberincidents géopolitiques ciblant le Canada, soit aussi bien ses entités gouvernementales que ses entreprises, ses institutions de recherche ou sa société civile. Nous avions alors fait le constat que les cyberincidents géopolitiques touchant le Canada faisaient rapidement les manchettes pour tomber ensuite encore plus vite dans l'oubli. Nous jugions que les Canadiens n'avaient pas toutes les données à leur disposition pour bien comprendre l'ampleur cumulative et la prévalence des cyberactivités étrangères visant leur pays. Nous avons donc rendu librement accessible en ligne un répertoire dans le but de documenter les cyberincidents de notoriété publique en précisant leur nature, leurs cibles et, dans la mesure du possible, leurs instigateurs. L'exercice avait aussi pour but de compiler une liste des cyberactivités étrangères ciblant le Canada de telle sorte que la population puisse se faire une bonne idée de l'évolution de ce phénomène.

Trois ans plus tard, notre base de données renferme aujourd'hui 93 cyberincidents géopolitiques qui ont touché le Canada depuis 2010. De ce nombre, il y en a eu 14 en 2022 seulement. En fait, nous avons pu observer que la fréquence des incidents semblables est en nette augmentation. Comme je l'indiquais, nous recensons uniquement les incidents de notoriété publique, si bien qu'il y en a assurément encore bien davantage qui n'ont toujours pas été signalés.

[*Français*]

Ces 93 incidents incluent différents types d'activités malveillantes: de l'espionnage économique contre des entreprises et des universités canadiennes; de la surveillance électronique clandestine d'activistes et d'organisations non gouvernementales basées au Canada; ainsi que de la collecte de renseignements visant des organisations gouvernementales canadiennes, entre autres.

Nos données indiquent par ailleurs que la très grande majorité de ces incidents proviennent de quatre pays seulement: la Chine, la Russie, l'Iran et la Corée du Nord. S'il n'est pas toujours certain que les gouvernements de ces pays sont responsables de chacune de ces attaques, il fait peu de doute que ces quatre États posent des défis majeurs en matière de cybersécurité pour le Canada.

En 2021 et en 2022, notre équipe a également publié des rapports annuels synthétisant nos principales observations quant aux cyberincidents les plus récents. Ces rapports avaient également pour but de mettre en lumière certaines tendances actuelles qui nous apparaissaient comme critiques pour la sécurité nationale du Canada.

● (1000)

[*Traduction*]

Notre dernière évaluation, publiée en 2022, se concentrait sur les tendances suivantes: la menace grandissante des cyberattaques par rançongiciels contre des entités canadiennes, parfois commanditées par un État, susceptibles de perturber des infrastructures essentielles ou de servir à dissimuler la collecte clandestine de renseignements; les ciblages de plus en plus agressifs d'activistes, d'exilés et de dissidents basés au Canada par des puissances étrangères à des fins d'espionnage, d'intimidation et de harcèlement; et la hausse du nombre de cybermercenaires, qui commencent à cibler des entités canadiennes, fort probablement à la demande de puissances étrangères.

Il va sans dire que ces trois tendances ne constituent pas le portrait complet des cybermenaces auxquelles le Canada fait face actuellement. Il faudrait également surveiller attentivement le conflit en Ukraine et l'espionnage économique constant des activités de recherche et développement au Canada, par exemple.

Ce que j'essaie de démontrer avec ces faits, cependant, c'est que les enjeux de cybersécurité ne constituent pas une menace future, hypothétique et lointaine pour le Canada. Les cybermenaces sont déjà présentes. Même si elles peuvent sembler discrètes ou intangibles, elles ont des répercussions directes sur la vie de nombreuses personnes au Canada tous les jours.

Par conséquent, j'estime qu'il est urgent de s'attaquer plus vigoureusement à ces enjeux et d'en discuter plus honnêtement et publiquement. La réunion d'aujourd'hui offre une excellente occasion de le faire.

Je serai ravi de répondre à vos questions.

Le président: Merci, monsieur Rapin.

Monsieur Calkins, vous disposez de six minutes.

M. Blaine Calkins: Merci, monsieur le président.

La réunion d'aujourd'hui est très éclairante.

Ma première question, qui s'adresse à l'un ou l'autre des témoins, est la suivante: s'il survenait une cyberattaque coordonnée tous azimuts par tous les acteurs malhonnêtes dans le monde, le Canada serait-il en mesure de se protéger? Est-ce qu'il y aurait une défaillance de nos systèmes essentiels?

Mme Kristen Csenkey: Je peux répondre à cette question.

À l'heure actuelle, le gouvernement du Canada, par le biais des divers ministères chargés de protéger les Canadiens et les infrastructures essentielles du Canada, fait de son mieux. Il y a toujours des progrès à faire, particulièrement lorsqu'il s'agit de signaler les cyberattaques. En ce moment, il n'est pas obligatoire de signaler les cyberattaques majeures. Si les PME, ou les entreprises dans cette catégorie, avaient l'obligation de signaler les cyberattaques, cela nous aiderait à évaluer l'ampleur de la situation. Cela nous fournirait également davantage de renseignements nous permettant de mieux évaluer la menace et les risques et d'élaborer un cadre visant à mieux protéger certaines industries et des entreprises du secteur privé.

Le gouvernement fait de son mieux, mais nous pouvons en faire davantage. Entre autres, nous pourrions imposer le signalement obligatoire des cyberattaques majeures.

[*Français*]

M. Alexis Rapin: Je vais répondre en français si vous me le permettez.

En ce qui concerne les infrastructures critiques, je pense qu'il y a un risque. Les infrastructures critiques sont effectivement extrêmement importantes. Elles portent bien leur nom, car elles sont critiques. Or les cyberattaques sur les infrastructures critiques représentent une menace à risque élevé, mais peu probable.

Le fait que les cyberattaques sur les infrastructures critiques représentent une menace à risque élevé veut dire que, bien évidemment, il faut y penser, s'y préparer et se doter de plans au cas où elles se produiraient. Cependant, elles restent assez peu probables.

À mon avis, il y a peut-être un risque pour nous à trop accorder d'attention aux menaces qui pèsent sur les infrastructures critiques dans la mesure où, comme je le dis, ce sont des choses qui sont relativement improbables.

Très peu, voire aucune, ne se sont véritablement matérialisées au Canada. Par contre, de nombreuses autres menaces beaucoup plus discrètes, moins graves, mais qui ont quand même des conséquences parce qu'elles se répètent et se produisent au quotidien, attirent moins notre attention et suscitent moins de réflexion de notre part.

Je pense que c'est un problème, parce que l'enjeu des infrastructures critiques est quelque chose qui est très visible et pour lequel ce n'est pas forcément très difficile de tracer des lignes rouges, d'être clair sur ce qui serait toléré ou non et ce qui susciterait une réponse vigoureuse ou non.

Devant cet ensemble de plus petites menaces qui, prises individuellement, ne sont pas jugées comme assez graves pour susciter une réponse, mais qui, de manière cumulée, produisent des dégâts qui sont à mon avis problématiques, je ne suis pas certain qu'on ait une bonne stratégie et une manière d'essayer de les décourager et de les empêcher.

● (1005)

[*Traduction*]

M. Blaine Calkins: Le simple fait que nous ne sommes pas une cible suffisamment importante en tant que pays et que nos infrastructures essentielles ne sont pas non plus une cible suffisamment importante… Toutefois, nous sommes membres d'organismes comme l'OTAN. Je pense que l'augmentation que nous observons est directement liée au fait que nous fournissons à l'Ukraine de l'équipement de défense.

Seriez-vous d'accord pour dire que l'aide que nous fournissons à l'Ukraine nous met à risque? Je ne dis pas que nous ne devrions pas fournir de l'aide à l'Ukraine, mais est-ce que d'autres acteurs utilisent cela comme prétexte pour s'infiltrer dans nos systèmes de défense?

[*Français*]

M. Alexis Rapin: Selon moi, en termes comparatifs, le Canada n'est, pour le moment, pas une cible prioritaire pour la Russie ou pour les cyberacteurs qui se placeraient à son service.

D'après ce qu'on observe et les informations dont je dispose, le facteur géographique semble quand même jouer un rôle important. Ce sont les pays plutôt proches de l'Ukraine ou de la Russie et les membres de l'OTAN qui sont les plus visés. Je pense à la Pologne, à la Slovaquie et aux États baltes, notamment, qui, d'après ce que j'ai vu publiquement, ont subi beaucoup plus d'attaques que le Canada.

Si la Russie avait pour but de punir le Canada en encourageant ses réseaux criminels à déployer des logiciels de rançon ou en encourageant des activistes à mener des opérations de piratage et de divulgation d'information contre le Canada, par exemple, on les aurait déjà vus et on aurait déjà observé une recrudescence très marquée. Or, d'après ce que j'observe, ce n'est pas le cas.

Cela étant…

[*Traduction*]

Le président: Nous allons devoir nous arrêter là.

Merci, monsieur Calkins.

Monsieur May, vous disposez de six minutes.

M. Bryan May: Merci, monsieur le président.

J'ai été ravi d'apprendre, madame Csenkey, que vous fréquentez la Balsillie School. Je connais bien cette école. Je viens moi-même de la région de Waterloo, alors je connais bien cet établissement et le travail extraordinaire qui y est effectué. En fait, il y a quelques semaines seulement, j'ai eu le plaisir d'accompagner le ministre Champagne à l'Institut Périmètre, qui est situé tout près, pour le lancement de la Stratégie quantique nationale du Canada. Je dois avouer que je n'ai absolument rien compris à la plupart de ce qui a été abordé, mais je reconnais le travail fantastique qui y est accompli.

Sur ce, pouvez-vous nous expliquer dans quelle mesure les progrès de l'intelligence artificielle et de la technologie quantique modifient l'environnement de cybermenaces au Canada?

Mme Kristen Csenkey: Je vous remercie beaucoup pour cette question, monsieur May.

Je dirais que certaines technologies peuvent avoir d'énormes répercussions sur la cybersécurité. Nous pouvons les qualifier de perturbatrices. Nous pouvons les qualifier aussi de technologies émergentes. Parfois, nous les considérons comme étant une menace ou comme étant très perturbatrices. Cependant, de mon point de vue, ces technologies interagissent également avec les humains. Ce sont les humains qui créent les technologies. Nous travaillons avec ces technologies et nous les utilisons à diverses fins.

Prenons, par exemple, les ordinateurs quantiques. Ils peuvent être utiles dans de nombreux domaines. Nous pouvons examiner cela autrement que dans l'optique de la défense. Nous pouvons examiner les avantages que comporte, par exemple, l'expansion de l'intelligence artificielle pour améliorer les simulations et bien d'autres choses, notamment les prévisions météorologiques.

Lorsqu'il est question d'investir dans certaines technologies et d'en mettre au point dans le but de renforcer les capacités du Canada, je pense qu'on peut compter sur des experts dans divers pôles régionaux qui accomplissent un excellent travail, mais je crois que nous avons besoin d'une plus grande collaboration pour contrer les menaces associées à l'utilisation de ces technologies en particulier, tout en gardant à l'esprit que la technologie ne constitue pas la seule menace. Il y a aussi la possibilité que certains acteurs malhonnêtes utilisent certaines technologies d'une manière qui pourrait causer du tort.

L'une des façons d'accroître la collaboration pour contrer ces menaces serait de tirer parti des partenariats existants. Il faut tirer parti des partenariats qui existent chez nous, au Canada, entre le gouvernement, l'industrie et le milieu universitaire par l'entremise des divers centres de recherche qui se consacrent à ces types de technologies en particulier, et nous devons aussi tirer parti des voies de partenariat existantes parmi nos alliés.

● (1010)

M. Bryan May: Merci.

Monsieur Rapin, avez-vous quelque chose à ajouter? Vous avez bien couvert le sujet, je suppose.

Dans le contexte de l'adoption massive des technologies émergentes au sein de la population canadienne, quelles tendances, selon vous, entraînent les plus grands risques liés à la cybersécurité?

Vous pouvez répondre en premier, monsieur.

[*Français*]

M. Alexis Rapin: Parlez-vous de technologies, particulièrement de nouvelles technologies, d'innovation?

[*Traduction*]

M. Bryan May: Oui. Je pense notamment aux véhicules intelligents, à la technologie prêt-à-porter, etc. Devrions-nous nous préoccuper de certaines technologies qui pourraient être vulnérables aux cyberattaques?

[*Français*]

M. Alexis Rapin: Je ne serais pas en mesure de hiérarchiser les enjeux selon leur importance, mais quelque chose attire beaucoup mon attention, et c'est l'Internet des objets. Il y a une prolifération exponentielle des objets connectés. Pour le Canada, très simplement, cela veut dire que la surface d'attaque augmente. Il y a plus d'appareils par lesquels on peut mener des cyberattaques et des cyberopérations.

Actuellement, dans bien des cas, les objets connectés sont le maillon faible de la chaîne. Ce sont de petits objets qui ont été conçus pour être peu coûteux et très faciles à utiliser, entre autres. Souvent, ce que les constructeurs vont sacrifier dans leur conception, c'est la cybersécurité.

Il y a peut-être des réflexions à avoir concernant les normes de cybersécurité à imposer aux objets connectés. Il faudrait s'assurer, par exemple, qu'ils ne deviendront pas, dans un avenir rapproché, une espèce de porte d'entrée privilégiée pour des brèches ou des compromissions de systèmes plus importantes.

[*Traduction*]

Le président: Merci, monsieur May.

[*Français*]

Monsieur Garon, vous avez la parole pour six minutes.

M. Jean-Denis Garon: Merci beaucoup.

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

Monsieur Rapin, j'aimerais savoir si, en matière d'échanges d'information sur la cybersécurité, le Canada est un acteur crédible parmi ses alliés. Je pense notamment au Groupe des cinq. Comment ces échanges se font-ils? Est-ce donnant, donnant?

Le Canada est-il en mesure d'être assez performant en matière de collecte et de production d'informations pour être un allié crédible auprès du Groupe des cinq, notamment?

● (1015)

M. Alexis Rapin: Dans le cas du Groupe des cinq, c'est un peu un repas-partage. Tout le monde est censé apporter quelque chose à manger et, ensuite, on partage ce qu'il y a à manger.

M. Jean-Denis Garon: C'est cela. Maintenant, ce qu'on doit savoir, c'est si le Canada cuisine beaucoup.

M. Alexis Rapin: Je ne suis pas en mesure de répondre à cela. Malheureusement, je ne siège pas aux comités du Groupe des cinq et je n'ai pas d'information privilégiée là-dessus.

Toutefois, l'opinion secondaire que je peux donner, c'est que, pour bien des chercheurs et bien des gens qui travaillent à cela, le Canada n'est pas perçu comme un acteur qui apporte beaucoup à la table. Je ne dis pas que c'est forcément l'opinion très tranchée qu'ont tous les membres, mais c'est souvent l'opinion qui transparaît.

M. Jean-Denis Garon: Nous comprenons la nuance, et c'est tout à fait adéquat de le mentionner.

Cela étant dit, je remarque que le Canada a beaucoup tardé, dans bien des cas, à prendre des décisions stratégiques et importantes, dernièrement. On peut penser à celui de Huawei, mais il y en a d'autres. Je me demande si cela n'a pas nui à notre crédibilité auprès de nos alliés et si cela n'a pas changé négativement la perception qu'ils ont de nous.

M. Alexis Rapin: C'est sûr que le Canada n'a pas brillé particulièrement à cet égard. On a peut-être donné un peu l'impression qu'on suivait le mouvement plutôt que l'impression qu'on prenait une décision ferme et déterminée.

À mon avis, il y a beaucoup de facteurs qui entrent en ligne de compte. Ce que j'entends souvent, auprès de collègues étrangers notamment, c'est que le Canada a l'image d'un pays qui est très « gentil », ou qui a peut-être ce qu'on pourrait appeler une culture de sécurité nationale...

M. Jean-Denis Garon: Diriez-vous qu'on le trouve naïf?

M. Alexis Rapin: Non. En tout cas, ce n'est pas du tout les opinions que j'entends. Toutefois, c'est peut-être une question de maturité quant aux questions de sécurité nationale; on n'est pas toujours prompt à empoigner le problème et à vouloir s'y attaquer de front.

M. Jean-Denis Garon: Permettez-moi de changer un peu de sujet et d'aborder une question d'actualité que je trouve extrêmement importante.

Vous savez que la firme McKinsey a fait beaucoup affaire avec le Canada. On parle de centaines de millions de dollars de contrats octroyés, notamment par le ministère de la Défense nationale. On sait que McKinsey, qui est une firme très peu reconnue pour ses normes d'éthique, fait beaucoup affaire avec la Chine. Cela fait partie du développement de son nouveau marché principal depuis les 15 ou 20 dernières années.

Les Canadiens et les Québécois ont-ils raison d'être inquiets quant à d'éventuelles fuites d'information? Le cas échéant, pensez-vous que nous devons avoir des mécanismes de transparence pour ces types de contrats plus élaborés?

M. Alexis Rapin: Je ne suis pas du tout en mesure de répondre à cette question, bien honnêtement.

M. Jean-Denis Garon: Je comprends.

Madame Csenkey, on a parlé de la menace des ordinateurs quantiques et d'autre chose. J'ai l'impression que, dans beaucoup de circonstances où on a des vulnérabilités, comme des cyberattaques, le facteur humain y est pour beaucoup. Dans bien de cas, l'ingénierie sociale fait qu'on a des vulnérabilités, et ce, indépendamment des investissements qu'on fait dans nos infrastructures.

Selon vous, le Canada fait-il suffisamment d'efforts pour que le risque lié aux facteurs humains soit le plus minimal possible?

[*Traduction*]

Mme Kristen Csenkey: Monsieur le président, j'aimerais remercier M. Garon pour sa question.

J'aimerais d'abord revenir sur une question que vous avez posée plus tôt au sujet du rôle du Canada au sein du Groupe des cinq, et ensuite, je vais répondre à votre question.

Le Groupe des cinq, comme nous le savons, est un partenariat important et fiable visant l'échange de renseignements de sécurité, et il peut aussi servir à l'échange d'informations reliées à la cybersécurité.

Comme je l'ai mentionné durant mon exposé, dans un article récent que j'ai co-rédigé, on explique que les alliés n'ont pas tous la même compréhension de certaines menaces à la cybersécurité, surtout parmi les alliés du Groupe des cinq. Lorsqu'il s'agit de trouver une solution à ces problèmes en matière de cybersécurité, je pense que le Canada pourrait prendre les devants au sein du Groupe des cinq pour aborder et favoriser la compréhension de certains enjeux de cybersécurité, comme la menace quantique. Cela pourrait peut-être se faire par le biais d'un consortium quantique dirigé par le Groupe des cinq.

Il faut comprendre que le Groupe des cinq est un partenariat pour l'échange de renseignements de sécurité et d'informations. C'est son objectif principal. Toutefois, nous avons vu que d'autres partenariats entre des alliés, comme AUKUS, peuvent avoir des objectifs secondaires pouvant nous permettre de collaborer au sujet de certains enjeux en particulier. Nous savons que...

● (1020)

Le président: Malheureusement, nous allons devoir nous arrêter là. Je suis certain que vous aurez l'occasion de poursuivre là-dessus.

[*Français*]

Monsieur Boulerice, vous disposez de six minutes.

M. Alexandre Boulerice: Merci beaucoup, monsieur le président.

Je remercie nos témoins d'être ici pour cette étude importante.

Madame Csenkey, en juillet 2021, vous avez publié un article intitulé « Selling Simulations: The Seduction of Cold War Techno-Fetishism in a Postmodern Cyber World ».

Premièrement, serait-ce possible pour vous de faire parvenir au Comité cet article scientifique pour qu'il puisse faire partie de notre rapport?

Deuxièmement, pouvez-vous nous indiquer comment cette analyse s'applique en ce moment aux tensions ou aux conflits qu'on voit avec la Russie et la Chine?

[*Traduction*]

Mme Kristen Csenkey: Monsieur le président, je serais heureuse de le transmettre au Comité.

Je vais inclure dans mon propos certains des arguments formulés dans l'article que le député vient de mentionner. Lorsqu'on parle de la technologie et des cybermenaces, le discours exclut souvent les acteurs humains, les intentions des humains, des idées à propos de certaines technologies et certaines capacités découlant de l'expérience et de la réalité vécues en ce qui a trait à la cybersécurité, qui constitue un système sociotechnique complexe. Quand on parle des menaces à la cybersécurité et de l'interconnexion entre les humains et la technologie, on peut inclure dans la discussion les services, les gens, les entreprises privées et les technologies connectées utilisées par différents secteurs.

J'aimerais insister sur le fait que, lorsqu'on parle des technologies connectées et qu'on les associe, par exemple, aux infrastructures essentielles, on favorise une compréhension plus dynamique des enjeux de cybersécurité liés aux infrastructures essentielles. Il est question à la fois des gens, des services, des exploitants privés et des technologies utilisées par…

Pour revenir sur une chose qui a été mentionnée lors de la première partie de la réunion, je dois dire que nous ne pouvons pas envisager les enjeux de cybersécurité en vase clos. Ils touchent différents aspects de la défense, c'est vrai, mais aussi de la sécurité nationale. Il y a aussi un aspect économique.

Je pense que, lorsqu'on parle des enjeux de cybersécurité et qu'on les associe aux technologies, aux gens, aux services, etc., nous devons savoir qu'il existe des considérations liées à la cybersécurité dans chaque secteur. Différents services sont fournis dans chaque secteur et diverses technologies sont utilisées, et, je le répète, il faut comprendre qu'il y a des liens entre eux.

Nous pouvons aussi comprendre que chaque secteur est confronté à des menaces, à des vulnérabilités et à des risques différents, mais il y a aussi des points communs. Lorsque nous parlons des problèmes de cybersécurité, nous devons aussi penser à des solutions à ces problèmes. Il n'existe pas une solution unique à tous les problèmes.

[*Français*]

M. Alexandre Boulerice: Merci beaucoup, madame Csenkey.

Monsieur Rapin, vous avez parlé des effets concrets des cyberattaques sur la vie des gens.

On l'a vu, l'été dernier, lors de la panne de Rogers; celle-ci n'avait pas été provoquée par une cyberattaque, mais par un problème de maintenance. Les gens se sont retrouvés extrêmement démunis. Ils marchaient dans les rues et cherchaient des adresses sur des cartes.

Il n'y a pas eu de conséquences, de punition, pour Rogers. Le fait d'être aussi dépendants d'une poignée de compagnies de télécommunication privées qui n'ont aucun compte à rendre n'est-il pas une preuve de notre vulnérabilité?

● (1025)

M. Alexis Rapin: Je ne pense pas être en mesure de statuer sur la question ou de me prononcer sur le lien qu'il peut y avoir entre la concentration de l'industrie et la vulnérabilité des infrastructures.

J'ai l'impression que ce qui va être plus important que la dispersion du marché, c'est la redondance des infrastructures ainsi que le fait d'avoir des systèmes de sauvegarde et d'avoir pensé la résilience en amont, peu importe le nombre d'acteurs qui sont impliqués. Il faut que quelqu'un, à un moment donné, réfléchisse à ce qui se passerait si telle attaque se produisait contre telle infrastructure et ainsi de suite.

J'ai le sentiment que c'est peut-être par là qu'il faudrait commencer.

M. Alexandre Boulerice: Pensez-vous que le gouvernement fédéral devrait avoir la responsabilité d'exiger des normes sur la redondance des systèmes, afin qu'il y ait une meilleure résilience des systèmes lors d'une situation quelconque?

M. Alexis Rapin: Je pense qu'il faudrait y songer, oui.

Des réflexions du genre sont menées aux États-Unis, particulièrement depuis la cyberattaque par rançongiciel contre Colonial Pipeline. De prime abord, sur papier, cet incident aurait pu ressembler à peu près à n'importe quelle autre attaque par rançongiciel, mais il a finalement eu des conséquences colossales. Une fois qu'une pression a été appliquée à un point bien particulier dans la chaîne, les conséquences ont été disproportionnées.

Je pense qu'il y a effectivement des réflexions à mener sur cet aspect.

[*Traduction*]

Le président: Je vous remercie, monsieur Boulerice.

Chers collègues, nous nous trouvons encore dans la même situation. Cette fois-ci, nous devons absolument nous arrêter à 10 h 45, alors je vais accorder aux prochains intervenants trois minutes, trois minutes, une minute, une minute, trois minutes et trois minutes.

Allez-y, madame Gallant.

Mme Cheryl Gallant: Le 8 juillet, il y a eu une panne chez Rogers, comme on l'a mentionné, et, la semaine dernière, le service 911 est tombé en panne dans les Maritimes. Il y a deux semaines, les responsables de l'aviation civile à Transports Canada ont émis un NOTAM dans la foulée d'une panne au sein de la FAA.

Le gouvernement devrait-il être obligé d'avertir le public lorsqu'une cyberattaque visant un système majeur est en cours? Le gouvernement ne nous a pas informés au sujet du ballon lorsqu'il était au-dessus de nous, alors pourquoi croire qu'il nous informerait d'une cyberattaque en cours?

Mme Kristen Csenkey: Je vous répondrai que, en ce qui a trait aux enjeux de cybersécurité qui deviennent d'importantes menaces à la cybersécurité, nous devons d'abord savoir que de nombreuses personnes et entreprises n'ont pas une bonne compréhension de ces éléments. Il est bien de signaler les cyberincidents, mais nous devons revenir en arrière et commencer par le début.

Nous devons veiller à ce que les considérations en matière de cybersécurité dans le cadre de certains projets en particulier, de certains...

Mme Cheryl Gallant: Monsieur le président, elle ne répond pas à la question, alors je vais m'adresser à M. Rapin.

Est-ce que le public devait être mis au courant d'une cyberattaque en cours contre des systèmes majeurs au Canada?

[*Français*]

M. Alexis Rapin: Je vais répondre en français, si vous me le permettez.

Mon opinion est que, oui, il devrait y avoir plus de transparence. Bien évidemment, en tant que chercheurs, nous sommes subjectifs parce que nous aimerions avoir plus d'information pour faire notre travail, mais je pense qu'il y a manifestement un intérêt public à avoir plus de transparence. Nous observons que les gens ne se sentent pas nécessairement concernés, or ils sont concernés. C'est ce qu'on constate avec les incidents que vous nous avez donnés en exemple. Les gens deviennent subitement choqués par ce qui se passe et ils ne comprennent pas, parce que le débat public sur les enjeux cybernétiques au Canada est très faible, car il y a peu d'information pour l'alimenter.

Ce serait bénéfique pour tout le monde si on pouvait avoir davantage de transparence sur ces enjeux.

● (1030)

[*Traduction*]

Mme Cheryl Gallant: Généralement, combien de temps faut-il à une entité pour se rendre compte que son système est victime d'une attaque, par rapport à une défaillance logicielle?

[*Français*]

M. Alexis Rapin: Je ne pourrais pas vous fournir de données précises à cet égard.

[*Traduction*]

Mme Cheryl Gallant: Le Canada n'a pas encore été victime d'une cyberattaque complètement dévastatrice. Pouvez-vous expliquer au Comité à quoi pourrait ressembler une véritable cyberattaque?

[*Français*]

M. Alexis Rapin: L'exemple qui revient très souvent serait une cyberattaque contre le réseau électrique. Cela pourrait causer beaucoup de dégâts. Nous en avons eu des exemples en Ukraine, en 2015 et en 2016, si ma mémoire est bonne. Plusieurs centaines de milliers de personnes se sont retrouvées sans électricité pendant plusieurs heures. Je ne sais pas à quel point le réseau électrique canadien est vulnérable.

[*Traduction*]

Le président: Monsieur Rapin, je comprends qu'il vous est difficile de répondre à cette question, mais il reste que c'est une bonne question. Si c'est possible, vous pourriez fournir une réponse par écrit ultérieurement. Ce serait peut-être une bonne façon de faire.

La parole est maintenant à M. Sousa pour trois minutes.

M. Charles Sousa (Mississauga—Lakeshore, Lib.): Merci, monsieur le président.

Les témoins précédents ont parlé de ce qui semble être une menace mondiale. Le Canada n'est pas le seul pays visé. Nous avons parlé du Groupe des cinq et des partenariats que nous essayons d'établir avec d'autres pays pour nous protéger et protéger le reste du monde. Ces enjeux ont des répercussions sur nos chaînes d'approvisionnement et les façons de faire des entreprises, et non seulement sur la politique, les élections et la défense. Ils ont de réelles conséquences économiques.

Nous avons aussi entendu parler de vases clos, qui semblent exister au Canada. La coopération s'améliore, mais il y a aussi des vases clos partout dans le monde, même au sein du Groupe des cinq. Vous avez mentionné que vous-même vous n'êtes pas au courant de tous les problèmes. Je me demande comment il est possible de coopérer avec d'autres États et, en même temps, de protéger notre propre sécurité nationale. Nous ne voulons pas divulguer trop d'informations.

Je suis également préoccupé par la guerre cognitive et les fausses nouvelles, qui contribuent à perturber notre mode de vie et notre démocratie. J'ai entendu parler de beaucoup de solutions et de l'absence de solutions. Il semble que ce soit la réponse. Il y a très peu que nous pouvons faire, car nous sommes encore en train d'apprendre et de nous adapter.

Quelqu'un a répondu qu'on ne nous dit rien, qu'il y a ce Big Brother, cette matrice. Qui est « on »?

[*Français*]

M. Alexis Rapin: Quand j'évoquais l'idée de transparence... Cela peut concerner différents types d'entités.

Le gouvernement fédéral pourrait être plus transparent. Il y a près d'un an, Affaires mondiales Canada a subi un cyberincident majeur. J'ai des sources qui me donnent de très bonnes raisons de penser que c'est la Russie qui est derrière cela et que cela n'a pas pris beaucoup de temps pour comprendre que c'était elle qui l'était.

Pour le moment, le gouvernement est très réticent à divulguer cette information, alors que ce serait d'intérêt public et qu'il serait important que le public canadien le sache.

[*Traduction*]

M. Charles Sousa: Je vais vous poser la même question, madame Csenkey, car ce que j'entends, c'est ce qu'on entend toujours, c'est-à-dire qu'il y a un certain nombre de groupes qui sont responsables, et on tente de coopérer pour trouver une solution tout en protégeant notre sécurité nationale.

Comment appliquer les solutions dont vous parlez en ce qui concerne les vases clos, alors que nous savons que des discussions se tiennent et qu'il faut faire preuve de transparence, même avec d'autres pays, même avec des pays qui ne font pas partie du Groupe des cinq, sans divulguer des informations concernant la sécurité nationale?

Le président: Veuillez répondre très brièvement, s'il vous plaît.

Mme Kristen Csenkey: C'est une grosse question, mais je vais essayer d'être aussi rapide que possible.

Premièrement, dans le meilleur des cas, il est difficile de cerner les cyberattaques et les motivations et d'identifier les personnes, les groupes ou les États responsables de ces attaques. Ce n'est pas facile. Par exemple, il peut s'agir d'un groupe de cybercriminels qui s'en prennent à une certaine cible pour soutirer de l'argent. Il peut s'agir d'un groupe qui travaille pour le compte d'un…

● (1035)

Le président: Pardonnez-moi, madame Csenkey, mais le temps de M. Sousa est écoulé.

Vous disposez d'une minute, monsieur Garon.

[*Français*]

M. Jean-Denis Garon: Madame Csenkey, si vous pouviez soumettre au Comité une réponse écrite à la question précédente, je vous en serais reconnaissant.

Monsieur Rapin, la diplomatie est-elle encore une solution avec la Chine pour essayer de prévenir les cyberattaques ou doit-on plutôt adopter une approche plus préventive?

M. Alexis Rapin: Je ne suis pas certain d'être en mesure de répondre à votre question.

Je peux vous dire qu'aux États-Unis, où on a pris conscience à mon avis beaucoup plus tôt qu'ici du problème massif causé par l'espionnage économique chinois par exemple, l'administration Obama a tenté une approche diplomatique.

À l'époque, le président Obama est allé rencontrer son homologue en Chine, et un accord a été négocié pour essayer de mettre un terme à l'espionnage économique. De ce qu'on a pu savoir, cela semble avoir fonctionné pendant environ une année. En tout cas, il y a eu une baisse majeure des activités d'espionnage économique chinoises. À la crise suivante, ou pour diverses raisons, l'espionnage économique a repris.

Je ne dis pas cela pour discréditer l'approche diplomatique. Il y a de la diplomatie à faire sur certains aspects.

M. Jean-Denis Garon: La diplomatie n'est donc pas suffisante.

M. Alexis Rapin: Je dirais qu'elle trouve ses limites selon les circonstances.

[*Traduction*]

Le président: Nous allons encore une fois devoir nous arrêter là.

[*Français*]

Vous avez la parole pour une minute, monsieur Boulerice.

M. Alexandre Boulerice: Merci, monsieur le président.

Monsieur Rapin, vous m'avez inquiété quand vous avez dit qu'il y a eu 93 cyberincidents connus au Canada depuis 2010, avec une fréquence à la hausse. Ce n'est pas surprenant que cela vienne de la Chine, de la Russie, de l'Iran et de la Corée du Nord. Il y a des opérations d'espionnage, de surveillance et de collecte de renseignements.

Ces cyberincidents ou cyberattaques visent-ils des infrastructures publiques, soit des agences, des ministères, ou plutôt des compagnies privées comme les banques, où l'on cherche de l'information sur des citoyens et des citoyennes?

M. Alexis Rapin: Ce n'est pas facile de se prononcer là-dessus. Selon l'information en source ouverte et publique que nous utilisons, la nature et le nombre des entités canadiennes visées sont rarement clairs. Par exemple, nous utilisons des rapports de firmes de cybersécurité qui vont mentionner que des entités canadiennes ont été touchées. Nous ne savons pas si elles sont nombreuses ou si c'est seulement une ou deux; nous ne savons pas non plus si ce sont des compagnies, des entités gouvernementales ou autres.

[*Traduction*]

Le président: Merci, monsieur Boulerice.

Monsieur Kelly, vous avez trois minutes.

M. Pat Kelly: Merci.

J'aimerais continuer de parler des 93 incidents précis que vous avez enregistrés en 2010. Vous avez dit que la Chine, la Russie, l'Iran et la Corée du Nord sont les principaux… peut-être que l'ensemble de ces 93 incidents peuvent être attribués à ces quatre pays. Vous avez parlé d'espionnage économique, mais vous avez aussi parlé de la surveillance des activistes. Dois-je comprendre que vous faites référence aux dissidents qui se trouvent au Canada, aux diasporas? Vous avez parlé du nombre de gens qui sont touchés.

Pouvez-vous me dire combien de Canadiens sont victimes de ce genre d'attaques ou sont la cible de ces attaques? Pouvez-vous nous expliquer un peu plus dans quelle mesure ces cyberincidents géopolitiques ont une incidence sur des Canadiens et nous dire quels genres de torts sont causés par ces incidents?

[*Français*]

M. Alexis Rapin: C'est difficile à chiffrer, parce que cela peut prendre différentes formes et revêtir des niveaux d'agressivité différents, selon la personne qui est visée. Dans le cas de la communauté ouïghoure, par exemple, cela peut être extrêmement agressif. Dans d'autres cas, cela peut prendre d'autres formes. En décembre dernier, par exemple, Amnistie internationale Canada a été visée par une cyberattaque menée vraisemblablement par la Chine. Le niveau d'implication de l'acteur qui est visé peut varier, et donc le niveau d'agressivité de l'attaque aussi.

Je pense qu'on a répertorié trois pays qui, jusqu'ici, visaient des activistes, des organisations non gouvernementales ou des dissidents au Canada. Chronologiquement, le premier a été l'Arabie saoudite, qui a visé un dissident établi au Canada. Cela avait été révélé par le Citizen Lab, à l'époque. Ensuite, il y a eu la Chine, qui s'en est notamment prise aux Ouïghours et qui a mené des opérations contre des membres du Falun Gong. Puis, plus récemment, on a aussi commencé à voir l'Iran faire ce genre de choses. On le soupçonne actuellement de faire de l'espionnage électronique en marge de manifestations.

● (1040)

[*Traduction*]

M. Pat Kelly: Puis-je vous demander, en ce qui concerne la Chine et ses cyberattaques contre la diaspora chinoise au Canada — contre ses citoyens et des citoyens canadiens — si les bureaux diplomatiques de Pékin au Canada sont impliqués dans ces attaques? Est-ce que ces attaques proviennent strictement de l'extérieur ou est-ce qu'elles sont menées avec la collaboration des missions diplomatiques chinoises au Canada?

[*Français*]

M. Alexis Rapin: Malheureusement, je ne dispose pas du tout d'informations qui me permettraient de répondre à cette question.

[*Traduction*]

Le président: Je vous remercie, monsieur Kelly.

Madame O'Connell, vous disposez de trois minutes.

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

Je vous remercie tous les deux de comparaître aujourd'hui.

Monsieur Rapin, je veux parler des différences dans votre base de données que je trouve intéressantes, les différences entre les attaques, par exemple. Je crois savoir qu'on peut acheter à petit prix dans le Web clandestin des logiciels ou des programmes malveillants. Ce type d'attaque sous forme de chantage contre une entreprise pourrait n'être même pas lié à un adversaire étranger, par exemple. Il y a cette distinction à faire. Il y a aussi une distinction à faire entre une attaque contre un organisme gouvernemental, par exemple, ou un ministère, et une attaque contre des entités privées.

Durant la présente étude, nous cherchons à obtenir des recommandations visant à améliorer nos systèmes. L'un des problèmes, c'est que le CST, le SCRS ou notre cybercommunauté n'a pas la possibilité d'intervenir auprès d'entités privées, même si elles ont été victimes d'une attaque par un acteur étranger. Il en va de même aussi, dans certains cas, en ce qui a trait à des infrastructures essentielles. Souvent, ce sont des municipalités qui sont propriétaires de telles infrastructures. En fait, la Loi sur le SCRS interdit à cet organisme de communiquer de l'information aux municipalités, aux provinces, etc.

Pouvez-vous nous parler des différences et formuler quelques recommandations sur les moyens à prendre pour nous assurer de faire la distinction entre une attaque commise par, disons, un mauvais acteur et une attaque perpétrée par un État étranger malveillant, et nous parler des divers niveaux?

[*Français*]

M. Alexis Rapin: Il faut considérer différents axes d'action. Tout ne pourra pas être résolu par le SCRS, la GRC ou même des organismes fédéraux. Comme vous le dites, beaucoup d'infrastructures qu'on peut considérer comme critiques et qui sont les plus vulnérables sont plutôt aux bas échelons, où il y a parfois moins de ressources et moins d'expertise pour en assurer la cybersécurité.

Il y a différents cas, notamment aux États-Unis, où des groupes de pirates étatiques étrangers ont visé des infrastructures municipales ou celles d'États, puisqu'ils s'attendaient à ce que les protections soient plus faibles à ce niveau. Il y a donc différents axes et différents niveaux à considérer.

Je crois que Mme Csenkey a évoqué, tantôt l'idée d'obliger les organisations qui gèrent des infrastructures considérées comme critiques à signaler les cyberincidents. Je crois que les États-Unis viennent de le faire ou sont sur le point de le faire. C'est une bonne pratique, et je pense qu'on devrait envisager.

[*Traduction*]

Le président: Merci, madame O'Connell.

Au nom du Comité, je tiens à remercier les deux témoins.

Comme vous pouvez le constater, il s'agit d'un sujet brûlant et très complexe. J'ai appris aux nouvelles ce matin que le groupe d'Elon Musk va couper l'accès à l'Ukraine à l'information fournie grâce au satellite. À mon avis, cela pose un immense risque pour la sécurité et un danger clair et immédiat dans le cadre de cette guerre.

Si vous avez des opinions à ce sujet, j'aimerais particulièrement les connaître.

Quoi qu'il en soit, je dois, malheureusement, mettre fin à la réunion.

Cela étant dit, chers collègues, la séance est levée.