CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

44e LÉGISLATURE, 1re SESSION

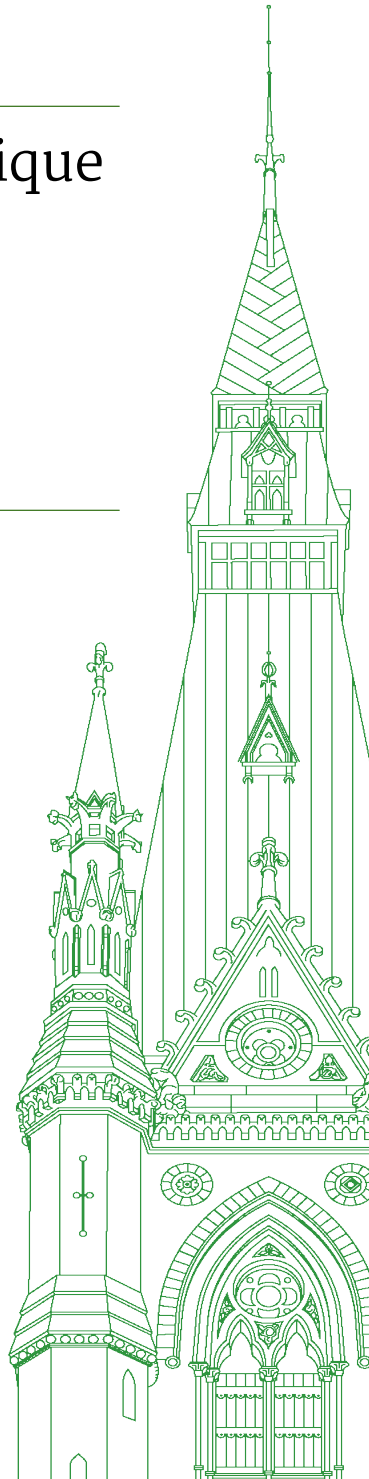
Comité permanent de la sécurité publique et nationale

TÉMOIGNAGES

NUMÉRO 028

PARTIE PUBLIQUE SEULEMENT - PUBLIC PART ONLY

Le mardi 7 juin 2022



Président : L'honorable Jim Carr

Comité permanent de la sécurité publique et nationale

Le mardi 7 juin 2022

● (1205)

[*Traduction*]

Le président (L'hon. Jim Carr (Winnipeg-Centre-Sud, Lib.)): Conformément au paragraphe 108(2) du Règlement et à la motion adoptée par le Comité, le jeudi 3 mars 2022, le Comité reprend son étude sur l'évaluation de la posture de sécurité du Canada par rapport à la Russie.

Nous accueillons aujourd'hui M. Ken Barker, professeur à l'Institute for Security, Privacy and Information Assurance de l'Université de Calgary, à titre personnel; Mme Juliette Kayyem, maître de conférences en sécurité internationale, chaire d'enseignement Belfer, au Kennedy School of Governement de l'Université Harvard et M. David Shipley, directeur général de Beauceron Security.

Bienvenue à tous. Je vous demanderai de présenter une déclaration préliminaire de cinq minutes. Quand il vous restera 30 secondes, vous verrez cette carte. Je suis très rigoureux quant au temps de parole, afin que ce soit juste pour tout le monde.

J'aimerais maintenant demander à M. Ken Barker de présenter sa déclaration préliminaire.

Monsieur, vous avez la parole dès que vous êtes prêt.

M. Ken Barker (professeur, Institute for Security, Privacy, and Information Assurance, University of Calgary, à titre personnel): Merci beaucoup de m'avoir invité. Je suis heureux de me joindre à vous aujourd'hui.

Je vais probablement dire des choses ici qui sont peut-être un peu différentes de ce que vous pourriez entendre d'un expert en sécurité. Je vais parler en particulier du fait que la vulnérabilité aux cyberattaques n'a pas vraiment changé depuis le début de la guerre entre la Russie et l'Ukraine. Ce que je dis, c'est que la vulnérabilité n'a pas changé, mais ce n'est pas nécessairement le cas de la posture de la menace.

Essentiellement, il existe aujourd'hui exactement les mêmes menaces que celles qui existaient auparavant. Les Russes n'ont probablement pas amélioré leurs attaques au cours des derniers mois ou avec le début de la guerre contre l'Ukraine. Rien n'a réellement changé, alors que se passe-t-il avec la vulnérabilité du Canada?

En tant que producteur d'énergie, le Canada est plus susceptible d'être la cible d'une attaque de la Russie. Évidemment, les pressions dues aux sanctions, etc. mènent la Russie à chercher des occasions potentielles d'attaquer les autres sources qui pourraient soutenir l'Occident. Des attaques dirigées contre ces secteurs se sont produites depuis le début de la guerre, mais il semble que le secteur — en tant que ressource vulnérable et faisant partie des infrastructures essentielles du Canada — était bien préparé et a réussi à se défendre contre les attaques que nous avons vues au cours des deux derniers mois.

Les attaques sont très différentes des réussites. Il y a un nombre considérable d'attaques de tous les acteurs, étatiques et apatrides, au quotidien, et ce, depuis des années. Si l'on ne s'était pas défendu de manière appropriée, cela aurait posé un grave problème bien avant la guerre elle-même. En fait, c'était un grave problème, et nous avons fait beaucoup de choses pour tenter de nous protéger.

Cependant, nous ignorons ce que nous ne savons pas; il y a quelque chose que l'on appelle les attaques du jour zéro qui pourraient se produire. Ce sont des attaques que l'on ne connaissait pas auparavant. Ces attaques pourraient être lancées sur nous à différents moments, sans que nous nous y attendions, parce que nous n'y sommes pas préparés. Nous ne savons pas que la menace plane ou quelles sont ces vulnérabilités. Cependant, nous n'avons constaté aucune augmentation de ces attaques au cours des deux derniers mois. Selon toute vraisemblance, si des attaques d'origine inconnue étaient lancées à ce stade, il y aurait probablement eu des failles dans les systèmes, mais nous n'avons pas réellement constaté cela, comme s'y attendaient de nombreuses personnes.

Le Canada investit dans le cadre du programme du Réseau canadien d'indicateurs de durabilité, et je pense que c'est une étape essentielle pour aller dans la bonne direction. C'est un investissement essentiel au chapitre de la cybersécurité actuelle et future du Canada. Il a été lancé en 2019, bien avant que cela ne se produise; alors, en réalité, le Canada a fait quelques progrès considérables ces derniers temps pour s'établir sur des bases très solides.

Ce que nous voulons vraiment faire, c'est construire une sorte d'écosystème cybersécurisé. Les infrastructures essentielles du Canada sont en général vulnérables parce qu'elles sont construites selon d'anciens systèmes qui sont connus pour être particulièrement vulnérables. Ce que je veux dire par anciens systèmes, c'est qu'il s'agit de systèmes qui existaient avant que l'Internet des objets, l'Ido, ne commence à se concrétiser. Avec l'arrivée de l'Ido et la nécessité de remplacer les anciennes composantes par celles connectées à Internet, nous exposons en fait certaines de nos infrastructures essentielles à une potentielle menace et attaque. Cela fait partie de ce qui est étudié dans la recherche et au niveau de l'organisation dans le secteur privé.

Les grandes entreprises sont probablement assez bien protégées en ce moment. La réalité, c'est que le secteur privé a investi beaucoup d'argent parce qu'il reconnaît sa vulnérabilité. Par conséquent, les acteurs du secteur privé ont réussi à faire avancer les choses de manière significative au cours des 20 dernières années. Cependant, les petites et moyennes entreprises sont simplement vulnérables à diverses attaques, et il faut investir davantage pour les protéger d'une certaine manière. Cependant, il est peu probable qu'elles soient une cible spécifique de la Russie, à moins qu'elles fassent partie de certains secteurs de cybersécurité ou qu'elles soient des fournisseurs d'infrastructures essentielles.

Le principal problème, c'est qu'il y a une grave pénurie d'experts dans ce domaine. Les établissements postsecondaires tentent d'y remédier. Il faut perfectionner et recycler les travailleurs actuels. La main-d'œuvre et le public en général manquent d'éducation et de connaissance, et le recrutement d'experts internationaux pourrait aider, mais il est peu probable que cela soit suffisant, simplement parce qu'ils sont très demandés.

Je vais m'arrêter là.

● (1210)

Le président: Parfait. Juste à temps. Bravo.

J'invite maintenant Mme Juliette Kayyem à faire sa déclaration préliminaire d'une durée maximale de cinq minutes.

S'il vous plaît, allez-y dès que vous êtes prête.

Mme Juliette Kayyem (maître de conférences en sécurité internationale, chaire d'enseignement Belfer, Kennedy School of Government, Université Harvard, à titre personnel): Merci de m'avoir invitée. Un de mes anciens étudiants est maintenant député. Taleeb était ici... je ne vois rien, mais je suis heureuse d'être ici.

Quand on m'a demandé de venir ici, j'ai dit clairement, car je voulais le déclarer, que je ne suis pas une experte de l'évaluation des risques auxquels est exposé le Canada. Je suis experte dans ce que nous appelons dans notre domaine la « période qui suit l'explosion », la réponse immédiate en aval, sur quoi je travaille à l'échelle internationale, qui consiste essentiellement à savoir quelles sont les capacités dont nous disposons, surtout dans le domaine cybernétique, advenant qu'une mauvaise chose se produise.

Comme le disait M. Barker, on se pose beaucoup de questions sur la vulnérabilité accrue pour un pays comme le Canada, compte tenu du conflit russe. Un grand problème se pose dans mon secteur, dans le secteur de la préparation: on se demande pourquoi il n'y a pas plus d'activité. Il peut y avoir plusieurs réponses. La meilleure réponse que nous avons jusqu'ici, c'est que peut-être, tout comme la capacité militaire, nous avons surestimé la cybercapacité de destruction de la Russie par rapport à sa capacité de créer des perturbations, des perturbations que nous pouvons gérer. Il se pourrait également que l'invocation de l'article 5 par l'OTAN ait peut-être apporté de la discipline, l'idée que toute attaque contre des infrastructures essentielles qui a des répercussions sur des personnes serait assimilée à une attaque militaire. Nous ne savons pas et nous n'avons pas terminé... que suppose donc la préparation à cet égard?

Dans l'ensemble — et, par une coïncidence amusante, j'ai participé il y a environ deux semaines à une séance d'information à ce sujet au Canada —, tout comme les États-Unis, le Canada et les infrastructures de son secteur privé ciblaient ce que nous appelons les capacités liées à la « période avant l'explosion »; autrement dit, empêcher, en amont, une sorte d'infiltration, une sorte d'explosion, pour ainsi dire. Ces capacités sont importantes et essentielles, mais la chose sur laquelle nous ne nous sommes pas assez penchés, surtout en coordination avec les États-Unis et les États du Nord, c'est ce qui se passerait s'il y avait une perturbation.

Nous mesurons la réussite à l'aune de notre capacité d'empêcher davantage de dommages de se produire. Autrement dit, à quelle vitesse peut-on intervenir? À quelle vitesse peut-on rétablir les systèmes? Ma norme est la suivante. Peut-on rendre quelque chose moins mauvais? Dans le secteur des infrastructures informatiques essentielles, comme l'expliquait M. Barker, on se concentre beaucoup sur la façon de contrer le piratage, les rançongiciels ou l'État-nation, et on se concentre moins sur ce que l'on ferait si cela se produisait. Y a-t-il plus qu'un interrupteur, ce qui est généralement le cas de ces éléments?

Jusqu'ici, nous avons tiré de nombreuses leçons de cette situation. Nous avons appris beaucoup du Colonial Pipeline des États-Unis, qui n'avait pas beaucoup de capacité.

Le délai d'intervention est primordial. Savez-vous quand votre système a été infiltré? À quelle vitesse pouvez-vous vous protéger contre ce que l'on appelle les pertes en cascades? Autrement dit, même s'il y a une perturbation ou une destruction, qui est encore plus importante, pouvez-vous arrêter les pertes en cascades et pouvez-vous demander au secteur privé de le faire?

Que signifient les pertes en cascades? C'est simplement qu'il y a l'élément initial, et puis il y a toutes les choses qui se produisent après le coup qui auraient pu être arrêtées si vous aviez été en mesure de gérer le préjudice.

Ensuite, quelle sorte de planification régionale a été mise en place? Nous savons certainement ici qu'aucune entreprise ni localité n'agit seule, mais en ce qui concerne la planification et la communication régionales, nous savons qu'il faut mieux comprendre les conséquences de la vulnérabilité. Il s'agit de savoir non pas seulement quel est le risque et quelle est la vulnérabilité, mais quelles sont les conséquences de la vulnérabilité.

Ensuite, je dirais que le troisième domaine dans lequel il y a un manque — et je pense que cela va sembler familier, dans tous les pays —, c'est qu'il faut davantage de communication avec le secteur privé au sujet des risques que vous constatez dans le gouvernement afin que nous puissions commencer à nous préparer.

● (1215)

Le président: Il vous reste 10 secondes.

Mme Juliette Kayyem: C'est la capacité de gestion des conséquences. Tout est une question de réaction quand on ne peut pas exactement mesurer le risque.

Merci.

Le président: Merci beaucoup.

J'aimerais maintenant demander à M. David Shipley de présenter sa déclaration préliminaire pour une durée maximale de cinq minutes.

Vous avez la parole, monsieur.

M. David Shipley (directeur général, Beauceron Security): Merci, monsieur le président et je remercie le Comité de me donner la possibilité d'être ici.

Je vais parler de trois recommandations essentielles. Premièrement, c'est qu'il faut rendre les déclarations d'incident obligatoires pour que l'on puisse savoir ce qui se passe en amont et en aval. Deuxièmement, je vais parler de la nécessité d'établir des normes en matière d'hygiène informatique de base pour tenter d'empêcher que les incidents se produisent. Troisièmement, je vais parler du besoin criant d'aider les petites et moyennes entreprises ainsi que le secteur public infranational — les soins de santé, les municipalités et l'enseignement supérieur — à assurer leur protection.

Je suis David Shipley et je suis le cofondateur et le directeur général de Beauceron Security. J'ai travaillé dans le secteur de la cybersécurité pendant la dernière décennie. J'ai obtenu le titre de gestionnaire agréé en sécurité de l'information de l'Association des professionnels de la vérification et du contrôle des systèmes d'information, et j'ai parlé des centaines de fois aux médias canadiens, au cours de la dernière décennie, au sujet des cyberattaques et de la manipulation des médias sociaux.

Beauceron sert près de 600 clients allant des plus grandes banques d'Amérique du Nord aux compagnies de télécommunications nationales, en passant par le gouvernement, les petites entreprises et plus. Notre technologie sert à éduquer plus d'un demi-million de personnes pour qu'elles connaissent davantage le rôle qu'elles jouent dans la cybersécurité et qu'elles s'en soucient davantage. Selon le « rapport d'enquête de 2022 sur l'atteinte à la protection des données » de Verizon, 82 % des cyberattaques réussissent en raison de l'élément humain, qu'il s'agisse de personnes qui se laissent prendre au piège de la manipulation émotionnelle dans des courriels, ce qu'on appelle l'hameçonnage, ou d'une erreur humaine dans l'utilisation ou la conception de la technologie. Le terme « cyber » met en relief à lui seul l'importance de l'élément humain. Le terme cyber vient du mot grec *kubernetes*, et il concerne la relation entre les personnes, la technologie et le contrôle. Un avenir dans lequel les personnes, les organisations, les gouvernements et la société contrôlent la technologie à laquelle ils se fient au quotidien est un avenir prometteur pour le Canada, mais ce n'est pas le présent dysfonctionnel dans lequel nous vivons.

Ceux qui cherchent à porter préjudice au Canada et à ses intérêts savent comment utiliser les technologies et contrôler les dommages. La capacité de la Russie à cet égard est bien documentée. La Russie a donné de l'expansion à sa capacité, avec des équipes de piratage soutenues par l'État, pour compromettre les infrastructures essentielles, comme il a été mentionné tout à l'heure, pirater les partis politiques et les gouvernements afin de trouver et divulguer les informations sensibles et plus. La Russie a favorisé l'épanouissement d'une industrie solide de la cybercriminalité et a des relations avec des gangs du crime organisé pour éviter d'être tenue responsable de ses actions. La Russie comprend également comment utiliser les sites Web et les plateformes des médias sociaux comme moyen de contrôler les gens par la désinformation. Marcus Kolga, de l'Institut Macdonald-Laurier, et d'autres ont également documenté cela. La manipulation des médias sociaux fait partie de l'éventail des armes, quand on parle de cyberconflit.

Les actions de la Russie dans le cyberespace ont eu de graves conséquences sur les Canadiens. Les cyberattaques des gangs criminels russes ont porté préjudice aux municipalités canadiennes, aux organismes de soins de santé et plus, et ont coûté des dizaines de millions de dollars. Selon l'entreprise de cybersécurité Emsisoft, plus de 4 000 organisations canadiennes ont été victimes des rançongiciels seuls, en 2021, avec des dommages estimés à pas moins de 654 millions de dollars.

Bien que le gouvernement du Canada ait fait des efforts considérables pour se protéger des cybermenaces, la plus grande partie du reste du Canada est aux mains du secteur privé ou du secteur public infranational. Pour réduire ce risque, nous devons mieux comprendre les cyberattaques, améliorer nos règlements en matière de cyberhygiène de base et augmenter les ressources de nos organisations les plus vulnérables.

Premièrement, nous devons mettre en œuvre une obligation de déclaration de cyberincident qui va au-delà des seules industries sous réglementation fédérale, et cela comprend les soins de santé ainsi que les chaînes d'approvisionnement vitales, y compris les secteurs manufacturiers et alimentaires. Nous sommes en retard par rapport aux États-Unis et à l'Europe à cet égard. La plupart des organisations ne vont pas collaborer volontairement avec le gouvernement fédéral pendant les incidents. Leurs équipes juridiques et de gestion du risque ou leur assureur leur disent de limiter le partage et la communication d'informations, parce que la collaboration avec le gouvernement est considérée comme offrant des gains limités et pouvant entraîner beaucoup de pertes. Cela signifie que nous perdons des informations essentielles sur les attaques visant le Canada et, surtout, que les causes profondes et les leçons importantes ne sont pas tirées ou communiquées de manière efficace.

Deuxièmement, il faut mettre en place une hygiène informatique nationale obligatoire. CyberSécuritaire Canada est un excellent début, mais la participation volontaire sera toujours faible. Nous devons tirer des leçons des programmes similaires du Royaume-Uni et lier l'accès aux marchés publics au respect des normes de cybersécurité de base.

Troisièmement, nos secteurs les plus vulnérables sont le secteur public infranational, comme l'enseignement supérieur, les municipalités et les soins de santé. Ils ont besoin de fonds dédiés du gouvernement fédéral pour améliorer leur sécurité le plus rapidement possible. Du côté du secteur privé, les petites et moyennes entreprises ont désespérément besoin d'aide pour se procurer les outils de sécurité dont elles ont besoin dans un environnement de plus en plus hostile.

Je m'en voudrais si je ne commentais pas la nécessité de réglementer les médias sociaux comme composante importante de notre stratégie nationale de cybersécurité pour que les Canadiens contrôlent les technologies qu'ils utilisent. Les algorithmes des médias sociaux qui amplifient la peur, la colère et la haine sont des outils que la Russie et d'autres ennemis exploitent fortement pour diviser notre société. Nous devons rendre aux Canadiens le contrôle sur le contenu qu'ils voient en exigeant que ce qu'ils voient par défaut sur les médias sociaux soit classé par ordre chronologique, et non pas selon un ordre décidé par un algorithme, et en rendant obligatoire la mise en place d'un modèle exigeant l'adhésion au contenu déterminé par un algorithme.

● (1220)

Le président: Vous avez 10 secondes, s'il vous plaît.

M. David Shipley: Si nous n'agissons pas aujourd'hui, nous nous condamnons à un avenir où nos entreprises seront paralysées par des vagues de tentatives d'extorsion étrangère, où nos citoyens et nos politiques seront empoisonnés par la division et la désinformation et où notre capacité de fournir les choses essentielles à la vie sera considérablement réduite.

Le président: Merci beaucoup, monsieur.

Merci à tous pour vos remarques. Nous passons maintenant à la première série de questions.

Nous commençons par Mme Dancho, qui dispose de six minutes.

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

Merci à tous les témoins d'être ici et à M. Shipley d'avoir pu être présent en personne.

Ma première question s'adresse à M. Shipley.

J'aimerais revenir sur quelques-unes des recommandations que vous avez formulées concernant la cyberhygiène obligatoire. L'une d'entre elles consiste à la lier aux exigences des marchés publics. Avez-vous d'autres choses à recommander?

M. David Shipley: L'idée de la lier aux marchés publics est venue du programme Cyber Esssentials du Royaume-Uni, dont s'inspire une partie de notre programme. Le Royaume-Uni a considérablement amélioré la sécurité de la chaîne d'approvisionnement de son gouvernement national. L'avantage pour le reste du pays est d'avoir des PME plus sûres. C'est un excellent point de départ.

Nous avons vu les avantages d'une bonne hygiène. Les mesures prises par l'Ukraine et le gouvernement des États-Unis pour se préparer au conflit que nous connaissons actuellement ont considérablement réduit les répercussions des efforts déployés par la Russie dans ce pays. Une bonne hygiène et une bonne préparation en amont nous épargnent beaucoup de misère.

J'ai eu un appel téléphonique d'une petite ou moyenne entreprise. C'était une quincaillerie. Elle a été frappée par un rançongiciel. Ça a été les pires trois journées de la vie du propriétaire. Il s'est avéré qu'il a fallu des semaines pour tout récupérer. Ils étaient de retour au stylo et au papier. Si seulement ils avaient eu plus d'aide et de ressources ou une incitation à investir dans la sécurité et l'aide pour le faire, ils auraient pu éviter ce mauvais jour.

La dernière chose que je mentionnerai à propos de la chaîne d'approvisionnement, c'est que vous ne savez jamais comment une faille dans la chaîne d'approvisionnement va se manifester. C'est un logiciel d'impôt en Ukraine qui a conduit à la paralysie en 2017 avec le virus effaceur malveillant appelé NotPetya. Il s'agissait d'une petite entreprise de logiciels fiscaux.

Les petites et moyennes entreprises peuvent connaître des répercussions surdimensionnées. Nous ne savons tout simplement pas comment la combinaison va se faire.

● (1225)

Mme Raquel Dancho: Pouvez-vous nous donner quelques exemples de la façon dont nous pouvons...? Vous avez mentionné la petite quincaillerie. Quel rôle le gouvernement joue-t-il pour encourager les entreprises? À quoi cela ressemble-t-il? Est-ce que c'est comme un allégement fiscal? Qu'est-ce que cela pourrait être, selon vous?

M. David Shipley: Eh bien, 48 % des petites entreprises ne dépensent rien en cybersécurité aujourd'hui. L'aide pourrait prendre la forme de crédits d'impôt. Vous pourriez également vous pencher sur des modèles comme le PCAN, qui a contribué à l'adoption du numérique et qui était essentiel pendant la pandémie. Malheureusement, cette adoption du numérique a en fait augmenté les vulnérabilités des petites et moyennes entreprises.

Nous devons intégrer la sécurité dans les subventions, les prêts et les autres mesures qui ont un lien direct avec les entreprises.

Mme Raquel Dancho: Merci beaucoup.

J'ai maintenant quelques questions pour M. Barker.

Vous avez récemment parlé dans un balado — je crois que c'était Cybersecurity Cubed — de la menace que représente l'informatique quantique pour nos réseaux actuels de cybersécurité et de cryptographie. Pouvez-vous faire part au Comité de vos commentaires sur la façon dont le Canada s'en tire dans ce domaine?

M. Ken Barker: J'ai probablement besoin d'un peu plus de contexte pour répondre à la question.

La menace existentielle de l'informatique quantique est probablement une menace future. Ce n'est pas une menace actuelle, en ce sens qu'elle menace les systèmes cryptographiques en place que nous utilisons actuellement pour faire fonctionner tous nos systèmes.

J'essaie d'éviter d'être trop technique ici.

À l'avenir, il est possible que l'informatique quantique puisse effectivement saper toutes les techniques de cryptage modernes et réduire la durée de vie, si vous voulez, de la période pendant laquelle quelque chose peut être considéré comme cryptographiquement sûr. Cette menace ne se pose pas à l'heure actuelle. Pour être franc, elle pourrait se concrétiser dans 10 ou 20 ans. Les défenseurs de la technologie quantique diront certainement que c'est pour bientôt. Ils n'ont pas tort. La réalité est que c'est probablement encore passablement loin.

La menace est cependant toujours réelle aujourd'hui dans le sens où, si elle se concrétise dans 20 ou 25 ans, nous disposerons probablement d'une cryptographie à résistance quantique à ce moment-là. Cependant, les données existantes qui sont actuellement sécurisées par le cryptage moderne deviendront vulnérables dans 20 ans. Si elles sont stockées quelque part de manière cryptée et que nous pensons qu'elles sont sûres pour les 2 000 prochaines années, elles pourraient alors devenir vulnérables. Toutes ces données cryptées héritées que nous considérons comme très sûres à l'heure actuelle pourraient devenir très vulnérables à ce moment-là. Une grande partie de ces données pourraient être divulguées ou piratées et se trouver quelque part. Elles pourraient devenir vulnérables à ce stade.

Je ne suis pas sûr d'avoir répondu à l'essentiel de votre question. C'est une question très compliquée.

Mme Raquel Dancho: Oui. Je pense que vous nous avez donné à tous un cours accéléré sur cette question complexe.

Est-ce que l'un de nos adversaires s'y intéresse activement? Investissent-ils dans ce domaine? Avez-vous entendu dire qu'ils en discutent?

Vous avez mentionné que, dans 10, 20 ou 25 ans, toutes nos technologies cryptées pourraient être menacées par l'informatique quantique de nos adversaires. Devrions-nous avoir cette discussion maintenant ou est-ce un peu trop tôt?

M. Ken Barker: Non, je pense que nous devrions avoir ces discussions maintenant. Les mécanismes que nous pourrions vouloir mettre en place dans 20 ans vont prendre 20 ans à élaborer. Nous parlons des d'efforts de recherche et de perfectionnement fondamentaux.

Le Canada, à bien des égards, est un chef de file dans ce domaine. Il y a plusieurs années, nous avons fait des investissements qui étaient essentiels à la promotion de la technologie quantique, mais je dois dire que le reste du monde commence à nous rattraper. Je pense que nous avons l'occasion d'être des chefs de file mondiaux dans cet espace particulier. Cela contribuera évidemment à protéger notre cybersécurité.

● (1230)

Le président: Merci beaucoup.

Mme Raquel Dancho: Merci beaucoup.

Le président: J'aimerais maintenant donner la parole à M. Noormohamed pour son bloc de questions de six minutes.

La parole est à vous, monsieur.

M. Taleeb Noormohamed (Vancouver Granville, Lib.): Merci, monsieur le président.

Merci à tous les témoins d'être avec nous aujourd'hui.

Je m'adresse en particulier à mon ancienne professeure, madame Kayyem, je suis heureux de vous voir. J'aimerais, si vous me le permettez, commencer par vous poser quelques questions, s'il vous plaît.

Vous avez parlé de perturbation et de destruction, et du fait que nous pouvons gérer la perturbation, mais que la destruction est une tout autre paire de manches. Ce qui me préoccupe, c'est que l'un des défis auxquels nous sommes exposés est que, lorsque nous examinons les répercussions des robots russes au chapitre de la diffusion de fausse information... Tout d'abord, ils diffusaient de la désinformation sur la COVID et essayaient de semer la discorde avec cette idée de briser la confiance envers les institutions publiques. Nous avons constaté une proximité entre ce discours et les opinions d'extrême droite, puis — quelle surprise! — un lien avec des messages en ligne très pro-russes et anti-ukrainiens.

Je me demande si, oui ou non, l'érosion de l'opinion qu'a le public de la politique commence à se déplacer vers le domaine de la destruction d'une manière à laquelle nous n'avons peut-être pas pensé. J'aimerais beaucoup avoir votre avis sur la question. Au Canada, nous commençons certainement à le voir. C'est quelque chose qui, je pense, nous préoccupe tous.

Mme Juliette Kayyem: Je pense que c'est vrai. Je pense que vous avez tout à fait raison de dire que toutes les crises ne sont pas des catastrophes. En d'autres termes, si nous sommes construits pour cela, nous pouvons — advenant tout type d'attaque — survivre à quelque chose si nous y sommes préparés.

Cela devient — je reprends le terme de l'OTAN — « destructeur » si vous ne pouvez pas gérer même les plus petites choses. Elles s'appuient les unes sur les autres. C'est la notion même de pertes en cascade. Si vous ne pouvez pas arrêter le mal à proximité de la vulnérabilité... bien que vous ne sachiez même pas quelles seront les répercussions en aval, surtout dans le contexte cybernétique, ce que nous avons vécu ici, aux États-Unis, dans le cas d'importantes infrastructures. En raison d'une simple attaque par rançongiciel comme celle visant le Colonial Pipeline, qui était vraiment simple et pas très complexe, vu qu'ils n'avaient pas la capacité de réagir, tout le système a été hors service pendant une semaine. Ce n'est pas complexe.

Une des façons de voir cette relation est... En tant que nation et en tant que gouvernement, vous vous concentrez vraiment sur ce qui est destructeur chez la Russie. Je pense que l'OTAN l'a clairement exprimé. Il ne va pas définir la différence entre une attaque perturbatrice et une attaque destructrice. Je pense que c'est une bonne chose. En d'autres termes, il s'agit en fait de maintenir suffisamment de flou dans le système pour que l'adversaire ne sache pas où se situe la limite. La dernière chose que vous voulez faire est de dire: « Nous considérons ceci comme destructeur et ceci comme seulement perturbateur. »

Je pense que la meilleure réponse... Nous ne sommes pas dans le monde de l'astrophysique. Le fait que nous parlions de cybersécurité ou de cyberattaque les fait paraître technologiques. Du côté de la réaction, ce n'est pas très complexe. Il n'est pas nécessaire de savoir coder. Il s'agit en grande partie de disposer de systèmes de communication dotés de multiples défenses et de systèmes qui empêchent les pertes en cascade, en d'autres termes, de systèmes de soutien régionaux divisés ou parallèles qui peuvent assurer une aide mutuelle. Si un système énergétique tombe en panne, vous pouvez partager avec les autres ou obtenir des systèmes de leur part. Ce sont des capacités de gestion d'urgence qui ont fait leurs preuves.

J'ai passé de nombreuses années à essayer de faire comprendre au monde de la cybersécurité qu'il n'est pas nécessaire de réinventer la roue. Une grande partie de ce que nous avons appris des attaques perturbatrices et destructrices était déjà connue.

M. Taleeb Noormohamed: Dans le même ordre d'idées, lorsque nous pensons au monde de la cyber... que, pour une raison ou une autre, des gens considèrent toujours comme trop complexe, alors qu'il n'est peut-être pas aussi compliqué que nous le percevons, comme vous l'avez expliqué. Lorsque vous regardez ce qui se passe aux États-Unis et que vous regardez où se situe le Canada sur ce spectre et ensuite, lorsqu'on pense à ce que vous avez dit concernant l'incapacité de la Russie à bien mener une guerre terrestre et, sans doute, l'incapacité ou le manque de volonté de la Russie de mener une guerre en ligne en ce moment, à quoi devrions-nous penser en ce qui concerne la Russie?

Y a-t-il des choses qui nous échappent, à nous, à l'Occident, en ce qui concerne l'origine du prochain événement? Si tel est le cas, pouvez-vous nous faire part de vos réflexions à ce sujet? Sur quoi devrions-nous porter notre attention, afin d'être aussi bien préparés que possible?

● (1235)

Mme Juliette Kayyem: Je ne veux même pas prétendre savoir quelle est la stratégie, mais maintenant, malheureusement, nous — les Ukrainiens, avec le soutien de nos deux pays — risquons de nous retrouver pendant longtemps dans une situation pénible qui sera moins transparente parce qu'elle ne se déroule pas dans les grandes villes. Les médias, les États-Unis, les Canadiens, nous allons tous nous y intéresser moins.

Au chapitre de la vulnérabilité, nous pourrions revenir à une époque où il n'y avait pas de répercussions sous forme de sanctions et où les rançongiciels et autres acteurs pouvaient fonctionner en toute liberté, en utilisant la Russie et ses capacités. Ces activités peuvent sembler moins cautionnées par l'État, mais elles le sont indéniablement.

Le président: Merci beaucoup.

Madame Michaud, je me tourne maintenant vers vous pour un bloc de questions de six minutes, dès que vous serez prête.

[*Français*]

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

Je remercie les témoins d'être présents aujourd'hui. Nous leur en sommes très reconnaissants.

Je vais m'adresser à vous, madame Kayyem.

Je vais lire, en anglais, l'extrait d'un article qui est paru dans le *Washington Examiner* à propos de votre livre, *The Devil Never Sleeps*. Voici ce qu'on mentionne dans cet article à propos de votre livre.

[*Traduction*]

> [Cela] souligne que les dirigeants du gouvernement et du secteur privé ne doivent plus concentrer toute leur attention et leurs ressources sur la prévention des catastrophes.
>
> Ils doivent plutôt apprendre à planifier en conséquence et à utiliser tous les outils disponibles pour atténuer les conséquences défavorables lorsqu'une catastrophe survient.

[*Français*]

Vous dites entre autres qu'on aurait dû prévoir l'invasion de l'Ukraine par la Russie et qu'on aurait dû se demander ce qui allait se produire et comment on allait y réagir. Vous parlez de la possibilité de mettre moins l'accent sur la prévention.

J'aimerais que vous nous en disiez plus à ce sujet, dans la mesure où nous avons entendu plusieurs experts nous dire que le Canada n'était pas suffisamment préparé à faire face à des menaces ou à des cybermenaces par rapport à d'autres pays du Groupe des cinq, par exemple.

Dans cette mesure, comment le Canada aurait-il dû se préparer ou comment devrait-il se préparer à la possibilité qu'un géant comme la Russie menace par exemple les infrastructures essentielles du Canada?

[*Traduction*]

Mme Juliette Kayyem: Je vous remercie de la question.

À certains égards, les limitations qui existent avant une guerre, comme celles qui touchent votre capacité ou votre accès au renseignement, existeront même au cours de celle-ci. Merci d'avoir mentionné le livre. Je dois dire que j'ai passé 25 ans dans ce que nous appelons « tous les dangers ». Essentiellement, je ne m'intéresse pas seulement à la cybersécurité. Je m'intéresse aux vulnérabilités des nations comme la vôtre et la mienne. J'ai beaucoup travaillé sur la notion d'une capacité de réaction régionale nord-américaine en matière de cybersécurité et de changement climatique, car le type d'attaques et de vulnérabilités que nous connaissons actuellement vont nécessiter une attention commune de la part des États-Unis, du Mexique et du Canada, étant donné nos capacités.

Nous devons concentrer notre sentiment de réussite sur notre capacité à réagir et à minimiser les préjudices, ce qui est particulièrement vrai à cet égard. Une chose que je vous invite à faire valoir auprès du secteur privé, qui a essentiellement... C'est sans doute un peu brutal, mais le secteur privé a essentiellement concentré la quasi-totalité de ses efforts de sécurité « en amont de l'attaque ». Autrement dit, si nous pouvons empêcher la fuite, nous essaierons d'empêcher les mauvaises choses de se produire et allons rester, comme j'aime à le dire, en amont de l'attaque. Il est possible d'insister en demandant quel est leur plan d'intervention, quel est le type d'exercices de simulation en cas de cyberattaque.

Le point le plus important sur lequel je vais conclure est le suivant. La bifurcation entre la cybersécurité et la sécurité physique, qui est apparue dans votre pays et dans le mien, doit être réglée d'une manière ou d'une autre. Toutes ces attaques nous montrent qu'il n'y a plus vraiment de cyberattaques. Il s'agit plutôt d'une cyberattaque doublée d'une attaque physique. Ce qui s'est passé dans bon nombre de ces entreprises, et je sais que vous en êtes conscients, de même que ce qui s'est passé dans nos institutions gouvernementales, c'est que l'appareil de cybersécurité et l'appareil de sécurité physique — les points de contrôle traditionnels, les armes et les gardes, comme nous les appelons — ont été mis en place. Il n'existe pas beaucoup de synergie entre eux en cas de cyberattaque, et je pense que nous devons vraiment insister sur ce point auprès du secteur privé.

Il y aura toujours des conséquences physiques. Il s'agit rarement de simples questions au sujet de la vie privée, des renseignements personnels ou de la réputation. L'adversaire souhaite qu'il y ait des perturbations et, pire encore, de la destruction.

● (1240)

[*Français*]

Mme Kristina Michaud: Madame la présidente, je vais utiliser le temps qu'il me reste pour poser une petite question au professeur Barker, qui est spécialisé en informatique et en référentiels de données qui préservent la confidentialité.

En mai 2022, l'Université d'Ottawa produisait ce document:

[*Traduction*]

Comment le Canada peut s'adapter à un contexte de sécurité qui se détériore, un rapport du groupe de travail sur la sécurité nationale de l'École supérieure d'affaires publiques et internationales.

[*Français*]

Cette publication exhortait le gouvernement à envisager la création d'un nuage ultrasecret à l'échelle du gouvernement, comme beaucoup d'alliés l'auraient fait avant nous, sous diverses formes. Ce nuage comprendrait de vastes quantités de données stockées par chaque ministère et organisme. Ce serait une façon concrète de protéger ces données en cas d'attaque.

Que pensez-vous de l'idée de créer un nuage ultrasecret pour stocker les informations confidentielles du gouvernement? Serait-ce une bonne façon de se prémunir contre certaines cyberattaques?

[*Traduction*]

M. Ken Barker: J'aimerais d'abord contester la question un peu. J'ignore ce qu'est un nuage « top-secret ». Si un nuage est une ressource partagée accessible à des personnes pour de nombreuses raisons valables, alors pour le rendre ultra-secret, vous devez utiliser le contrôle d'accès. Le contrôle d'accès est en fait un système dans lequel vos données ultra-secrètes sont stockées et où vous limitez l'accès d'une quelconque manière.

Le président: Vous disposez de 10 secondes, s'il vous plaît.

M. Ken Barker: Donc, je ne crois pas vraiment... Le vocabulaire est peut-être populiste, mais il n'est pas approprié.

Le président: Merci beaucoup.

Monsieur MacGregor, c'est à votre tour, vous disposez de six minutes. La parole est à vous.

M. Alistair MacGregor (Cowichan—Malahat—Langford, NPD): Je vous remercie, monsieur le président.

Madame Kayyem, j'aimerais commencer par vous. J'aurais aimé que vous soyez là avant notre dernière réunion, puisque nous rencontrions le ministre de la Protection civile, Bill Blair. Le Comité a eu l'occasion de le questionner quant à son rôle. Comme vous le savez, le ministère de la Sécurité publique et de la Protection civile a été divisé. Nous avons désormais deux ministères responsables de ces deux domaines respectifs.

En ce qui concerne une grande partie de vos propos, lorsque je regarde la lettre de mandat du ministre concernant la protection civile... Vous pouvez la lire en ligne. Notre comité veut au bout du compte déposer un rapport avec des recommandations spécifiques.

Si l'on examine les responsabilités de notre ministre de la Protection civile, y a-t-il quelque chose que vous aimeriez voir dans ce rapport afin que le ministre se concentre spécifiquement sur cela?

Mme Juliette Kayyem: Je me concentrerais sur deux domaines, étant donné ma compréhension, qui n'est pas aussi approfondie que la vôtre.

La première tient à la capacité de gestion des urgences transfrontalières. En cas de cyberattaque à Detroit, disons dans le secteur automobile, auprès des fabricants d'équipement d'origine, quelles sont les capacités, les communications et les structures en place qui permettront de traiter cette situation comme une intervention sans frontières? Il le faut. Cela va avoir un impact sur les deux pays. Il va y avoir un impact, comme nous l'avons observé avec certaines des manifestations récentes, sur les passages frontaliers et notre capacité de traverser la frontière. Il s'agit là du premier impact.

Il faut aussi se demander quel devrait être le mandat du gestionnaire des urgences, car je suis d'accord avec vous. Je suis d'avis que la distinction entre la sécurité publique et la gestion des urgences peut être difficile à faire parfois. J'ai parlé d'une exigence, mais il y en a deux. De quoi le ministre a-t-il besoin pour réagir à ce que nous appelons, dans mon milieu, « tous les dangers »? En d'autres termes, vous ne pouvez pas vous concentrer uniquement sur ce que sera la riposte informatique. Il y aura toutes sortes d'impacts. Il en va de même pour le climat et pour une attaque terroriste. Les conséquences sont généralement les mêmes.

Il m'arrive de penser — et je sais que c'est assurément votre cas — qu'en raison de la structure du gouvernement, des ministères, la sécurité de l'information est reléguée au second plan en ce qui concerne la protection de nos réseaux. J'insisterais davantage sur des examens qui sont menés, sur les capacités existantes, sur les conséquences physiques d'une cyberattaque contre une grande industrie et sur les mesures que nous prenons pour combler l'écart entre la sécurité de l'information et la sécurité physique.

Je vous dirais que je conseille désormais à beaucoup d'entreprises de ne pas avoir de responsables de la sécurité de l'information ni de responsables de la sécurité et de n'avoir que des responsables de la protection, puisqu'il est trop difficile de savoir quel est le risque.

● (1245)

M. Alistair MacGregor: Je vous remercie.

Monsieur Shipley, j'aimerais m'adresser à vous.

Pouvons-nous faire des recommandations? Quels types d'investissements pourrions-nous faire en matière de dissuasion? Pouvons-nous faire en sorte que les personnes qui envisagent potentiellement une cyberattaque, peu importe, la forme...? Existe-t-il de bonnes options de défense? Je pense au vieil adage selon lequel la meilleure défense est une bonne attaque. Est-ce que ce genre de capacité est mise en place?

M. David Shipley: Je n'ai pas d'informations précises sur les opérations du CST. Nous savons que les pouvoirs législatifs ont été accordés et que la capacité de mener des opérations a désormais débuté...

M. Alistair MacGregor: Savez-vous si cela existe dans le secteur privé?

M. David Shipley: Nous ne voulons en aucun cas que le secteur privé riposte, car, tout d'abord, l'attribution est vraiment difficile. Je gérais la cybersécurité d'une université. Nous étions constamment victimes de piratage et avons été utilisés comme plateforme pour attaquer des entités gouvernementales ou du secteur privé, entre autres. Si quelqu'un commençait à riposter en attaquant mon université puisque, selon lui, nous étions la source d'origine, il toucherait la cible finale. Il s'agit d'un petit jeu de passe-passe amusant.

L'attribution est vraiment difficile. Le secteur privé ne devrait absolument pas riposter. Il devrait s'agir d'une responsabilité exclusive du gouvernement fédéral, qui devrait être exercée. Il me semble que le défi d'un point de vue stratégique est de savoir ce qui relève des services de maintien de l'ordre et ce qui relève de l'armée? Il nous faut plus de clarté à ce sujet, et nous devons faire preuve de souplesse. Il est important que le gouvernement se prononce fermement sur ce sujet.

Nous l'avons vu avec le gouvernement Biden après les attaques contre les infrastructures essentielles aux États-Unis. Le message provenait directement d'en haut: ne vous en prenez pas à nous. Qui est le ministre qui va réellement réagir ici au Canada?

M. Alistair MacGregor: Vous avez mentionné le rapport d'incident obligatoire. Nous avons constaté des problèmes dans le cadre d'autres études que nous avons menées. Qu'elles portent sur l'extrémisme violent à caractère idéologique ou sur les armes à feu, quand vous ne disposez pas de toutes les données nécessaires, vous prenez de mauvaises décisions aux plus hauts échelons. Si vous souhaitez élaborer à ce sujet, quelle est l'importance de disposer d'une vision complète de sa série de menaces qui pèsent sur nous et de pouvoir déployer nos ressources de manière appropriée?

M. David Shipley: En ce moment, ma plus grande préoccupation est la menace qui pèse sur le secteur des soins de santé au Canada. De toute évidence, la pandémie n'est pas encore terminée. Nous nous en remettons encore. Quand un hôpital est touché, il l'est pendant des semaines. Les patients atteints de cancer ne bénéficient pas des soins en temps voulu, d'autres interventions chirurgicales sont retardées, etc. Le partage de l'information n'est pas bon dans notre pays. Nous avons été victimes de multiples attaques. Un système provincial tout entier a été durement touché, et nous n'en avons pas tiré de leçons.

Le président: Vous disposez de 10 secondes, s'il vous plait.

M. David Shipley: Imaginez que nous ayons des accidents d'avion et que nous n'enquêtions pas sur eux ou ne communiquions pas les leçons à en tirer. Eh bien, il y aurait plus d'accidents d'avion.

M. Alistair MacGregor: Je vous remercie.

Le président: Merci beaucoup.

Chers collègues, nous passons maintenant à une deuxième série de questions.

Pour commencer, je céderais la parole à M. Lloyd pour cinq minutes.

Monsieur, la parole est à vous.

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

Ma question s'adresse à M. Shipley et porte spécifiquement sur la désinformation russe. Je suis préoccupé par le fait que nous avons parfois des œillères partisanes au sein du Comité. Il ne s'agit pas seulement d'un phénomène d'extrême droite.

Êtes-vous d'accord pour dire que les Russes exploitent et ont exploité des acteurs dans tout le spectre politique afin de faire avancer leur plan?

M. David Shipley: Les États-Unis et d'autres pays nous en donné la preuve. L'objectif peut être simplement de nous monter les uns contre les autres. Que les gens soient de gauche ou de droite, ils s'en moquent. Tant que nous ne nous faisons pas confiance, que nous ne communiquons pas, que nous ne pouvons pas faire de politique et que notre démocratie semble ne pas fonctionner, alors leur système semble légitime et leurs objectifs sont atteints. Le but est de nous paralyser.

Maintenant, ce qui m'effraie, c'est qu'il existe quelques preuves selon lesquelles certains groupes de camionneurs au Canada étaient influencés par des fermes de contenus qui voulaient simplement vendre des T-shirts et des casquettes merdiques. Notre démocratie est brisée pour que quelqu'un puisse vendre des T-shirts dénigrant le premier ministre.

M. Dane Lloyd: Un cas vraiment convaincant que nous avons vu la veille de l'invasion de l'Ukraine par Moscou était celui des députés de gauche qui disaient que le Canada ne devrait pas soutenir l'Ukraine puisqu'il s'agit d'un État fasciste. Voilà ce qui a été dit. Il s'agit d'une reprise de la propagande russe, et cela a été entendu jusque dans le Parlement canadien.

Êtes-vous d'accord pour dire qu'il s'agit d'un cas important de désinformation?

● (1250)

M. David Shipley: Je ne suis pas au courant de ces cas précis. Toutefois, en me fondant sur ce que vous dites, je préciserais que nous avons reçu des avertissements de nos agences de renseignement qui parlent d'opérations d'influence menées contre des députés de tous les partis, de diverses nationalités qui ont des intérêts, que ce soit la Russie, la Chine, etc. Tout cela fait partie du jeu, et c'est ce qu'ils font, que ce soit pour marquer des points, pour essayer de nous maintenir désengagés dans ce conflit ou quel que soit l'objectif national... cela en fait partie. Cela fait ressortir l'importance d'apprendre aux députés et aux politiciens à se protéger.

Une chose qui me préoccupe est la protection de nos partis politiques en général contre les opérations informatiques et les tentatives d'influence. Le piratage du Comité national démocrate aux États-Unis montre clairement que ce qui se passe lorsqu'un parti n'est pas sécurité peut avoir des conséquences dramatiques sur le cours des événements dans un pays.

M. Dane Lloyd: Je vous remercie.

Je tiens à ce que cela figure dans le compte rendu. Avez-vous relevé des preuves de la manière dont le discours russe « les Ukrainiens sont des nazis » a été utilisé afin de susciter la peur parmi les groupes politiques de gauche dans le monde et peut-être au Canada? Cela a-t-il été observé?

M. David Shipley: Je pense qu'il y a eu des signalements, des tentatives visant à dissimuler... je veux dire que c'est parfaitement logique. Comment faites-vous pour maintenir le Canada à l'extérieur du conflit alors qu'il y a tant de personnes d'un côté comme de l'autre? J'ai entendu des personnes de la droite dire: « Ce n'est pas notre combat, et pourquoi devrions-nous nous préoccuper de ce qui est arrivé? » Il y a des personnes de gauche qui disent: « bien, il y a des nazis et du fascisme ».

On veut seulement brouiller les cartes. Le problème, c'est que nous vivons à une époque de postvérité, et nous devons travailler là-dessus. La vérité doit encore exister quelque part.

M. Dane Lloyd: Je suis content que vous l'ayez dit officiellement.

Je vais m'adresser à Mme Kayyem.

Lorsqu'il est question de votre excellent travail sur ce problème lié à la sécurité nationale, je suis très préoccupé par les impulsions électromagnétiques. Il s'agit peut-être d'un fait bien connu, mais j'aimerais connaître votre opinion. Une explosion nucléaire qui se produit dans l'atmosphère peut avoir très peu de conséquences cinétiques au sol, mais elle pourrait avoir des conséquences dévastatrices sur nos appareils électroniques.

Cela pourrait-il être perçu comme une violation de l'article 5, et exiger une réponse de l'OTAN?

Mme Juliette Kayyem: Je pense vraiment que l'OTAN et l'administration Biden ont agi très intelligemment à ce sujet quant aux nouvelles menaces. Elles ne se penchent pas précisément sur la menace. Lorsqu'il est question de cybersécurité ou, comme vous l'avez mentionné, de perturbations électromagnétiques, elles envisagent les conséquences. Elles ont établi une distinction entre les deux très tôt.

Cela m'a pris un certain temps avant de comprendre ce qu'elles faisaient, parce qu'elles n'étaient pas très transparentes à ce sujet. Elles disaient: « écoutez, il y a des perturbations dans le monde, et nous les accepterons parce que c'est à ce prix que nous pouvons faire des affaires ». En d'autres mots, comme nous sommes connectés, parce que l'internet fonctionne, parce que nous avons besoin de nos appareils électroniques, nous allons toujours présumer qu'il existe un certain niveau de vulnérabilité.

Il y aura des perturbations parce que les gens se comportent tout simplement mal, mais ce ne sont pas des raisons pour entrer en guerre.

M. Dane Lloyd: Une impulsion électromagnétique ne serait pas une raison...

Mme Juliette Kayyem: Ce le serait si cela entraîne de la perturbation... La norme est la suivante: est-ce que cela perturbe la capacité de civils de vivre? En d'autres termes, est-ce qu'une mère ne serait pas en mesure de nourrir ses enfants, ou...

M. Dane Lloyd: J'ai seulement 10 secondes.

Recommanderiez-vous que nous prenions davantage de dispositions pour nous protéger contre les impulsions électromagnétiques?

Mme Juliette Kayyem: Oui, à presque tous les égards, je le pense.

Le président: Merci beaucoup.

Madame Damoff, c'est à votre tour, vous avez cinq minutes.

Mme Pam Damoff (Oakville-Nord—Burlington, Lib.): Merci.

Merci à tous nos témoins d'avoir fourni un témoignage aujourd'hui.

En fait, je veux poursuivre dans la même voie qu'un commentaire qu'a formulé mon collègue, M. Lloyd.

Madame Kayyem, je m'adresse à vous.

Les campagnes de mésinformation et de désinformation ciblent habituellement des différends existants sur le plan social et politique afin de tenter de nous diviser davantage. Nous le voyons de plus en plus.

Je me demande seulement si vous avez des recommandations à faire au gouvernement pour garantir que nous abordons cette menace convenablement et adéquatement, et si vous pouvez recommander des dispositions que nous pouvons prendre pour reconnaître ce qui se passe, mais aussi le contrer?

Mme Juliette Kayyem: Oui, cela a été contesté grandement aux États-Unis. Une récente tentative visant à créer un organe de surveillance, une nouvelle entité au sein du ministère de la Sécurité intérieure, qui se penchera sur la désinformation, a été abandonnée presque immédiatement lorsqu'elle a été attaquée.

Parfois, je pense que, non seulement nous compliquons trop les choses, mais que, en plus, nous savons maintenant ce qui fonctionne — je vais y revenir — des personnes fiables du gouvernement qui abordent réellement la mésinformation. Je pense que, pendant longtemps, nos gouvernements ont pensé que personne ne pouvait vraiment croire ces choses. Si vous vous y prenez assez tôt, qu'on parle de « déboulonner les mythes »... Chez FEMA, la Federal Emergency Management Agency, on a mis en place quelque chose qu'on appelle le « déboulonneur de mythes », qui est une façon de contrer les rumeurs qui circulent durant une quelconque crise. Voilà la première chose.

Ensuite, comme nous le disons dans le domaine de la gestion de crise, il faut avoir des chiffres constants et de l'espoir. En d'autres mots, les porte-parole du gouvernement doivent constamment fournir des faits. Ils ne peuvent pas se cacher. Ensuite, que faites-vous pour améliorer les choses? L'espoir est toujours important.

Enfin, et je pense que nous en apprenons beaucoup de l'Ukraine... nous pensions que nos gouvernements avaient adopté un mode passif face à cette mésinformation, comme si la Russie fait ce qu'elle fait, et nous n'avons rien. En fait, je pense que le fait que le Canada, les États-Unis et d'autres pays aient réussi à parler des activités auxquelles s'adonnait la Russie, et ce, tôt et souvent, a littéralement changé l'allure des combats contre la Russie. Cela a préparé les Ukrainiens. Cela nous a préparés, nous. Cela nous a tous préparés.

Je pense que d'excellentes leçons peuvent être tirées de la contre-attaque menée contre la mésinformation découlant seulement de la guerre en Ukraine.

Lorsqu'il est question des mesures à prendre dans l'avenir, je pense qu'il faut se pencher sur la question, parce que nous n'avons plus à être passifs maintenant. Nous avons toujours pensé que la meilleure réaction était de passer à autre chose. Ce n'est pas le cas.

● (1255)

Mme Pam Damoff: J'aimerais juste revenir sur quelque chose que vous avez dit: vous avez parlé de « personnes fiables du gouvernement », sauf que certains aspects de ces campagnes de mésinformation discréditent le gouvernement. Comment pouvez-vous faire en sorte que les gens croient ce que dit le gouvernement lorsqu'il est lui-même visé par la campagne? Ce n'est pas juste le gouvernement. Toutes nos institutions sont touchées par ces campagnes de désinformation.

Mme Juliette Kayyem: Tout ne sera jamais parfait, donc je vis dans un monde où mon objectif consiste à limiter le plus possible les préjudices. Dix-neuf pour cent des gens aux États-Unis ne sont pas encore vaccinés. Ce n'est pas un chiffre très reluisant, mais comme il y a beaucoup de mésinformation, ce n'est pas aussi grave que ce que je croyais; donc, d'une certaine façon, je pense que nous avons été en mesure d'y arriver.

Par contre, lorsque je parle de « gouvernement », je ne parle pas seulement de l'ordre national. Si on s'attarde précisément à la COVID, c'est vraiment une stratégie de communication locale qui est venue à bout de la réticence des gens à se faire vacciner en raison de la mésinformation. En ce qui nous concerne, le Dr Fauci a perdu la capacité de convaincre un bassin de personnes. C'est correct, et cela arrive. Vous vous tournez vers des porte-parole plus locaux.

Mme Pam Damoff: Il me reste seulement environ 30 secondes, que je vous laisse, afin de permettre à mes collègues de terminer. Il est presque treize heures.

Le président: Dans ce cas, nous passerons à Mme Michaud.

Vous avez deux minutes et demie, puis nous terminerons la séance avec M. MacGregor, qui aura deux minutes et demie, avant de lever la séance.

Madame Michaud, allez-y.

[*Français*]

Mme Kristina Michaud: Merci, monsieur le président.

Monsieur Shipley, j'aimerais vous poser une question relative à l'incident qui est survenu il y a quelques semaines à Sunwing. Cet incident a démontré l'importance de rapporter les cyberattaques. Dans un article, vous dites que le Canada devrait suivre l'exemple des États-Unis. Il y a quelques mois, les États-Unis ont adopté une loi qui exige que les organisations du secteur des infrastructures critiques rapportent tout incident de cybersécurité substantiel au département de la Sécurité intérieure dans les 72 heures suivant la découverte d'une attaque ou dans les 24 heures suivant le paiement d'une rançon.

À votre avis, est-ce que cela pourrait être une bonne façon d'aider les petites, moyennes et grandes entreprises privées ou celles qui gèrent les infrastructures essentielles d'un pays comme le Canada?

[*Traduction*]

M. David Shipley: Nous avons pris du retard pour ce qui est de mettre en place un système de signalement instantané maintenant. Des organisations canadiennes vont informer les États-Unis de ce qui leur est peut-être arrivé, et nous n'en savons rien. Le fait qu'on ait insisté pour réglementer les secteurs relevant du gouvernement fédéral, comme le transport, les banques, l'énergie et les télécommunications est une bonne chose, mais le problème se situe souvent à l'extérieur des secteurs de compétence fédérale.

Les dispositions qu'a prises l'Europe ont établi certains seuils. Quelle est la taille des entreprises qui ont une incidence importante sur l'économie? Puis, l'Europe a établi des seuils relatifs à la participation de ces entreprises et à leurs rapports à ce sujet. C'est important parce qu'une petite et moyenne entreprise... En ce qui concerne Sunwing, c'est le fournisseur de TI responsable du système d'émission des billets qui a été touché aux États-Unis. Pas Sunwing, mais plutôt le fournisseur de TI.

Comment pouvons-nous accéder aux leçons apprises, et comment pouvons-nous les communiquer de façon à déceler les vulnérabilités et à les régler, et tirer parti de ces leçons? Nous devons passer outre à la culture du blâme lorsqu'il est question de cybersécurité. Cette organisation était une victime. Pourquoi? Comment pouvons-nous apprendre de cette situation? Par exemple, lorsqu'il est question de nos hôpitaux, comment pouvons-nous prévenir des attaques visant 100 autres hôpitaux après qu'un d'entre eux a été victime d'une attaque et ainsi nous améliorer?

● (1300)

[*Français*]

Mme Kristina Michaud: Merci.

Il me reste peu de temps, mais j'aborderais la question du Costa Rica, un pays beaucoup plus petit que le Canada. Il y a quelques semaines, le pays a dû décréter l'état d'urgence parce qu'il avait été infiltré par un groupe de pirates russes. Ce sont les ministères des Finances, de la Santé et du Travail, et d'autres encore, qui sont complètement paralysés.

À votre avis, peut-on craindre ce genre de chose au Canada? Sommes-nous, au contraire, suffisamment préparés et protégés?

[*Traduction*]

M. David Shipley: Nous avons été victimes d'une attaque de logiciels rançonneurs de la part de gangs russes. Nous devons nous améliorer à cet égard. La cryptomonnaie et le flux monétaire alimentent ce problème.

Le président: Merci.

Monsieur MacGregor, c'est à vous pour les deux minutes et demie restantes de la séance.

M. Alistair MacGregor: Merci, monsieur le président.

Monsieur Shipley, lorsque vous avez parlé de la relation qu'entretenait la Russie avec des organisations criminelles, cela m'a rappelé l'Angleterre, il y a quelques siècles, lorsque le pays entretenait des liens avec des corsaires afin qu'ils fassent son sale boulot.

Pour ce qui est du signalement obligatoire d'incidents qui ne concernent pas les secteurs relevant du gouvernement fédéral, le gouvernement fédéral entretient une relation avec les provinces, même avec la Fédération canadienne des municipalités, donc ces gouvernements infranationaux... En ce qui concerne le secteur privé, en fait, j'aimerais savoir... Je suis d'accord avec vous pour dire que c'est important, mais souvent, lorsque des organisations criminelles tiennent une entreprise en otage, une de leurs menaces les plus graves tient au fait de dire que si vous informez la police, ils vous retrouveront.

Comment pouvons-nous faire pour contourner cette menace précise? C'est ce qui a fait en sorte que les entreprises privées détestent s'en remettre aux autorités, parce qu'il s'agit d'une menace très réelle envers leurs organisations.

M. David Shipley: Au chapitre des obstacles auxquels font face les entreprises au moment de signaler un incident, le plus important est le fait que les entreprises d'assurance disent souvent: « Nous nous occupons de la façon de réagir à cette infraction. Il nous en coûte moins cher de payer la rançon. N'avisez pas la police. Taisez-vous. » Si vous êtes une entreprise cotée en bourse, cela peut avoir une incidence sur le prix de vos actions. Cette situation stresse beaucoup les avocats.

Nous devons modifier l'équation du risque. Il faut faire en sorte qu'il soit nécessaire de signaler un incident sans quoi il faudra en subir les conséquences. Puis tout à coup, les avocats, les assureurs et d'autres personnes diront: « Nous devons informer le CST et d'autres organisations », et vous modifiez la relation.

Si les criminels savent que des lois en place exigent que les entreprises communiquent avec nous, peut-être qu'ils iront ailleurs. Je suis du même avis que Mme Kayyem. Je crois que nous devons faire mieux, mais que tout ne sera pas parfait. Selon une vieille expression du Nouveau-Brunswick, qu'utilisait mon père à la blague, « je n'ai pas à courir plus vite que l'ours. J'ai juste à courir plus vite que toi. » La même chose s'applique à la cybersécurité. Nous devons seulement nous améliorer progressivement dans ce domaine.

Le signalement obligatoire change l'équation. Nous en avons besoin. Si nous nous en remettons aux provinces, vous allez avoir des provinces nanties et des provinces démunies sur le plan de la sécurité. Est-ce que c'est le genre de pays...? Il s'agit d'un problème de sécurité nationale, et nous devons composer avec lui. Nous sommes trop petits pour régler le problème sans le centraliser, donc nous devons le faire.

M. Alistair MacGregor: Oui, comme il s'agit d'une infraction criminelle, le droit pénal relève de nous. La source du problème transcende souvent les compétences provinciales, ce qui veut dire que c'est le gouvernement fédéral qui a compétence. Oui, le fait de l'inscrire dans des contrats d'assurance...

Le président: Monsieur MacGregor, vous êtes le dernier à parler.

M. Alistair MacGregor: Je vais m'arrêter là. Merci, monsieur le président.

Le président: J'aimerais remercier de tout cœur les témoins qui ont partagé leur expertise et l'ensemble de leurs connaissances qu'ils ont accumulées au cours des années. On remonte peut-être à 25 ou 30 ans, mais cette situation se passe maintenant... c'est un sujet courant et très actuel. Au nom du Comité, et de tous les parlementaires, j'aimerais vous remercier de nous avoir accordé de votre temps, de nous avoir fait profiter de votre point de vue et de vos connaissances.

Chers collègues, cela met fin à cette partie de la réunion. Bonne journée, tout le monde. On se revoit dans quelques jours, soit jeudi.

La séance est levée.

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

PERMISSION DU PRÉSIDENT

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

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

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

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

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

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

SPEAKER'S PERMISSION

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

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

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

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

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