CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

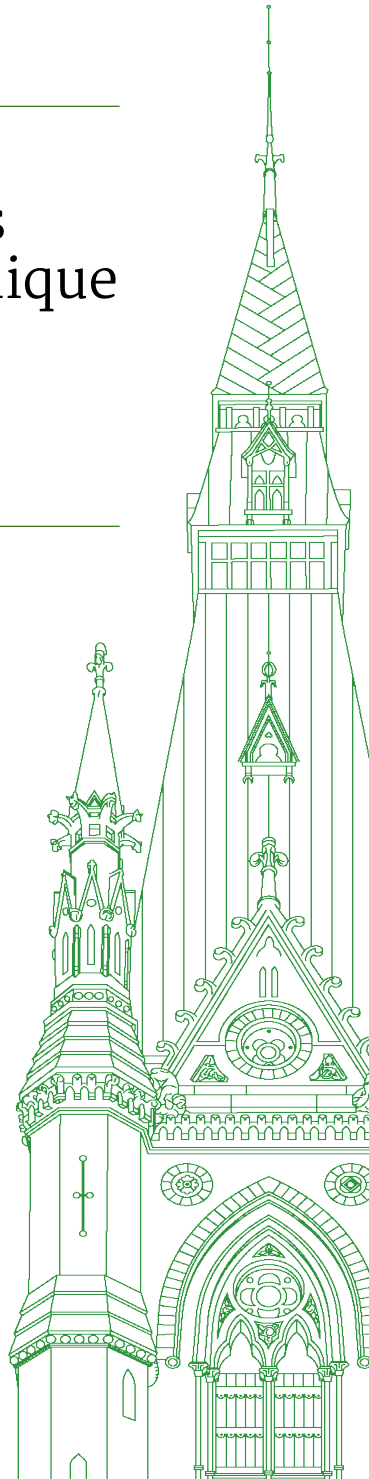
44e LÉGISLATURE, 1re SESSION

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

TÉMOIGNAGES

NUMÉRO 033

Le mardi 9 août 2022



Président : M. Pat Kelly

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le mardi 9 août 2022

● (1505)

[*Traduction*]

Le président (M. Pat Kelly (Calgary Rocky Ridge, PCC)): La séance est ouverte.

J'aimerais souhaiter à tous la bienvenue à la 33e séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. Conformément à l'alinéa 108 (3)h) du Règlement et à la motion adoptée par le Comité le mardi 26 juillet 2022, le Comité se réunit pour étudier les outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada.

La réunion d'aujourd'hui se déroule sous forme hybride, conformément à l'ordre de la Chambre du jeudi 23 juin 2022.

Aujourd'hui, nous recevons un groupe d'experts composé de trois témoins. Nous avons le plaisir d'accueillir Ronald Deibert, professeur en science politique et directeur, Citizen Lab, Munk School of Global Affairs and Public Policy, Université de Toronto. Nous accueillons également Brenda McPhail, directrice du Programme de la vie privée, de technologie et de surveillance, Association canadienne des libertés civiles. Nous attendons également Michel Juneau-Katsuya, chercheur sur les questions de sécurité nationale et de renseignement. Je crois savoir que nous sommes en train de régler quelques problèmes techniques que rencontre ce témoin. Nous allons donc entendre les déclarations préliminaires des deux autres témoins. Nous espérons bien sûr que notre troisième témoin se joindra à nous à temps pour pouvoir faire sa déclaration préliminaire.

Cela dit, je demanderais au professeur Deibert de commencer sa déclaration.

Vous avez la parole pendant un maximum de cinq minutes.

M. Ronald J. Deibert (professeur en science politique, et directeur, Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, à titre personnel): Merci, monsieur le président.

Je m'appelle Ron Deibert. Je suis professeur en science politique, ainsi que fondateur et directeur du Citizen Lab à la Munk School of Global Affairs and Public Policy de l'Université de Toronto.

Depuis 2001, les membres du Citizen Lab étudient les questions de sécurité de l'information, et l'un de leurs principaux domaines de recherche est l'industrie des logiciels espions mercenaires, dans laquelle des acteurs privés vendent des services de piratage aux gouvernements. Nous sommes largement reconnus comme l'une des principales autorités mondiales dans ce domaine.

Mon personnel et moi-même avons témoigné ou donné des séances d'information portant sur ce sujet à de nombreuses reprises à la Maison-Blanche des États-Unis, au Département d'État, au Congrès américain, au Parlement européen et à d'autres gouvernements. Je suis très heureux de m'exprimer à ce sujet pour la première fois devant un comité de la Chambre des communes du Canada.

Aujourd'hui, je souhaite mettre en lumière plusieurs thèmes qui ressortent de nos recherches.

Premièrement, l'industrie des logiciels espions mercenaires est très peu réglementée et s'étend rapidement. Le secteur manque de responsabilisation publique et de transparence. Elle prospère dans l'ombre du monde clandestin et s'élargit rapidement sans contrôle approprié.

Deuxièmement, nous avons documenté des préjudices et des abus importants dans presque toutes les administrations où des logiciels espions sont déployés. Les gouvernements utilisent de façon routinière des logiciels espions pour pirater la société civile, l'opposition politique, les journalistes, les avocats, les militants, les membres de leur famille et d'autres victimes innocentes, tant dans leur pays qu'à l'étranger, y compris des victimes qui vivent ici, au Canada.

Troisièmement, l'industrie des logiciels espions mercenaires n'est pas seulement une menace pour la société civile et les droits de la personne; elle menace aussi la sécurité nationale. Nous avons remarqué que les téléphones de certains chefs d'État et hauts fonctionnaires avaient été piratés par des logiciels espions. Il y a peu de temps, nous avons informé les autorités britanniques du piratage d'un appareil utilisé au 10, Downing Street, c'est-à-dire la résidence du premier ministre du Royaume-Uni. En bref, nos quelque 10 années de recherche montrent que l'industrie des logiciels espions est aujourd'hui l'une des menaces les plus graves qui pèsent sur la société civile, les droits de la personne et la démocratie.

La récente révélation de l'utilisation de logiciels espions par la GRC provoque de sérieuses inquiétudes.

Tout d'abord, les logiciels espions ne ressemblent pas à une mise sur écoute traditionnelle, mais plutôt à une mise sur écoute à la puissance mille. Les logiciels espions avancés sont à la surveillance ce que la technologie nucléaire est aux armes; ils représentent un bond en avant du point de vue du perfectionnement et de la puissance. Les dernières versions de ces logiciels permettent d'accéder silencieusement et sans entrave à l'ensemble du mode de vie d'une cible. Malgré les capacités de niveau nucléaire de ces logiciels, il est remarquable qu'ils n'aient fait l'objet d'aucun débat public au Canada, avant la récente révélation de la GRC.

Deuxièmement, le seuil d'utilisation, de surveillance, de transparence et de responsabilisation publique doit être beaucoup plus élevé que pour une écoute électronique traditionnelle. Cela est d'autant plus important que la GRC et d'autres organismes de sécurité au Canada ont un passé bien documenté en matière d'emplois abusifs de la surveillance et de pratiques discriminatoires.

Troisièmement, nous avons besoin de transparence quant aux fournisseurs auprès de qui les organismes canadiens se procurent cette technologie. Hier, le ministre de la Sécurité publique n'a pas voulu reconnaître devant notre comité le ou les fournisseurs auprès de qui le gouvernement canadien a acheté des logiciels espions. Il n'y a absolument aucune raison de ne pas divulguer cette information, et il y a un grand nombre de bonnes raisons de le faire. Notre approvisionnement devrait être transparent et régi par des règles relatives aux fournisseurs, afin que nous ne traitions pas avec des entreprises dont les clients comprennent des gouvernements étrangers qui menacent les valeurs et la sécurité du Canada — et que nous ne contribuions pas à enrichir ces entreprises.

Quatrièmement, l'existence même de cette technologie pose de graves problèmes de sécurité publique. Les logiciels espions mercenaires reposent sur la découverte de failles logicielles dont les fournisseurs de logiciels eux-mêmes ne sont pas conscients ou qu'ils n'ont pas corrigées. L'utilisation même de cette technologie alimente un marché qui exploite l'insécurité collective de tous nos appareils. Dans sa forme actuelle, le processus global que le Canada met en œuvre pour évaluer les enjeux de ces compromis est faible et opaque.

Cinquièmement, la révélation discrète de la GRC donne un très mauvais exemple au reste du monde. Le gouvernement canadien prétend protéger les droits de la personne et défendre la primauté du droit et la démocratie dans le monde entier. En adoptant cette technologie sans lancer un débat public ni imposer des limites appropriées, nous signalons essentiellement au monde entier que nous ne nous soucions pas vraiment de ces principes.

Je terminerai mon intervention en formulant sept recommandations précises.

Premièrement, il faut tenir des audiences publiques sur les dangers liés à l'industrie des logiciels espions mercenaires, d'autant plus que des Canadiens ont été victimes de ces dangers.

Deuxièmement, si des organismes canadiens doivent utiliser des logiciels espions, une consultation publique devrait être organisée et le gouvernement devrait élaborer un cadre juridique qui respecte la Charte et le droit international en matière de droits de la personne.

Troisièmement, le Canada devrait mettre en place de solides contrôles des exportations pour l'industrie canadienne de la surveillance. À l'heure actuelle, il n'y en a aucun.

Quatrièmement, le Canada devrait pénaliser les fournisseurs de logiciels espions qui sont connus pour faciliter les violations des droits de la personne à l'étranger, et ces pénalités devraient suivre le modèle américain.

Cinquièmement, des membres des plus hauts échelons du gouvernement canadien, comme le premier ministre, le ministre de la Sécurité publique et la ministre des Affaires étrangères, doivent faire des déclarations claires et fermes indiquant que nous prenons cette menace au sérieux.

Sixièmement...

● (1510)

Le président: Vous avez largement dépassé le temps qui vous était imparti. Veuillez énoncer rapidement les deux dernières recommandations.

M. Ronald J. Deibert: Sixièmement, le Canada devrait imposer aux personnes ayant travaillé dans nos organismes de sécurité une interdiction à vie de travailler avec des sociétés de logiciels espions mercenaires.

Enfin, le Canada devrait rendre publiques les entreprises avec lesquelles il passe des contrats et élaborer des lignes directrices pour les organismes canadiens afin qu'ils ne passent jamais de contrats avec des entreprises liées à des violations des droits de la personne à l'étranger.

Merci, monsieur le président. Je m'excuse d'avoir dépassé le temps qui m'était imparti.

Le président: Ce n'est pas grave.

Je vais maintenant demander à Mme McPhail de commencer sa déclaration préliminaire.

Mme Brenda McPhail (directrice, Programme de la vie privée, de technologie et de surveillance, Association canadienne des libertés civiles): Je vous remercie d'avoir invité l'Association canadienne des libertés civiles à comparaître devant vous aujourd'hui. Je suis reconnaissante au Comité d'avoir entrepris cette étude sur l'utilisation par la GRC de la technologie d'enquête sur appareil, car il s'agit d'une question d'intérêt national qui est aussi le symptôme d'un problème plus vaste de surveillance et de responsabilisation inadéquates de la police lorsqu'elle acquiert et utilise une technologie de surveillance avancée.

Les révélations concernant les outils d'enquête embarqués (OEE) ne sont que les dernières d'une série de révélations semblables provoquées par les médias qui concernent des techniques invasives, allant de la surveillance des médias sociaux aux simulateurs de sites cellulaires, en passant par une reconnaissance faciale illégale effectuée à l'aide de produits de la société Clearview AI. Il ne s'agit pas d'un cas isolé, mais plutôt d'un modèle qui révèle une crise en matière de responsabilisation.

Le secret opérationnel est un besoin légitime dans le cadre d'enquêtes particulières. Le secret entourant les politiques qui s'appliquent à des catégories de technologies de surveillance dangereuses n'est pas légitime au sein d'une démocratie. Nous ne devons pas permettre aux organismes chargés de l'application de la loi de confondre l'un avec l'autre afin d'éviter de rendre des comptes.

Pourquoi ces technologies sont-elles dangereuses du point de vue de la société civile? Comme le Comité est conscient des risques fondamentaux qu'elles présentent pour le droit à la vie privée, je vais donc me concentrer sur trois autres raisons.

Premièrement, nos organismes gouvernementaux encouragent une industrie qui est connue pour privilégier les profits au détriment des droits de la personne et pour alimenter les pires impulsions des gouvernements autoritaires. Je travaille avec un réseau d'organisations mondiales de défense des libertés civiles dans lequel nombre de mes collègues considèrent le Canada comme un modèle à suivre en ce qui concerne les questions d'application de la loi et les procédures établies. Ce genre de révélations nuit à notre réputation internationale, non seulement au niveau des gouvernements, mais aussi sur le terrain.

Deuxièmement, comme l'a fait remarquer le professeur Deibert, l'utilisation de ces outils encourage les forces de l'ordre à exploiter les vulnérabilités des technologies dont nous dépendons tous, au lieu de contribuer à corriger ces vulnérabilités. Nous savons depuis un certain temps que le CST a des responsabilités contradictoires en ce qui concerne son mandat cybernétique actif et sa responsabilité en matière de protection de notre cyberinfrastructure. Nous savons maintenant que la GRC fait face à un conflit semblable. Cela rend la vie de tous un peu moins sécuritaire chaque jour, au nom de la sécurité publique.

Enfin, il y a une question de procédure établie. Vos témoins d'hier ont fait remarquer que l'une des conditions d'utilisation de la technologie est la signature d'une entente détaillant les façons dont la technologie doit être protégée. Quelle est l'incidence de cette entente sur les divulgations judiciaires? Est-ce qu'il arrive que des procès ne soient pas intentés parce qu'ils révéleraient des détails de la technologie? En d'autres termes, comment le secret opérationnel compromet-il la quête de la justice?

Ce sont là quelques-uns des problèmes posés par la technologie. Quelles sont les éventuelles solutions à ces problèmes?

Tout d'abord, je crois vraiment que nous avons besoin d'un moratoire. Cette étude n'est que le début d'une importante conversation publique que nous devons avoir au Canada. S'il est vrai que cette technologie est une option de dernier recours, une brève interruption de son utilisation ne peut constituer un grand risque pour la sécurité publique — certainement pas si l'on compare ce risque aux droits à la vie privée et à l'application régulière de la loi qui sont en jeu, ainsi qu'aux répercussions sociales et diplomatiques qui découlent du fait que le gouvernement canadien tolère la vente et l'utilisation de logiciels espions.

Il faut donc revenir à l'essentiel, et la question fondamentale n'est pas de savoir « Comment s'assurer que la GRC ou tout autre organisme utilise ces outils de façon légale? » Il faut plutôt se poser la question suivante: « L'utilisation de ces outils est-elle nécessaire, proportionnée et conforme aux valeurs canadiennes? »

Vous ne serez probablement pas surpris d'apprendre que je pense que ce n'est pas le cas. Je crois que, comme l'Europe et les États-Unis l'ont fait, nous devrions inclure la possibilité d'interdire la vente de ce type de technologie d'espionnage à des États dans les conversations que nous devons avoir, mais s'il est démocratiquement débattu et déterminé que l'utilisation de la technologie est adaptée à un objectif étroit, la deuxième question que nous devrons alors nous poser est celle de savoir comment nous pouvons rendre la notion d'utilisation légale de la technologie plus significative en mettant à jour nos lois en vue de régir de manière appropriée les décisions d'achat et d'utilisation de ces technologies, et de fournir une transparence et une responsabilisation suffisantes pour gagner la confiance du public.

Pour que ces lois soient suffisantes, nous devons avoir des contrôles et des limites d'importation et d'exportation rigoureux et appliqués efficacement. Nous avons besoin d'un système dans lequel les décisions relatives à l'utilisation de technologies controversées susceptibles de porter atteinte aux droits ne peuvent plus être prises en coulisses. Pour ce faire, nous avons besoin non seulement d'évaluations obligatoires des facteurs relatifs à la vie privée, mais nous devons également envisager de créer un organe consultatif véritablement indépendant, qui travaille avec une transparence appropriée et qui est précisément chargé de fixer et d'évaluer des normes nationales pour l'acquisition et l'utilisation des technologies de surveillance, comme cela a été fait dans l'État de New York.

Nous devons également créer des obligations de produire des rapports publics sur l'utilisation des OEE. Le « Rapport annuel sur la surveillance électronique », qui a été mentionné à plusieurs reprises à titre de mesure de responsabilisation, est insuffisant. Les outils utilisés pour assurer cette surveillance sont importants. C'est la raison pour laquelle nous discutons actuellement de cette question. Pourtant, dans ce rapport, on se contente de fournir des statistiques sur toute surveillance audio ou visuelle. Cela nous amène à un dernier point.

Entre 2016 et 2020, une seule demande de mandat, parmi les 331 demandes mentionnées dans ce rapport, a été refusée. Cela laisse entendre que nous avons besoin qu'un amicus d'intérêt public soit présent pendant le traitement de ces demandes, afin de fournir une contrepartie aux positions de la police. Il y a d'autres problèmes et d'autres solutions à aborder, mais mes cinq minutes sont écoulées, alors j'attends vos questions.

● (1515)

Le président: Merci.

Bien que je n'aperçoive pas Michel Juneau-Katsuya à l'écran, permettez-moi de demander s'il s'est joint à nous.

Non? Communiquons-nous cependant avec lui?

Nous communiquons avec lui. D'accord.

Eh bien, il se peut que nous n'entendions pas la déclaration préliminaire du témoin Michel Juneau-Katsuya.

Nous allons devoir amorcer nos séries de questions.

Monsieur Bezan, je vous demanderais de lancer le processus.

M. James Bezan (Selkirk—Interlake—Eastman, PCC): Merci, monsieur le président.

Je tiens à remercier nos témoins de s'être joints à nous aujourd'hui et de nous faire profiter de leurs compétences dans ce domaine.

Je m'adresse maintenant au professeur Deibert et à Mme McPhail. Vos organisations ont-elles étudié en profondeur les fournisseurs qui sont potentiellement utilisés ici, au Canada — c'est-à-dire ceux qui vendent des logiciels espions?

M. Ronald J. Deibert: Qui de nous deux devrait répondre en premier?

M. James Bezan: C'est à vous d'en décider.

Professeur, puisque votre microphone est activé, pourquoi ne lanceriez-vous pas le débat?

M. Ronald J. Deibert: Bien sûr.

Nous avons largement répertorié les fournisseurs de logiciels espions du monde entier. Malheureusement, la réponse à cette question manque de transparence ici, au Canada. Aucun d'entre nous ne dispose d'informations publiques sur les fournisseurs auprès desquels le gouvernement s'approvisionne. Comme je l'ai mentionné au cours de la formulation de mes observations, cela est très problématique.

Comme vous l'avez constaté hier, lorsqu'on lui a posé cette question de manière pointue, le ministre de la Sécurité publique a refusé d'y répondre. Je ne pense pas que ce soit là une réponse légitime.

M. James Bezan: Madame McPhail...?

Mme Brenda McPhail: Nous n'avons pas mené de telles recherches.

M. James Bezan: D'accord.

Madame McPhail, au cours de votre déclaration préliminaire, vous avez mentionné que la GRC n'a peut-être pas entamé des poursuites relatives à certaines affaires criminelles ou à certaines menaces pour la sécurité nationale, parce qu'elle aurait été forcée de révéler qu'elle avait utilisé des OEE. Avez-vous des preuves à cet égard, à savoir que les agents préfèrent ne pas entamer de poursuites afin de protéger la technologie?

Mme Brenda McPhail: Il y a eu dans le passé une affaire appelée Projet Clemenza, où il a été révélé qu'un certain nombre de poursuites avaient été abandonnées au lieu de révéler le fait qu'une clé permettant d'accéder à des communications cryptées avait été obtenue par les forces de l'ordre. C'est le seul exemple que je connaisse, mais la mention d'un accord particulier, que vos témoins ont décrit hier comme une limite à l'utilisation des outils et à ce qui pouvait être dit à leur sujet en public, suscite des inquiétudes quant aux divulgations appropriées devant les tribunaux.

M. James Bezan: Pensez-vous que, si la GRC n'a pas entamé de poursuites, c'est parce qu'elle ne disposait pas d'un mandat approprié pour recueillir des renseignements sur ces personnes, ou qu'elle l'a fait en vertu d'autres mécanismes, comme ceux liés à la sécurité nationale?

Mme Brenda McPhail: Ce qu'on m'a dit m'a amené à comprendre que cela avait été fait pour protéger l'utilisation de l'outil, et non parce que les mandats appropriés n'avaient pas été obtenus.

M. James Bezan: D'accord.

Vous savez, souvent, lorsque je voyage à l'étranger, des fonctionnaires du ministère des Affaires étrangères ou du ministère de la Défense nationale m'informent de la possibilité que mon téléphone cellulaire soit piraté, et que la caméra et le microphone puissent être activés à tout moment. Croyez-vous qu'en tant que parlementaires ou en tant que personnes qui travaillent sur la Colline du Parlement, nous devons prendre des précautions supplémentaires ici, au Canada, étant donné que les téléphones que le gouvernement nous fournit pourraient être piratés non seulement par des acteurs étrangers, mais aussi par des acteurs nationaux?

J'adresse la question à Mme McPhail et au professeur Deibert.

Mme Brenda McPhail: Je pense que cette possibilité est préoccupante, mais je pense aussi que le professeur Deibert est la personne la mieux préparée à répondre à cette question.

M. James Bezan: La parole est à vous, professeur.

M. Ronald J. Deibert: Oui, je pense que c'est une préoccupation majeure. Le fait est que vous possédez des appareils qui sont très invasifs et qui ont tendance à être mal sécurisés dans l'ensemble, étant donné la nature de l'écosystème numérique dans lequel nous vivons. Ces appareils coexistent avec une industrie qui, comme je l'ai décrit, dépense des millions de dollars pour trouver des failles logicielles sans les divulguer aux fournisseurs, afin de pouvoir offrir ce piratage sous forme de services. Nous avons également documenté de nombreux cas de fonctionnaires et même de chefs d'État dont les appareils ont été piratés avec les logiciels espions les plus avancés. Comme je l'ai mentionné dans ma déclaration préliminaire, nous avons observé un dispositif de piratage au 10, Downing Street, c'est-à-dire la résidence du premier ministre du Royaume-Uni, et nous l'avons signalé aux autorités britanniques.

En vérité, personne n'est à l'abri des types de logiciels espions les plus avancés. Il n'y a pas de réglementation internationale dans ce secteur. Ces logiciels prolifèrent largement auprès des gouvernements du monde entier.

● (1520)

M. James Bezan: Professeur, d'après les recherches que vous avez menées, croyez-vous que, même si c'est contraire à l'éthique, des employeurs, y compris le gouvernement du Canada, pourraient obtenir l'autorisation d'utiliser des logiciels espions pour surveiller des employés et des personnes d'intérêt qui utilisent des appareils fournis par le gouvernement ou par l'entreprise? Y aurait-il une échappatoire dans la Loi qui leur permettrait d'éviter d'avoir à demander des mandats, parce qu'il s'agirait d'un bien appartenant à l'employeur?

M. Ronald J. Deibert: Eh bien, c'est là une question intéressante. Je sais qu'il existe toutes sortes de règles. Habituellement, des divulgations sont faites lorsque quelqu'un utilise un appareil au sein d'une institution, qu'elle soit publique ou non. Si des divulgations n'ont pas été faites, je dirais certainement que cette surveillance serait grandement contraire à l'éthique et peut-être même illégale.

Je pense que Mme McPhail serait mieux placée pour répondre à cette question sur le plan juridique.

Le président: Madame McPhail, vous disposez de quelques secondes si vous souhaitez répondre à la question.

Mme Brenda McPhail: Je pense qu'un certain nombre d'instruments juridiques distincts interagiraient et seraient pertinents dans cette situation. Il faudrait les examiner soigneusement afin de déterminer les types d'échappatoires qui pourraient exister.

Le président: Merci.

Nous allons maintenant céder la parole à Mme Hepfner pendant un maximum de six minutes.

Mme Lisa Hepfner (Hamilton Mountain, Lib.): Merci, monsieur le président.

Je remercie nos témoins de s'être joints à nous aujourd'hui et d'avoir apporté leur témoignage.

Monsieur Deibert, je voudrais revenir un peu sur votre déclaration préliminaire. Vous avez parlé de la façon dont les gouvernements utilisent des logiciels espions pour pirater les téléphones des gens. Vous avez mentionné que cela s'est produit ici, au Canada. Je me demande si vous pourriez nous fournir un peu plus d'informations sur les cas dont vous avez eu connaissance. Quels gouvernements sont impliqués dans le piratage? Quels cas avons-nous observés ici, au Canada?

M. Ronald J. Deibert: Certainement. Je vous remercie de votre question.

En 2018, nous avons constaté que l'Arabie saoudite entreprenait des activités d'espionnage. Nous avons pu observer, compte tenu de notre surveillance du réseau, qu'il y avait un appareil piraté au Québec. Nous avons finalement découvert que la personne dont l'appareil avait été piraté était un résident permanent canadien, nommé Omar Abdulaziz, qui était un ami très proche et un confident de Jamal Khashoggi. Nous avons publié notre rapport le 1er octobre 2018. Malheureusement, dès le lendemain, Jamal Khashoggi a été appréhendé et brutalement exécuté au consulat saoudien de Turquie.

Nous avons également documenté en détail le fait que les téléphones d'autres réfugiés et immigrants canadiens ont été ciblés ou piratés à l'étranger par des gouvernements étrangers, dans le cadre d'un nombre croissant de cas que nous qualifions de « répression numérique transnationale ».

En résumé, les Canadiens ne sont certainement pas à l'abri de ce risque mondial qui ne cesse de croître, et c'est précisément la raison pour laquelle je pense que nous devons entamer cette conversation très sérieuse, avec une approche beaucoup plus complète que celle que nous avons adoptée jusqu'à maintenant.

Mme Lisa Hepfner: D'accord. Eh bien, je conviens que c'est une bonne conversation à avoir, alors qu'entendez-vous par une approche plus complète? Comment pouvons-nous nous protéger contre ces mauvais acteurs internationaux?

M. Ronald J. Deibert: Tout d'abord, comme je l'ai indiqué dans mes recommandations, je pense que nous devons comprendre que nous avons l'obligation de faire plus que de prononcer des paroles à ce sujet. En fait, je souhaiterais même que nous prononcions des paroles à ce sujet. En vérité, je n'ai rien entendu de la part du ministère des Affaires étrangères ou du premier ministre qui équivaut aux déclarations qui ont été faites, juste pour vous donner un exemple, aux États-Unis et par l'administration Biden. Des déclarations percutantes ont été faites aux plus hauts échelons de la Maison-Blanche, du Département d'État et du Département de la Justice. Ils ont mené des enquêtes et ont commencé à pénaliser des entreprises, reconnaissant ainsi la gravité à l'échelle mondiale de ce problème qui relève à la fois des droits de la personne et de la sécurité nationale.

Je pourrais réitérer mes recommandations, mais je pense que nous devons commencer par remédier au fait qu'il n'y a pas de contrôles des exportations pour les entreprises canadiennes qui vendent des technologies de surveillance à l'étranger. Il faut que cela change. Nous devons être plus transparents quant à savoir auprès de qui nous nous procurons cette technologie. Comme vous avez pu le constater hier, le ministre de la Sécurité publique n'a même pas voulu reconnaître auprès de qui il achète cette technologie. Il n'y a aucune raison liée à la sécurité opérationnelle pour laquelle nous ne devrions pas divulguer cette information, et il y a de nombreuses bonnes raisons pour lesquelles nous devrions le faire. C'est parce que nos achats sont un levier pour l'industrie. Si nous consacrons des millions de dollars à l'achat de cette technologie, qui est très coûteuse, soit dit en passant, nous pouvons imposer des conditions aux entreprises et déclarer que nous n'achèterons pas des produits auprès d'entreprises qui ont été largement associées à des violations flagrantes des droits de la personne, tant à l'étranger qu'au Canada, à moins qu'elles ne respectent certaines normes.

● (1525)

Mme Lisa Hepfner: La GRC nous a dit qu'elle révélerait des secrets au milieu criminel si elle rendait publique la technologie qu'elle utilise. Je ne sais pas sur quoi s'appuie ce raisonnement.

Ce que nous savons, ou ce que dit la GRC, c'est qu'elle a utilisé cette technologie pour des raisons précises et ciblées comme le fait d'enquêter sur le terrorisme, sur des meurtres, sur des enlèvements ou sur des trafics. Cela a été fait avec une importante surveillance judiciaire, après avoir obtenu de nombreux mandats requis et avec la participation de services de police spécialisés. Et ce, depuis 2017.

Comment réagissez-vous à cette déclaration, compte tenu de ce que son étude nous a appris et de ce que nous avons entendu dire au sujet de l'utilisation de cette technologie par la GRC jusqu'à maintenant?

M. Ronald J. Deibert: Je dirais que la sécurité est un enjeu très sérieux, et que nous devons tous nous protéger des menaces que vous décrivez. Nos forces de l'ordre, nos services de renseignement et nos forces armées doivent être modernisés et équipés de manière adéquate, et il doit y avoir un contrôle judiciaire. Il est rassurant d'apprendre que la technologie a été utilisée pour ce type de cas et qu'un mandat a été obtenu pour autoriser son utilisation.

Ce n'est pas parce qu'on nous dit qu'un mandat a été obtenu qu'il s'agit d'une baguette magique qui fait disparaître tout le reste, et que nous devrions dire: « Ne cherchez pas plus loin. » Comme je l'ai indiqué, il n'y a vraiment aucune raison de ne pas divulguer les fournisseurs auprès desquels vous achetez cette technologie.

Nous ne voulons pas que l'argent des contribuables soit versé à certaines de ces sociétés mercenaires et malhonnêtes qui contribuent à des violations des droits de la personne à l'étranger et à des problèmes de sécurité nationale ici, au Canada.

Mme Lisa Hepfner: Je suppose que tout cela revient à dire qu'il n'y a aucune preuve que le gouvernement canadien a utilisé ce logiciel espion. Tout ce qui figure dans le compte rendu, c'est le fait que la GRC a utilisé la technologie dans certaines circonstances, sous contrôle judiciaire, pour lutter contre des crimes précis et graves.

M. Ronald J. Deibert: Si je compare ce que j'ai entendu hier à ce que j'ai lu dans les actualités, j'entends parler de quelque chose de différent.

Premièrement, cette révélation a semblé avoir été faite un peu de travers. Elle n'a pas vraiment été faite de manière franche. J'ai également entendu dire que le Commissariat à la protection de la vie privée n'avait pas été informé de cette affaire. De plus, au cours des deux derniers jours, les chiffres mentionnés ont changé.

Comme vous avez entendu ma collègue, Mme McPhail, le dire, les forces de l'ordre de notre pays ont l'habitude d'utiliser des techniques d'enquête et des technologies de surveillance, et de les divulguer seulement après coup. Ce n'est pas ainsi qu'on bâtit la confiance du public dans les forces de l'ordre d'un pays. Nous sommes meilleurs que cela.

Le président: Merci.

Cela dit, nous allons maintenant donner la parole à M. Villemure.

[*Français*]

Monsieur Villemure, vous avez la parole pour six minutes.

M. René Villemure (Trois-Rivières, BQ): Je vous remercie, monsieur le président.

Je m'adresserai d'abord à M. Deibert, puis à Mme McPhail.

Nous entreprenons cette étude afin de maintenir la confiance de la population, envers la GRC dans ce cas-ci. Comme nous l'étions un peu hier, la population est obligée de croire ce que la GRC nous a dit, parce qu'il n'y a pas de moyen de creuser davantage la question.

Afin de pouvoir mieux informer la population, j'aimerais vous poser une question, M. Deibert.

Pouvons-nous faire confiance lorsque nous sommes obligés de faire confiance?

[*Traduction*]

M. Ronald J. Deibert: Ma réponse à cette question consisterait à évoquer quelqu'un dont vous vous souviendrez — et nous montrons notre âge en ce moment —, à savoir Ronald Reagan, qui, en réponse à Mikhaïl Gorbatchev, a déclaré: « faisons confiance, mais vérifions ». Je pense que cela s'applique à tous nos organismes de sécurité. Dans une démocratie libérale, il est essentiel de disposer de garanties solides, de mécanismes de surveillance et d'un processus public de reddition de comptes, ainsi que de faire preuve de transparence.

Ce que nous voyons en ce moment est clairement un échec. Si vous comparez cela avec ce qui se passe dans d'autres pays, nous ne donnons pas un très bon exemple. Ce comportement cadre avec celui de certaines des démocraties imparfaites du monde entier.

Je pense que nous devons tendre un filet beaucoup plus robuste sous l'ensemble de ces outils si nous voulons utiliser ce type de technologie, qui, soit dit en passant, est comme un pas de géant en matière de capacités. Ce dont nous parlons en ce moment est très différent d'une mise sur écoute, parce qu'un tel dispositif permet de surveiller tous les aspects de la vie d'une personne et de son entourage.

Comme je l'ai dit au cours de ma déclaration, il s'agit d'une technologie de surveillance de niveau nucléaire. Nous avons donc besoin de mesures de protection appropriées à la hauteur de ce perfectionnement et de cette puissance.

● (1530)

[*Français*]

M. René Villemure: Ainsi, vous ne serez pas d'accord avec…

[*Traduction*]

Le président: Monsieur Villemure, j'ai arrêté votre temps, et je vous offre la possibilité de poursuivre votre intervention maintenant ou de faire une pause. Il vous restera quatre minutes et 10 secondes, et nous pourrons passer directement à la déclaration préliminaire de M. Juneau-Katsuya.

M. René Villemure: Nous entendrons la déclaration, je suppose.

Le président: C'est à vous de choisir.

M. René Villemure: Veuillez passer à la déclaration.

Le président: Je voudrais maintenant souhaiter la bienvenue à notre troisième témoin. J'espère que nous avons résolu tous nos problèmes techniques.

Bienvenue à la séance du Comité. Je vous autorise maintenant à faire votre déclaration préliminaire pendant un maximum de cinq minutes.

M. Michel Juneau-Katsuya (Expert et chercheur sur les questions de sécurité national et de renseignement, à titre personnel): Merci beaucoup.

[*Français*]

Je vous prie de m'excuser pour le retard, qui a été occasionné par des problèmes techniques.

Je vous remercie, monsieur le président et membres du Comité, de m'avoir invité à comparaître devant vous et de me donner l'occasion de m'adresser à vous au sujet d'une question importante, qui en engendre beaucoup d'autres.

D'entrée de jeu, j'aimerais résumer ma pensée. Celle-ci est basée sur mon expérience, qui s'échelonne sur plus de 40 ans au service de cette nation et dans le secteur privé. Cela fait aussi partie de mes recherches et du travail que j'ai fait dans le domaine de la sécurité nationale.

Ce qui est présenté au cœur de votre réflexion, c'est la pertinence, la légalité, la légitimité et la reddition de comptes en ce qui a trait à l'utilisation d'une ou des technologies permettant d'intercepter des conversations ou d'obtenir des informations qui peuvent être protégées par la Loi sur la protection des renseignements personnels et la vie privée.

Je tiens, dès maintenant, à souligner l'importance de la protection de la vie privée telle qu'elle est définie par la Charte et les lois canadiennes. Cette protection est l'une des pièces centrales d'une saine démocratie et, sans elle, il n'y a pas de démocratie possible.

Cela dit, je tiens à mettre en avant trois points qui sont au centre de mon témoignage, et sur lesquels je vais revenir.

Premièrement, en matière d'enquête dans le domaine de la criminalité ou de la sécurité nationale, on ne peut faire valoir l'adage selon lequel « la fin justifie les moyens ».

Deuxièmement, les joutes partisanes n'ont pas leur place dans un tel débat, et c'est le fruit de votre travail collectif qui apportera une meilleure protection à notre démocratie et à nos concitoyens.

Troisièmement, il a été conféré à ce comité une grande responsabilité morale et éthique pour ce qui est de fournir dans le cadre juridique les outils nécessaires pour que les hommes et les femmes qui sont chargés de nous protéger puissent le faire adéquatement dans le respect des fondements de notre système juridique.

[*Traduction*]

Mon premier point est que toute personne responsable de la sécurité collective tombe dans un piège majeur si elle croit que la fin justifie les moyens. C'est la tromperie la plus dangereuse que les agents chargés de l'application de la loi affrontent dans le dédale de la bureaucratie et des systèmes judiciaires. Soucieux d'accomplir leur travail de protection et désireux d'arrêter les criminels et les terroristes prêts à nous nuire, certains agents peuvent être tentés de contourner la loi.

Notre propre histoire du Canada nous enseigne les erreurs des années 1960 et 1970, lorsque la GRC a été chargée d'arrêter des agents communistes ou des séparatistes fanatiques. Au nom de notre protection, les agents de la GRC ont enfreint la loi, croyant faire ce qu'il fallait. Ils ont été induits en erreur, et ils ont eu tort.

J'ai écouté et prêté attention aux témoignages qui vous ont été apportés au cours des derniers jours. Je n'ai pas vu ni entendu l'histoire se répéter. J'ai vu des agents qui, selon moi, tout en subissant la pression de ne pas mettre en péril des capacités opérationnelles ou tactiques, répondaient à vos questions du mieux qu'ils pouvaient et dans la mesure du possible. Grâce à votre important travail, il est évident que nous pourrons renforcer le processus d'approbation en améliorant la consultation avec le commissaire à la protection de la vie privée, les mécanismes de rapport et d'évaluation, et la Loi elle-même.

En outre, j'ai été heureux d'entendre dire que le système judiciaire a maintenu en place les freins et les contrepoids. C'est une bonne nouvelle, et cela nous permet d'espérer que nous sommes sur la bonne voie en vue d'améliorer notre système démocratique et notre processus de reddition de comptes.

● (1535)

[*Français*]

Le deuxième point, que j'ai évoqué plus tôt, m'inquiète davantage, car j'ai observé des comportements de certains membres du Comité qui sont préoccupants. Poser des questions, et même des questions difficiles, c'est le travail et la responsabilité des membres du Comité. Cependant, un principe directeur doit dominer: vous vous devez de protéger et de promouvoir les intérêts de cette nation, et non pas les intérêts partisans de vos visées politiques. Si vous avez des questions qui touchent les capacités techniques, tactiques ou stratégiques, il faut les poser à huis clos.

[*Traduction*]

N'oublions pas que les audiences du Comité sont publiques. Certains malfaiteurs, qu'ils soient des criminels ou des agents étrangers, écoutent ces délibérations et prennent des notes. En posant des questions dans lesquelles on insiste pour obtenir, par exemple, le pays d'origine d'une technologie qui doit rester secrète, on sert sur un plateau d'argent les moyens pour les malfaiteurs de contrer les capacités tactiques. De plus, en continuant de faire de fausses allégations de surveillance de masse, alors que rien ne prouve que cette surveillance existe, on induit les Canadiens en erreur, et on divise notre société. Trente-neuf cas et 41 dispositifs répartis sur plus de cinq ans ne constituent pas une surveillance de masse.

[*Français*]

Comme je l'ai mentionné au début de mes remarques, j'observe et j'analyse les menaces dirigées contre la société et nos citoyens et citoyennes depuis plus de 42 ans. J'ai été l'un de ceux et celles qui se sont engagés corps et âme afin de protéger notre pays et ses habitants en servant dans les rangs. J'ai vécu les frustrations et les succès relativement à nos enquêtes et à nos efforts pour empêcher les criminels, les espions et les terroristes de nous faire du mal individuellement ou collectivement. Je ne peux pas vous décrire avec assez de justesse et de rigueur les vagues d'émotions qui habitent les enquêteurs lorsqu'un « pas bon » gagne parce qu'il a profité d'une imperfection de notre système démocratique ou légal.

Hier, M. Philippe Dufresne, vous a parlé de...

[*Traduction*]

Le président: Je vais devoir vous demander de conclure, car vous avez considérablement dépassé le temps qui vous était imparti.

M. Michel Juneau-Katsuya: Il me reste trois paragraphes à lire.

[*Français*]

Je vous remercie.

[*Traduction*]

Le président: Vous pourriez peut-être les résumer.

M. Michel Juneau-Katsuya: D'accord, je vais reprendre ma déclaration.

M. Dufresne lui-même a souligné hier l'importance de mettre l'accent sur l'intérêt public ou de travailler à la protection de l'intérêt public. La confiance est aujourd'hui plus cruciale que jamais, tant pour notre système démocratique, que vous représentez, que pour les forces de l'ordre et les organismes de sécurité qui travaillent dur pour nous protéger.

[*Français*]

Je vous remercie de votre attention, et j'espère que vous ne me tiendrez pas rigueur des commentaires et avertissements que j'ai formulés; ils étaient nécessaires.

[*Traduction*]

Votre travail joue un rôle important dans la correction de ces tendances et dans la mobilisation de l'attention accrue que la population réclame.

Le président: Merci. Je vais vraiment devoir laisser M. Villemure reprendre ses questions.

Vous avez quatre minutes et 10 secondes pour le faire. La parole est à vous, monsieur Villemure.

M. Michel Juneau-Katsuya: C'est dommage, car c'était un bon exposé.

Des députés: Oh, oh!

Le président: Je vous crois, mais notre temps est...

[*Français*]

M. René Villemure: Je vous remercie, monsieur le président.

Je discutais justement de la confiance avec M. Deibert.

Je reviens à mon point principal. Les agissements de la GRC sont-ils de nature à préserver la confiance ou, au contraire, à semer le doute?

M. Michel Juneau-Katsuya: La question s'adresse-t-elle à moi, monsieur Villemure?

M. René Villemure: Oui, commençons par vous.

M. Michel Juneau-Katsuya: Je crois que les actions de la GRC sont effectivement importantes pour essayer de gagner et de conserver la confiance du grand public. Les mécanismes de reddition de comptes et de consultation ainsi que les mécanismes juridiques en place sont nécessaires pour conserver et pour améliorer cette confiance.

Je crois que nous avons appris des diverses situations que nous avons vécues antérieurement. Les réponses qui ont été fournies hier, et surtout les pistes de réflexion qui ont été fournies par M. Dufresne ou par les autres intervenants, sont d'excellentes pistes pour aider le Comité à faire les bonnes recommandations.

M. René Villemure: Je vous remercie beaucoup.

Monsieur Deibert, pour le bien de la population générale, qui ne connaît pas bien tous les concepts, pourriez-vous décrire ce que peut faire un logiciel espion?

[*Traduction*]

M. Ronald J. Deibert: Nous étudions de nombreux types de logiciels espions, et les plus perfectionnés permettent un accès permanent à l'appareil d'une cible, ce qui permet aux personnes qui utilisent le logiciel de faire tout ce qu'elles veulent sur l'appareil, et même plus que ce qu'un utilisateur peut faire, à l'insu de ce dernier. Certaines des versions les plus récentes de ces logiciels espions utilisent ce que l'on appelle des versions « zéro clic », ce qui signifie qu'il n'est pas nécessaire de piéger une cible en la faisant cliquer sur un lien dans un faux message. Un organisme gouvernemental client du logiciel espion peut simplement lancer une commande pour prendre le contrôle de n'importe quel appareil dans le monde qui est vulnérable à ce type d'exploitation.

Une fois que vous avez pénétré dans un appareil, vous pouvez intercepter et écouter n'importe quel appel téléphonique. Vous pouvez lire les courriels et les messages texte, même ceux qui sont chiffrés. Vous pouvez activer silencieusement la caméra et le microphone de l'appareil, voir tous les contacts, modifier des fichiers, accéder au nuage de données d'une personne et la localiser. Il s'agit d'une technologie de surveillance extraordinairement puissante.

N'oubliez pas que nous vivons à une époque différente de celle d'il y a 20 ans, lorsque la mise sur écoute consistait à placer un dispositif sur une ligne fixe, ou à installer un microphone ou un localisateur GPS dans la voiture d'un suspect. Ces dispositifs vous permettent de faire tout cela et plus encore, car ils sont conçus par leurs fabricants pour être aussi intrusifs que possible. Ils sont conçus, ainsi que les applications qu'ils contiennent, pour espionner tous les aspects de notre vie, et constituent donc une mine d'or de renseignements à la disposition des clients des logiciels espions.

● (1540)

[*Français*]

M. René Villemure: Je vous remercie, monsieur Deibert.

Hier, on nous a expliqué qu'il y avait des mandats et que, suivant la partie VI du Code criminel, un juge devait valider et autoriser le recours à ces outils d'enquête. Cela constituerait un bon mécanisme de surveillance.

Je ne sais pas si vous êtes d'accord avec moi sur le fait qu'une situation peut être légale tout en étant non éthique. Comme cela a été dit, la loi date d'une vingtaine d'années et la technologie évolue à un rythme effarant.

Même s'il y a des précautions sur le plan juridique, l'utilisation de ces outils d'enquête peut-elle devenir non éthique?

[*Traduction*]

M. Ronald J. Deibert: Merci, monsieur le président.

Je pense que la révélation du fait que des mandats sont obtenus est assurément rassurante. Je suis heureux que ce ne soit pas le contraire; cependant, je pense que nous devons placer la surveillance judiciaire dans le contexte d'un certain nombre de facteurs liés à cet environnement — le sujet dont nous parlons.

Tout d'abord, je pense qu'il existe un problème de transparence et de responsabilisation envers le public au sein de nos organismes d'application de la loi. Il existe en fait une tendance, comme l'a dit ma collègue, Mme McPhail, à ne pas divulguer à l'avance certaines techniques d'enquête qui nécessitent une consultation publique. Encore et encore, ces techniques sont révélées par les médias ou d'une manière détournée, et les choses ne devraient pas se faire ainsi.

Deuxièmement...

Le président: Le temps prévu pour une réponse est écoulé. Pourriez-vous résumer en quelques secondes, et je devrai ensuite passer à M. Green.

M. Ronald J. Deibert: Cette technologie pose des problèmes de sécurité publique. Des intérêts sont en jeu, car elle exploite des failles présentes dans les logiciels qui nous rendent tous vulnérables, au lieu de les divulguer aux fournisseurs.

Le président: Merci.

Monsieur Green, vous avez six minutes au plus.

M. Matthew Green (Hamilton-Centre, NPD): J'aimerais poursuivre sur ce sujet, car je pense qu'il est important, dans l'intérêt de ce comité, que nous nous fassions une meilleure idée de ce à quoi ressemble ce secteur.

Professeur Deibert, vous avez parlé de sociétés mercenaires et malhonnêtes. Pourriez-vous nous en dire plus à ce sujet, en vous basant sur vos recherches, et nous dire à quoi ressemble ce secteur, quels en sont les acteurs, d'où vient l'expertise en la matière et pourquoi nous devrions nous en inquiéter?

M. Ronald J. Deibert: On sait très peu de choses sur cette industrie, qui opère dans l'ombre par définition. Elle est semblable au commerce de la technologie des armes ou du renseignement privé. Ces entreprises n'aiment en général pas divulguer publiquement ce qu'elles font ou qui sont leurs clients, ce qui rend la responsabilisation et la transparence très difficiles. Le Citizen Lab, ainsi que plusieurs autres organismes, ont passé plus de 10, voire 15 ans, à enquêter sur cette industrie en s'appuyant sur diverses méthodes techniques et médicolégales.

Nous avons constaté qu'il n'existe pratiquement aucune réglementation internationale applicable à cette industrie; ces membres vendent leurs produits à n'importe quel client gouvernemental. Malheureusement, la plupart des gouvernements dans le monde sont autoritaires ou antilibéraux, et naturellement, ils n'utilisent pas cette technologie de la manière dont nous espérons qu'elle sera utilisée ici, mais pour s'en prendre à l'opposition politique, à la société civile, aux journalistes, aux militants et autres. Ils gagnent ainsi des millions de dollars et dissimulent leur infrastructure institutionnelle aux enquêteurs comme nous.

Il s'agit d'un problème de sécurité nationale et de droits de la personne très grave à l'échelle mondiale. Il suffit de regarder les réactions aux plus hauts échelons du gouvernement des États-Unis. La Maison-Blanche de Biden, le Département de la Justice, le Département d'État et le Département du Commerce ont tous déclaré exactement ce que je suis en train de vous dire. Nous avons pris du retard face aux menaces posées par l'industrie mondiale des logiciels espions mercenaires, et nous devons de toute urgence remédier à cette situation.

● (1545)

M. Matthew Green: Je sais qu'il y a eu des reportages locaux, et nous en avons entendu parler aujourd'hui, dans le témoignage du gouvernement, qui font référence à un ancien premier ministre, Stephen Harper, qui aurait été impliqué. Je pense qu'un ancien ambassadeur en Israël aurait également été mêlé à cette affaire, ou aurait du moins été signalé comme l'ayant été. Pouvez-vous parler de la relation entre les personnes au sein des gouvernements qui pourraient avoir obtenu les cotes de sécurité les plus élevées et qui agissent ensuite comme — et je pense que vous l'avez très bien formulé — un secteur « mercenaire »? Pouvez-vous parler des dangers que représentent les personnes qui ont accès à des cotes de sécurité élevées et qui rejoignent ensuite ce secteur, qu'il s'agisse d'organismes élus ou civils, mais aussi de certains de nos organismes d'application de la loi les plus importants?

M. Ronald J. Deibert: Il s'agit d'une préoccupation très grave, car il existe une porte tournante très bien documentée, avec des gens qui travaillent pour les services de renseignement et qui partent ensuite gagner de l'argent, pour certains de manière très honorable, malheureusement, et pour d'autres non. Je pense qu'il est honteux qu'un ancien premier ministre soit associé à la vente de technologies de surveillance, et à la médiation de ventes d'entreprises canadiennes à des clients du Golfe qui ont un passé bien documenté de violations des droits de la personne. C'est pourquoi j'ai dit dans mes recommandations que nous devions imposer aux personnes qui ont travaillé pour les services de renseignements et d'application de la loi une interdiction à vie de travailler pour des entreprises mercenaires de logiciels espions.

Nous devons également, dans ce pays, établir des règles claires en matière de contrôle de l'exportation de technologies de surveillance. Le Citizen Lab a documenté l'exportation de technologies de censure et de surveillance fabriquées par des entreprises basées au Canada qui ont permis des violations des droits de la personne à l'étranger qui seraient inacceptables dans notre pays. Je suis choqué de constater qu'il n'existe réellement aucun octroi de licence ni aucun contrôle des exportations dans ce pays pour l'exportation ou la vente de logiciels espions et de technologies de surveillance du type de celles dont nous parlons ici. Cette situation doit changer.

M. Matthew Green: Pour que les choses soient claires et que vos propos soient consignés au procès-verbal, monsieur, s'agit-il d'une recommandation que vous faites au Comité afin qu'il recommande, à son tour, la mise en œuvre de ces mesures, ou s'agit-il d'un simple commentaire?

M. Ronald J. Deibert: Oui, tout à fait, ce point figurait dans mon témoignage à titre de recommandation particulière. Les entreprises canadiennes ont désespérément besoin de conseils, de règles de base claires pour savoir à qui elles peuvent vendre leur technologie, afin d'éviter qu'elles ne fournissent des technologies de surveillance, comme elles l'ont fait, à des régimes étrangers tels que les Émirats arabes unis, la Russie, la Turquie et d'autres pays, et permettent des pratiques qui constitueraient clairement une violation de la Charte dans notre pays.

M. Matthew Green: Nous craignons toujours que notre gouvernement puisse faire indirectement ce qu'il n'est pas autorisé à faire directement en tirant profit, par exemple, de renseignements qui pourraient être obtenus illégalement par des acteurs étrangers. Il pourrait s'agir d'acteurs étrangers amis; vous pouvez prendre l'exemple de l'utilisation de Pegasus dans des pays comme le Mexique. Pegasus n'est qu'une marque. C'est la technologie qui est intrusive.

M. Ronald J. Deibert: C'est exact.

M. Matthew Green: Pourriez-vous formuler des commentaires sur la possibilité que le gouvernement ait en sa possession des renseignements qui pourraient être sensibles sur le plan politique? Nous avons constaté que cette technologie était utilisée à l'encontre des médias et de l'opposition partisane. Pourriez-vous développer ce point et formuler des commentaires à ce sujet?

M. Ronald J. Deibert: Monsieur le président, je pense que de nombreux fabricants de logiciels espions entretiennent des liens étroits, pour des raisons géostratégiques, avec les gouvernements des pays dans lesquels ils sont implantés. Je ne serais pas surpris que les renseignements recueillis par ces sociétés de logiciels espions pour le compte de clients gouvernementaux ne finissent par être transmis à des personnes particulières liées aux autorités gouvernementales de leur pays d'origine, ce qui constitue également un risque pour la sécurité.

Nous devons faire preuve d'une diligence raisonnable accrue en matière d'approvisionnement. Avec tout le respect que je dois à l'un de mes collègues du groupe de témoins, je ne vois aucun motif de sécurité opérationnelle qui nous empêche de divulguer à qui nous achetons cette technologie. Le fait de divulguer ce renseignement n'a réellement aucune incidence et ne donne aucun indice à qui que ce soit. Il s'agit d'une bonne pratique et d'une approche mûre à un problème du XXI^{e} siècle.

Le président: Merci.

Sur ce, nous allons passer à M. Williams, qui aura cinq minutes au plus.

M. Ryan Williams (Baie de Quinte, PCC): Merci beaucoup, monsieur le président.

Je vais également poser des questions au professeur Deibert.

Monsieur Deibert, merci d'être présent aujourd'hui.

En ce qui concerne l'utilisation par la GRC de ces systèmes de piratage de téléphones cellulaires de type Pegasus, ce comité a entendu hier que ces outils étaient utilisés depuis 2017, et que pas une seule consultation n'a eu lieu avec le bureau du commissaire à la protection de la vie privée. Ils l'ont appris aux nouvelles. Vous comprenez bien, comme vous l'avez démontré, les répercussions que cette technologie peut avoir. Trouvez-vous acceptable la décision de la GRC de dissimuler ces renseignements aux Canadiens?

● (1550)

M. Ronald J. Deibert: Non, je trouve que c'est tout à fait inacceptable, monsieur le président. Je pense avoir entendu quelque chose de légèrement différent dans le témoignage. Il m'a semblé que l'un des agents de la GRC a déclaré qu'ils utilisaient ce type de technologie bien avant 2017, ce qui n'est vraiment pas surprenant. Comme l'a indiqué Mme McPhail il y a quelques instants, les organismes chargés de l'application de la loi sont souvent réticents, pour des raisons diverses, à l'idée de divulguer les types de techniques de surveillance qu'ils utilisent ou des technologies précises, et les cachent au public, puis, d'une manière ou d'une autre, ces renseignements sont divulgués, par les médias, les demandes d'AIPRP ou autres, et ils doivent se dépêcher de produire des documents pour justifier *ex post facto* la manière dont ils les utilisent.

M. Ryan Williams: Je pense que l'une des recommandations de cette étude sera que tous les organismes gouvernementaux, quels qu'ils soient, devraient être tenus de réaliser ou être mandatés pour réaliser légalement une évaluation des facteurs relatifs à la vie privée. Êtes-vous d'accord avec cette recommandation?

M. Ronald J. Deibert: Oui, complètement. Ce serait la moindre des choses, à mon avis.

M. Ryan Williams: Merci.

Madame McPhail, votre organisme a qualifié les OEE d'option nucléaire de surveillance pour la GRC. Pourquoi parlez-vous d'option nucléaire?

Mme Brenda McPhail: Merci pour cette question.

Je pense que le professeur Deibert a abordé cette question, mais je vais la développer.

Hier, un témoin de la GRC a déclaré, pour paraphraser, qu'ils n'envisagent pas d'effectuer une évaluation des facteurs relatifs à la vie privée simplement parce qu'ils utilisent une nouvelle technologie. Ils se demandent si la technologie permet un nouveau type d'intrusion.

Cette approche semble assez logique jusqu'à ce que vous l'analysiez, car cette définition de la nature de la recherche ne tient pas compte de la réalité d'un OEE, qui permet toutes les intrusions en même temps sur un appareil que nous — et non eux — possédons.

Pratiquaient-ils des écoutes auparavant? Bien sûr. Ces écoutes permettaient-elles d'accéder au contenu de toute forme de communication écrite et orale, professionnelle et privée, rétrospectivement et prospectivement, y compris les données qui ne se trouvent pas sur l'appareil même, mais dans le nuage? Bien sûr que non. S'agit-il du même niveau d'intrusion? Non. La police a-t-elle installé des caméras cachées dans des maisons et des lieux d'affaires après avoir obtenu un mandat par le passé? Bien sûr. Une seule caméra avait-elle la capacité de se déplacer avec un sujet d'enquête du travail à la maison, de la chambre à la salle de bain, 24 heures sur 24? Bien sûr que non. S'agit-il du même niveau d'intrusion? Non.

Un OEE peut en faire plus. Il peut enregistrer des sons en direct. Il peut surveiller les emplacements. Il recueille les identifiants des appareils. Il enregistre les recherches sur Internet. Il suit l'utilisation des applications.

Une EFVP aurait-elle dû être exigée? Bien sûr. Mais, comme le dit le professeur Deibert, même une EFVP ne suffit pas face à l'énormité de cette intrusion.

M. Ryan Williams: Pensez-vous que, quel que soit l'organisme gouvernemental qui utilise une nouvelle technologie, celui-ci devrait être tenu de procéder à une évaluation des facteurs relatifs à la vie privée?

Mme Brenda McPhail: Tout organisme gouvernemental souhaitant utiliser une technologie de surveillance susceptible de porter atteinte aux droits et présentant un risque élevé pour le public devrait assurément être tenu de réaliser une évaluation des facteurs relatifs à la vie privée obligatoire, qui devrait être rendue publique sous une forme appropriée.

M. Ryan Williams: Merci.

Monsieur Juneau-Katsuya, dans le cadre de votre travail avec le gouvernement dans le passé ou de vos recherches, avez-vous constaté que d'autres organismes que la GRC utilisaient une technologie semblable à celle sur laquelle nous enquêtons avec la GRC?

M. Michel Juneau-Katsuya: Il faudrait vous montrer un peu plus précis, mais certaines des technologies, bien sûr...

M. Ryan Williams: Je veux dire le SCRS, le CST, ce genre d'organisme. Savez-vous si d'autres organismes gouvernementaux que la GRC utilisent une technologie semblable à celle de Pegasus?

M. Michel Juneau-Katsuya: D'autres organismes l'utilisent, probablement, oui.

M. Ryan Williams: Merci.

Monsieur le président, je pense que mon temps est écoulé.

Le président: Il vous reste environ 15 secondes, donc je ne sais pas si...

Le président: Très bien, voilà ce que j'aime entendre. De cette façon, nous allons pouvoir rester dans les temps.

Sur ce, nous passons à Mme Shanahan, qui dispose d'un maximum de cinq minutes.

M. Ryan Williams: Je vais céder mon temps.

Mme Brenda Shanahan (Châteauguay—Lacolle, Lib.): Je suis désolée, monsieur le président. Je ne suis pas prête à poser des questions.

Le président: Oh, j'espère que je ne me suis pas trompé dans l'ordre des interventions.

Madame Vandenbeld, allez-y, s'il vous plaît.

Mme Anita Vandenbeld (Ottawa-Ouest—Nepean, Lib.): Merci beaucoup, monsieur le président.

Je suis heureuse de comparaître à nouveau devant ce comité. La dernière fois que j'ai comparu devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, c'était pour l'étude sur Cambridge Analytica et Facebook, et j'ai trouvé que nous avions fait un très bon travail non partisan sur cette question.

Il s'agit, bien entendu, d'une question qui me préoccupe très profondément. J'aimerais adresser ma première question au professeur Deibert. Comme vous le savez — et je pense que nous faisons tous les deux partie du comité directeur de World Movement for Democracy —, j'admire depuis longtemps une grande partie du travail effectué par le Citizen Lab dans le monde, à la fois sur la désinformation et sur le cyber-harcèlement des militants des droits de la personne. Je pense que vous avez soulevé des points très préoccupants quant à la manière dont les régimes autoritaires utilisent ce type d'outils.

Pour ce qui est de l'objet précis de l'étude de ce comité, je sais que certains des éléments que vous avez mentionnés, en particulier lorsque vous parlez de la répression numérique transnationale et autres, pourraient être abordés de manière plus appropriée par le comité des affaires étrangères ou même par le Sous-comité des droits internationaux de la personne, dont je fais partie. Je pense que ces thèmes susciteraient un grand intérêt, notamment le contrôle des exportations.

La question que je souhaite vous poser est plus précise. Je pense que vous conviendrez que lorsque la GRC utilise ces outils dans un cadre très étroit — il me semble que vous avez utilisé des termes comme « proportionné » et « nécessaire » — avec une surveillance judiciaire et des mandats, cette utilisation est très différente de celle qu'en font des régimes comme la Chine ou l'Iran. Si l'on met de côté les questions telles que celles des fournisseurs et des contrôles de l'exportation, vous avez mentionné quelque chose qui me semble intéressant. Vous avez parlé de seuils. Pourriez-vous nous en dire un peu plus sur ce à quoi ressembleraient ces seuils destinés à empêcher les abus de ce type de pouvoir?

● (1555)

M. Ronald J. Deibert: Je pense que dans l'ensemble, il est rassurant d'avoir entendu hier le témoignage de la GRC et du ministre indiquant que les cas d'utilisation de ce type de technologie ont été entrepris avec une autorisation judiciaire. Cependant, comme je l'ai déjà dit, je pense que le fait que la GRC nous dise qu'il y a eu une autorisation judiciaire ne doit pas être considéré comme une sorte de baguette magique qui fait disparaître tout le reste: « Circulez, il n'y a rien à voir. »

Tout d'abord, nous savons qu'il existe un passé bien documenté d'abus au sein des forces de l'ordre dans ce pays. Il existe un passé documenté de pratiques discriminatoires. Je m'inquiète également de la nature de la technologie même et je me demande, avec tout le respect que je dois aux juges en qui j'ai confiance, s'ils comprennent vraiment la portée, l'échelle, le degré de sophistication et la puissance du type de technologie intrusive dont nous parlons et que Mme McPhail vient de décrire avec précision.

Je pense également que nous devons également aborder certaines questions d'équité. Mon équipe et moi-même procédons régulièrement à des analyses judiciaires des victimes de logiciels espions. Dans plusieurs cas, nous avons récupéré des copies du logiciel espion et fait des divulgations responsables aux distributeurs, contrairement à ce que font les organismes gouvernementaux. Ces divulgations ont donné lieu à des correctifs de sécurité qui ont touché plusieurs milliards de personnes dans le monde. Si le gouvernement refuse de communiquer ces renseignements aux fournisseurs et met en péril notre sécurité à tous, il doit mettre en place une procédure adéquate. Cette procédure est généralement nommée « procédure d'évaluation des vulnérabilités ». À l'heure actuelle, comme je l'ai dit dans mon témoignage, le processus mis en place dans ce pays est faible. Il est opaque. Pour être honnête, il est loin d'être au niveau qu'exige une démocratie libérale mûre.

Ce sont là quelques-unes de mes préoccupations, qui vont bien au-delà du fait que la GRC nous a simplement dit que ces utilisations avaient été autorisées par un juge.

Mme Anita Vandenbeld: Merci. Voilà qui est très utile.

Monsieur Juneau-Katsuya, j'ai remarqué que vous n'aviez pas terminé la dernière partie de votre déclaration préliminaire. Je veux vous donner un peu de temps pour le faire maintenant.

M. Michel Juneau-Katsuya: Je vous en remercie du fond du cœur.

Je veux attirer votre attention sur le fait que, malheureusement, notre société, en particulier notre démocratie, est en état de siège. Nous sommes confrontés à une menace énorme. Probablement depuis les années 1600 et 1700, lorsque le concept initial de démocratie a commencé à apparaître, nous n'avons jamais été menacés comme nous le sommes actuellement. L'extrême droite, la droite alternative, se développe. On entend un discours populiste. Certaines personnes utilisent la démagogie pour essayer de convaincre les gens et provoquer de l'insécurité.

De ce point de vue, je soutiens complètement l'idée de créer plus de contrôle, plus de responsabilité et plus de transparence. Ce que je veux, c'est parvenir à un équilibre, un équilibre qui ne nuise pas à la capacité d'attraper les malfaiteurs. Malheureusement, les beaux discours, les théories et les débats philosophiques — ils ne s'en soucient pas.

● (1600)

Le président: Merci. Nous avons beaucoup dépassé le temps imparti, mais nous avons pu tout entendre.

Nous allons maintenant passer à M. Villemure pour deux minutes et demie.

[*Français*]

M. René Villemure: Je vous remercie, monsieur le président.

Monsieur Deibert, je vous demanderais de répondre à ma question de façon brève, parce que mon temps de parole est limité.

Êtes-vous en faveur d'un recours à une tierce partie, qui examinerait les actions de la GRC en matière d'outils de surveillance?

[*Traduction*]

M. Ronald J. Deibert: Oui. Je suis favorable à ce que le plus grand nombre de parties légitimes possible contribuent à veiller à ce que nous assurions une responsabilisation adéquate pour faire face au grand bond en avant des capacités technologiques dont disposent aujourd'hui les organismes chargés de l'application de la loi et de la sécurité.

[*Français*]

M. René Villemure: Je vous remercie beaucoup.

Monsieur Juneau-Katsuya, vous avez mentionné à la fin de votre dernière intervention que d'autres agences utilisaient probablement cette technologie.

Croyez-vous que des parlementaires et des élus ont été surveillés au fil du temps par des agences?

M. Michel Juneau-Katsuya: Il a fallu surveiller des parlementaires, effectivement, parce qu'il y a aujourd'hui des parlementaires de tous les échelons, que ce soit municipal, provincial ou fédéral, qui sont à la solde de gouvernements étrangers et qui ne travaillent pas nécessairement pour le Canada.

Il existe donc ce que l'on appelle des agents d'influence, qui peuvent agir consciemment ou inconsciemment. Or, le résultat est le même pour la sécurité nationale canadienne, et cela expose le Canada à un risque.

M. René Villemure: Les outils comme le logiciel Pegasus sont-ils utilisés ou cela s'est-il passé auparavant?

M. Michel Juneau-Katsuya: Ils étaient utilisés auparavant et ils le sont aussi maintenant. Ce n'est pas quelque chose de nouveau. Depuis toujours, les agences étrangères tentent de recruter des élus. Cela est relativement assez facile pour elles parce que les élus ne suivent malheureusement pas toujours les consignes du Service canadien du renseignement de sécurité ou ils les ignorent, car cela sert leurs buts personnels et intentionnels.

M. René Villemure: Je vous remercie beaucoup.

Monsieur Deibert, plus tôt, vous avez dit que c'était la moindre des choses de procéder à l'évaluation des facteurs relatifs à la vie privée.

Qu'est-ce qui serait l'idéal?

[*Traduction*]

M. Ronald J. Deibert: Je pense que nous devons établir une sorte de présence intégrée du Commissariat à la protection de la vie privée. Pour être franc, j'ai été très déçu d'entendre que le Commissariat à la protection de la vie privée n'était pas informé de l'utilisation de ces techniques d'enquête avant les récentes révélations. Nous devons donc établir une présence beaucoup plus forte et, à mon avis, fournir encore plus de capacités et de ressources aux commissaires à la protection de la vie privée, afin qu'ils puissent assurer la surveillance de nos organismes responsables de la sécurité.

Il ne s'agit pas de dénigrer la mission très importante des forces de l'ordre et des autres organismes responsables de la sécurité dans ce pays. Nous voulons qu'ils soient bien équipés, mais nous devons avoir des organismes pour surveiller la surveillance. C'est aussi, en partie, la mission du Citizen Lab. Nous assurons une fonction de surveillance.

Le président: Merci, professeur Deibert.

[*Français*]

M. René Villemure: Je vous remercie.

[*Traduction*]

Le président: Nous avons dépassé le temps imparti.

Nous allons maintenant passer à M. Green, qui aura deux minutes et demie.

M. Matthew Green: Merci.

Madame McPhail, vous avez recommandé la mise en place d'une contrepartie civile aux demandes de mandats de la police dans le cadre de la procédure judiciaire. Pourriez-vous développer cette idée, car c'est un point que j'ai retenu comme faisant référence à ce qui pose un peu problème en matière de responsabilisation dans la procédure liée aux mandats.

Mme Brenda McPhail: Avec plaisir.

Cette idée fait écho à une recommandation que j'ai formulée lors de la récente étude sur les technologies de reconnaissance faciale. Pour contrer la tendance persistante de la police à acquérir et à utiliser des technologies de surveillance sophistiquées et potentiellement controversées sans en informer le public, nous devrions suivre l'exemple de lieux comme l'État de New York et la Nouvelle-Zélande, et mettre sur pied un comité consultatif indépendant qui serait composé d'intervenants pertinents de la communauté juridique, du gouvernement, de la police et de la sécurité nationale, de la société civile et, bien entendu, de nos organismes de réglementation pertinents, comme le Commissariat à la protection de la vie privée.

Il pourrait servir d'organisme national d'établissement de normes, d'organisme consultatif, et examinerait de manière proactive les types de technologies que nos forces de police souhaitent utiliser pour moderniser leurs techniques d'enquête et les étudier en tenant compte de toute une série de considérations, y compris des considérations éthiques et juridiques, et des considérations liées aux normes et valeurs canadiennes. Il pourra ensuite recommander des normes, des normes d'excellence, aux organismes policiers, non seulement à l'échelle nationale, mais aussi à l'échelle provinciale et territoriale — car, bien entendu, le maintien de l'ordre est aussi une question provinciale et territoriale — afin d'assurer une certaine uniformité et de garantir au public que les droits sont respectés et que les policiers disposent des outils dont ils ont besoin pour accomplir leur travail difficile.

● (1605)

M. Matthew Green: Merci.

Le Conseil de l'Europe reconnaît que l'utilisation de l'outil Pegasus constitue une violation de l'article 8 sur le droit à la vie privée de la Convention européenne des droits de l'homme.

Le cadre juridique canadien garantit-il des protections de la vie privée similaires à celles de l'article 8 de la Convention européenne, de sorte que l'utilisation d'outils d'enquête sur appareil ayant des capacités technologiques semblables à celles de Pegasus pourrait être considérée comme illégale?

Mme Brenda McPhail: Excusez-moi. Est-ce à moi que vous posez la question?

M. Matthew Green: Oui.

Mme Brenda McPhail: Je pense qu'il est bien connu que le régime de protection de la vie privée du Canada a pris du retard. Je crois que de nombreuses déclarations ont été faites devant ce comité depuis près de 10 ans, dans lesquelles étaient décrites les lacunes de nos lois sur la protection de la vie privée, tant dans le secteur public que privé, qui ne protègent pas...

Le président: Merci, madame McPhail. Nous avons dépassé le temps imparti.

Nous passons maintenant à M. Hallan.

Bienvenu au comité de l'éthique et merci de vous joindre à nous aujourd'hui. Vous avez la parole pour cinq minutes.

M. Jasraj Singh Hallan (Calgary Forest Lawn, PCC): Merci, monsieur le président.

Merci aux témoins d'être présents.

Monsieur Juneau, j'aimerais revenir sur une réponse que vous avez donnée à mon collègue, M. Williams. J'ai trouvé très intéressant que vous disiez que d'autres organismes utilisent également des logiciels semblables à Pegasus. Quels autres organismes utilisent ce type de logiciel et quel usage en font-ils?

M. Michel Juneau-Katsuya: Il s'agit des organismes responsables de la sécurité nationale.

C'est un outil d'enquête. Ils doivent le posséder pour pouvoir suivre certaines cibles, des personnes très dangereuses. C'est l'un des outils à leur disposition.

M. Jasraj Singh Hallan: Quel type de logiciel utilisent-ils? S'agit-il toujours du même logiciel ou est-il différent pour chaque organisme?

M. Michel Juneau-Katsuya: Je ne dispose pas encore de tous les renseignements sur le type de logiciel ou le nom du logiciel. Je ne suis pas en mesure de vous répondre.

M. Jasraj Singh Hallan: D'autres organismes utilisent-ils des logiciels différents — vous n'avez pas besoin de les nommer — ou le même logiciel est-il utilisé par d'autres organismes?

M. Michel Juneau-Katsuya: Je ne dispose pas des renseignements sur celui qu'utilise la GRC, je ne peux donc pas faire de comparaison.

M. Jasraj Singh Hallan: À votre avis, est-il utilisé uniquement sur des Canadiens ou également sur des ressortissants étrangers? Utilisent-ils le même logiciel sur les ressortissants étrangers?

M. Michel Juneau-Katsuya: À ma connaissance, il n'est utilisé que sur les Canadiens. Encore une fois, cette information doit être vérifiée, car je ne suis pas au fait de toutes les utilisations opérationnelles.

M. Jasraj Singh Hallan: À votre avis, l'utilisation du logiciel a-t-elle toujours été faite avec un mandat, ou bien une partie de cette utilisation se fait-elle sans mandat?

M. Michel Juneau-Katsuya: Je pense que son utilisation nécessite un mandat.

M. Jasraj Singh Hallan: À chaque fois?

M. Michel Juneau-Katsuya: Encore une fois, je n'ai pas vérifié tous les organismes, donc je ne suis pas en mesure de confirmer et de certifier que toutes les utilisations ont été faites avec un mandat. Si je prends l'exemple d'un organisme comme le SCRS, aucune enquête n'est effectuée sans une procédure de vérification régulière. Selon le niveau d'enquête, il peut être nécessaire d'obtenir un mandat d'une cour supérieure.

M. Jasraj Singh Hallan: En ce qui concerne l'approbation d'un mandat émanant d'une cour supérieure, un même juge prend-il un grand nombre des décisions visant à accorder ce mandat? Avez-vous vu différents juges?

M. Michel Juneau-Katsuya: J'ai eu affaire à plusieurs juges. Ce n'est pas toujours le même juge, mais certains juges ont été sélectionnés en raison du degré de confidentialité et du niveau de sécurité nationale.

M. Jasraj Singh Hallan: D'accord, merci.

Monsieur Deibert, après avoir regardé la séance du Comité tenue hier, vous avez entendu ce qu'ont dit les témoins. L'une des questions dont tout le monde parle en ce moment est la confiance et à quel point elle a été brisée. Vous en avez parlé, et beaucoup d'autres personnes en parlent.

Après avoir entendu les propos du ministre de la Sécurité publique, comment pensez-vous que les Canadiens pourraient aujourd'hui avoir confiance en certaines de nos institutions?

● (1610)

M. Ronald J. Deibert: Il existe incontestablement un problème de confiance dans les institutions publiques, et nous ne sommes pas les seuls dans ce cas. À l'échelle mondiale, on observe un déclin de la confiance dans les institutions publiques. Nous ne sommes donc pas les seuls.

Si nous voulons donner le bon exemple au reste du monde et nous améliorer le plus possible, je pense que nous pouvons facilement faire mieux que ce que nous avons vu dans cette dernière affaire qui, comme je l'ai déjà dit, suit le schéma d'affaires précédentes. Tout d'abord, nous devons procéder à une consultation publique très claire, à la mesure de l'importance de la technologie dont nous parlons ici, qui représente un bond en avant des capacités de surveillance.

Sans cette consultation publique et en essayant d'aborder ce sujet comme ils l'ont fait dans le passé, en le cachant au public et en ne divulguant pas des renseignements qui pourraient facilement l'être, je pense que nous donnons un mauvais exemple.

M. Jasraj Singh Hallan: Je suis d'accord avec vous sur ce point.

Monsieur Juneau, vous avez dit que les politiciens à tous les échelons ont fait l'objet d'une surveillance. Inutile de citer des noms, mais pouvez-vous nous dire combien de politiciens, selon votre expérience, ont été surveillés?

M. Michel Juneau-Katsuya: Non, je ne peux pas donner de chiffre précis étant donné que dans le concept de sécurité nationale...

M. Jasraj Singh Hallan: S'agit-il de dizaines, de vingtaines ou de centaines? Pouvez-vous nous donner un ordre d'idée?

M. Michel Juneau-Katsuya: Encore une fois, il m'est difficile de donner des chiffres, car nous travaillons sur la base du besoin de savoir. Par exemple, si mes collègues travaillent sur la Russie, ils ne sauront pas si je travaille sur la Chine et ne connaîtront pas certaines de mes cibles.

Ce dont nous sommes sûrs, c'est que plusieurs pays étrangers ont réussi à recruter des élus — municipaux, provinciaux ou fédéraux — et ont été capables d'exercer une influence de cette manière.

À la fin de leur mandat, certains ministres vont également travailler pour des entreprises étrangères qui agissent directement contre les intérêts nationaux et la sécurité nationale du Canada. Le fait que certaines personnes quittent la fonction publique suscite des inquiétudes, compte tenu de ce qu'elles ont fait pendant leur mandat et de ce qu'elles font après avoir assumé une charge publique.

M. Jasraj Singh Hallan: D'accord. Merci.

Monsieur...

Le président: Vous avez largement dépassé le temps imparti, mais cette réponse est tout à fait fascinante.

M. Jasraj Singh Hallan: Merci, monsieur le président.

Le président: Sur ce, je vais donner la parole à Mme Khalid. Mme Khalid sera la dernière intervenante de la deuxième série de questions. Puis nous passerons à la suivante.

Allez-y, madame Khalid.

Mme Iqra Khalid (Mississauga—Erin Mills, Lib.): Merci beaucoup, monsieur le président.

Professeur Deibert, un membre de mon personnel a suivi un certain nombre des cours que vous avez donnés à titre de professeur à l'Université de Toronto, et il avait de très bonnes choses à dire sur votre rôle et votre expertise dans ce domaine. Je vous remercie sincèrement d'être ici aujourd'hui. Merci beaucoup. Le lien est personnel.

Je sais que les députés ont posé des questions auxquelles vous n'êtes pas vraiment en mesure de répondre parce que vous ne disposez pas des renseignements directs. Une grande partie de ce dont nous discutons au sein de ce groupe repose sur des hypothèses et des suppositions, et s'inscrit davantage dans une perspective politique que dans une perspective basée sur des faits ou sur des preuves.

Je vais commencer par le professeur Deibert, si vous le permettez, et poser une question sur la désinformation.

Nous parlons des institutions qui nous gouvernent et de la confiance du public. Comment le concept selon lequel la GRC et les institutions policières contrôlent et surveillent les Canadiens...? Quel genre de répercussions cette situation entraîne-t-elle? Jusqu'à présent, la GRC et le commissaire à la protection de la vie privée nous ont dit exactement combien d'enquêtes ont été menées grâce à une surveillance utilisant des OEE. Quelle est l'incidence de ces méthodes sur la façon dont le public perçoit la GRC et nos institutions dirigeantes en général, étant donné le climat de désinformation et les théories du complot colportées lors des récents événements? Professeur Deibert, souhaitez-vous formuler des commentaires à ce sujet?

M. Ronald J. Deibert: Si je comprends bien votre question, vous sous-entendez l'existence de désinformation au sujet de certaines des préoccupations soulevées quant aux risques et aux menaces que présente cette industrie particulière, à laquelle nos agences contribuent financièrement. Je pense que vous avez tout à fait tort. Nous avons mené pendant plus d'une décennie des recherches fondées sur des preuves, qui ont été largement citées. Celles-ci ont été réalisées grâce à des moyens techniques. Nous avons contrôlé des centaines de personnes dans le monde entier qui ne sont ni des criminels ni des terroristes et dont les téléphones ont été piratés à l'aide de ce type de logiciel espion par des gouvernements, tant autoritaires que démocratiques. Dans l'un des cas les plus récents, en Espagne, nous avons découvert une opération d'espionnage de surveillance massive...

● (1615)

Mme Iqra Khalid: Désolée de vous interrompre, mais nous parlons du Canada en particulier. La portée de la motion et de l'étude qui nous occupe concerne précisément la GRC. Nous parlons spécifiquement du Canada. Veuillez limiter vos réponses à ce sujet.

M. Ronald J. Deibert: D'accord. Comme je l'ai déjà dit, certaines des remarques que nous avons entendues dans le témoignage de la GRC étaient rassurantes pour ce qui est des chiffres et des autorisations judiciaires. Mais j'ai aussi entendu que ces chiffres changeaient au cours d'une journée. J'ai entendu que le commissaire à la protection de la vie privée n'était pas au courant de ce qui se passait. J'ai également entendu la GRC elle-même, dans une réponse à une question, dire: « Oui, nous surveillons les Canadiens », et il serait idiot de ne pas le dire puisque cela fait partie de son travail.

Le problème est précisément le manque de transparence et de responsabilisation à l'égard du public. En toute franchise, la façon dont nous entamons cette conversation n'est pas très logique. Ces renseignements ont été divulgués, me semble-t-il, presque par accident, et la conversation sur ce sujet important ne devrait pas être menée de cette manière. Il ne s'agit pas de désinformation. La question dont nous traitons ici est très importante. Nous devons faire preuve de maturité et en parler franchement, plutôt que de discréditer les personnes qui soulèvent ces questions importantes.

Mme Iqra Khalid: Merci pour votre réponse, professeur Deibert. Je vous en suis reconnaissante.

Monsieur Juneau-Katsuya, avez-vous des commentaires à faire à ce sujet?

M. Michel Juneau-Katsuya: J'aime beaucoup, comme je l'ai dit, la nécessité d'exercer un contrôle, le fait d'exiger une responsabilisation et une transparence optimales. Ce sont les pierres angulaires de notre démocratie. En même temps, nous avons la responsabilité de lutter contre certaines menaces très graves et de protéger les Canadiens contre ces menaces qui ne se soucient pas du débat philosophique portant sur ce qui est bien et ce qui est mal. Ces personnes agissent, un point c'est tout.

Je suis entièrement et totalement en faveur de cette capacité à trouver le bon équilibre, à nous remettre en question et à travailler de manière constructive pour que les agents soient en mesure de remplir leurs fonctions, tout en veillant, comme je l'ai dit, à ce que la fin ne justifie pas les moyens. Nous devons être en mesure de trouver cet équilibre pour être efficaces.

On en revient aussi aux responsabilités des élus. La police travaille à la résolution d'un problème qui existe déjà. Nous essayons de régler les situations lorsque nous sommes confrontés au problème. Parfois, les problèmes, comme le terrorisme, découlent du fait que les politiciens n'ont pas pris de mesures plus tôt, lorsque le grief a été porté à leur attention. La question n'est pas nécessairement de croire au grief ou de l'accepter, mais vous devez être capable d'agir. Voilà pourquoi le travail de ce comité est si important.

Le président: Merci.

Voilà qui conclut cette tranche de cinq minutes. Nous passons maintenant à la troisième série de questions. Conformément à la formule adoptée par le Comité, le premier intervenant sera M. Bezan, qui disposera de cinq minutes.

M. James Bezan: Merci, monsieur le président.

Bienvenue à nos témoins. Tout à l'heure, je n'ai pas eu l'occasion de poser des questions à M. Juneau-Katsuya.

Monsieur, je suis abasourdi par le témoignage que vous venez de faire selon lequel des anciens politiciens et des politiciens sont considérés comme des menaces potentielles pour la sécurité nationale et sont surveillés.

D'après votre expérience en tant qu'ancien agent du SCRS et de la GRC, dans ces situations, la jurisprudence serait-elle respectée pour s'assurer que les droits garantis par la Charte sont protégés par la délivrance de mandats d'écoute électronique ou d'utilisation de logiciels espions sur ces personnes?

M. Michel Juneau-Katsuya: À ma connaissance, lorsqu'un mandat était nécessaire, oui, nous l'avons obtenu et la procédure judiciaire a été suivie. Très souvent, les politiciens ou les représentants élus, comme je le dis volontiers, n'étaient pas nécessairement la cible initiale, mais ont en fait attiré notre attention lorsque nous avons constaté que des agents de renseignements étrangers ou des criminels étrangers ou canadiens étaient en contact avec eux. Le SCRS ou la GRC ont commencé à s'intéresser à ces personnes lorsqu'elles ont mené certaines activités ou accompli certains actes douteux compte tenu des responsabilités de leurs fonctions.

● (1620)

M. James Bezan: Dans ces situations, devrais-je, en tant qu'élu qui a soutenu très ouvertement l'Ukraine, Taïwan et d'autres démocraties menacées, craindre d'être espionné par les agences fédérales canadiennes en raison du soutien que j'ai offert à ces pays?

M. Michel Juneau-Katsuya: Non, mais vous vous inquiétez probablement du fait que des entités étrangères puissent vous espionner ou...

M. James Bezan: Toujours. Je suppose tout simplement que c'est le cas.

M. Michel Juneau-Katsuya: C'est pourquoi la GRC existe, pour essayer de vous protéger en raison des positions que vous prenez. C'est ce que nous apprécions dans notre société, cette capacité pour nos élus de s'exprimer franchement et de parler au nom de notre communauté, comme vous le faites.

Malheureusement, vous pouvez également devenir une cible, et c'est là que nous intervenons.

M. James Bezan: Lorsque nous examinons l'utilisation globale de la technologie — et elle a probablement changé de façon assez spectaculaire depuis le temps où vous travailliez au SCRS —, comment pouvons-nous nous assurer qu'elle est utilisée à bon escient? Vous avez dit dans votre déclaration préliminaire que vous ne vouliez pas que ce comité entre dans les détails et sape la capacité opérationnelle, mais, comme vous l'avez dit, nous avons également besoin de transparence et de responsabilisation, et nous devons savoir qui utilise cette technologie et comment elle est appliquée.

Où se situe la contrepartie dans cette situation, qui fait que nous minons la capacité de nos organismes d'application de la loi et de nos organismes responsables de la sécurité nationale à protéger les Canadiens?

M. Michel Juneau-Katsuya: Je pense que certains des éléments de preuve et des témoignages présentés par le professeur Deibert et d'autres personnes vont dans le bon sens, soit le fait de disposer de certaines entités capables d'effectuer des contrôles et des vérifications et d'exiger la responsabilisation nécessaire. Je pense que ce que j'ai entendu hier — peut-être que certaines personnes ont entendu des choses différentes — est que la GRC était ouverte à l'idée de cette responsabilisation. Peut-être que cela ne s'est pas fait assez vite ou que la transparence n'a pas été assurée assez tôt de l'avis de certaines personnes, mais voilà ce qu'est la démocratie en marche. C'est quelque chose qui doit être constamment vérifié.

Pour avoir été un agent de première ligne, je suis entièrement favorable à la capacité de...

M. James Bezan: À titre d'agent de première ligne, le SCRS peut-il, en tant qu'agence de renseignement, recueillir des preuves qui ne sont pas visées par la Loi sur la preuve au Canada ou le Code criminel? Le SCRS peut-il déployer ce type de logiciel espion sans mandat?

M. Michel Juneau-Katsuya: Le SCRS doit habituellement obtenir un mandat pour recueillir ce genre de preuves sensibles et utiliser ce genre de technologie.

M. James Bezan: Uniquement s'il s'agit d'un Canadien. S'il s'agit d'un étranger, l'obtention d'un mandat n'est pas nécessaire?

M. Michel Juneau-Katsuya: Non. Si une personne représente une menace pour la sécurité nationale, le SCRS peut agir à l'encontre d'un étranger. Par exemple, certains diplomates ne sont pas des diplomates, mais des espions étrangers. Nous les ciblons.

Le président: Le temps est écoulé.

Nous allons maintenant passer à Mme Vandenbeld. Vous avez cinq minutes au plus.

Mme Anita Vandenbeld: Merci beaucoup.

J'aimerais commencer par poser une question à Mme McPhail. Lorsque je faisais mes études supérieures, je siégeais au conseil d'administration de l'Alberta Civil Liberties Association, alors j'applaudis l'excellent travail que vous faites.

Dans votre témoignage, vous avez notamment déclaré, à la toute fin, qu'il y avait plus de problèmes, mais aussi plus de solutions, et que vous n'aviez pas le temps de toutes les exposer.

Je pense que ce qui intéresse beaucoup ce comité, ce sont les solutions. Pourriez-vous nous en dire un peu plus sur ce que vous considérez comme des solutions et sur la manière dont l'utilisation légale et légitime de ce type de technologies pourrait être faite sans abus et avec une responsabilisation adéquate?

Mme Brenda McPhail: Je pense qu'il existe un certain nombre de façons de procéder à une réforme juridique de tout un éventail de lois, qui permettrait d'améliorer la base de référence de la responsabilisation et de la transparence.

Les témoins précédents ont parlé hier de rendre obligatoires les évaluations des facteurs relatifs à la vie privée, et j'appuie cette recommandation à titre d'exigence de base. On a également mentionné l'idée, que j'appuie, d'inclure l'existence de la vie privée en tant que droit fondamental de la personne dans nos lois sur la protection de la vie privée dans les secteurs public et privé. Cette inclusion changerait la nature de l'exercice consistant à trouver un équilibre pour déterminer si les entreprises ou les gouvernements sont autorisés à mener des pratiques intrusives pour la vie privée. Elle place le droit au centre des préoccupations, soit à la place qu'il devrait occuper dans cette équation.

Il convient également d'examiner la partie VI du Code criminel qui, à ma connaissance, n'a pas subi de modifications significatives depuis un peu plus de 20 ans. Des avocats de la défense expérimentés, en particulier, pourraient être très utiles à ce comité pour recommander des modifications à cette partie, en se fondant sur leur expérience de ce genre de technologies modernes à mesure que leur utilisation se répand dans les affaires criminelles.

Enfin, dernier point concret, les États-Unis ont créé une liste d'entités de fournisseurs de logiciels espions interdits. Le Canada devrait absolument envisager d'en faire de même, ce qui offrirait au public une certaine assurance que l'argent de nos impôts ne va pas soutenir ces entreprises dangereuses et mercenaires.

● (1625)

Mme Anita Vandenbeld: Merci beaucoup.

Ma prochaine question est destinée à M. Juneau-Katsuya. Vous avez mentionné dans votre témoignage la nécessité d'établir un équilibre. Nous sommes certes tous très favorables à la transparence, mais vous avez dit dans votre témoignage que même lorsque notre comité se réunit ici pour demander des comptes, les personnes malveillantes écoutent. Pourriez-vous nous expliquer un peu comment nous pourrions établir cet équilibre tout en évitant de fournir des renseignements qui pourraient aider ces personnes malveillantes?

M. Michel Juneau-Katsuya: Je pense que nous disposons de mécanismes qui nous permettent — parfois à huis clos — d'entendre et de poser des questions difficiles. La Chambre des communes a créé un comité permanent sur la sécurité et le renseignement, qui est capable d'aller dans tous les ministères pour remonter la piste de certaines affaires. C'est extrêmement important.

La difficulté que nous rencontrons est que les députés en fonction sont élus — tout comme les membres de ce comité — et qu'à chaque élection, de nouveaux députés arrivent avec une nouvelle équipe, un nouveau groupe qui n'a pas nécessairement l'expérience, les connaissances ou le réseau nécessaires pour approfondir la question autant que nécessaire.

Devrions-nous disposer d'un plus grand nombre de comités comme le CSARS, le comité sur la sécurité et le renseignement, qui était un chien de garde et qui, au fil du temps, a fini par devenir un chien de poche? Il ne fait pas vraiment tout le travail nécessaire pour observer et critiquer certains problèmes, et pour y apporter des solutions.

Voilà le problème: parfois, les systèmes politiques interfèrent avec le travail du comité et minent son indépendance.

Vous avez mentionné dans l'un de vos commentaires précédents que vous appréciez le caractère non partisan du Comité et le travail qui a été accompli. Voilà ce qu'il faut chercher à maintenir autant que possible, car, en fin de compte, nous devrions travailler pour cette nation, et non pour nos intérêts partisans.

Mme Anita Vandenbeld: Je suis tout à fait d'accord.

Combien de temps me reste-t-il?

Le président: Il vous reste 20 secondes.

Mme Anita Vandenbeld: Merci beaucoup.

M. Michel Juneau-Katsuya: J'aimerais simplement ajouter que nous passons beaucoup de temps à parler des forces de l'ordre, qui est le leitmotiv de cette discussion, mais que nous avons omis de parler du monde privé. Les entreprises privées utilisent beaucoup plus ce type de technologie que les forces de l'ordre, qui sont beaucoup plus surveillées.

Le président: Merci.

Nous ne pouvons aborder qu'un nombre limité de sujets dans le cadre d'une seule et courte étude, mais, en effet, nous avons entendu à maintes reprises la nécessité de moderniser la Loi sur la protection des renseignements personnels, qui s'appliquerait aux intérêts privés et aux sociétés.

[*Français*]

Monsieur Villemure, vous avez la parole pour deux minutes et demie.

M. René Villemure: Je vous remercie beaucoup, monsieur le président.

Madame McPhail, croyez-vous que l'utilisation de ce genre de logiciel espion par les forces de l'ordre contrevient à la Charte canadienne des droits et libertés?

● (1630)

[*Traduction*]

Mme Brenda McPhail: D'après ce qu'on nous a dit au sujet de l'utilisation de ces outils, la GRC a essayé de respecter les limites de la Charte en s'assurant d'obtenir une autorisation judiciaire, en ne se servant de ces outils que pour un nombre restreint d'enquêtes et en s'assurant que ces utilisations ne concernaient que des crimes manifestement très graves. Le problème...

[*Français*]

M. René Villemure: Je suis désolé de vous interrompre, madame McPhail, mais je dispose d'un temps de parole limité.

Monsieur Deibert, vous avez mentionné dans vos recherches que le Canada présidait cette année la Freedom Online Coalition.

Croyez-vous que, à ce titre, le Canada a un devoir d'exemplarité?

[*Traduction*]

M. Ronald J. Deibert: Oui, je le pense.

[*Français*]

M. René Villemure: Quelle serait votre première suggestion?

[*Traduction*]

M. Ronald J. Deibert: Comme je l'ai dit, je pense que les hauts fonctionnaires, le premier ministre, le ministre de la Sécurité publique et la ministre des Affaires étrangères, doivent déclarer clairement et avec force que cette industrie, dont nous parlons au sein de ce comité, est une menace pour les droits de la personne, la démocratie et la sécurité nationale, et que nous allons prendre des mesures, en collaboration avec nos alliés aux États-Unis, en Europe et dans le monde, pour commencer à demander des comptes aux pires acteurs de cette industrie et à être nous-mêmes plus transparents et à rendre des comptes au public si nous devons utiliser cette technologie au niveau national.

[*Français*]

M. René Villemure: Il faudra commencer par le ton donné par les dirigeants, si je comprends bien.

[*Traduction*]

M. Ronald J. Deibert: Ce que nous n'avons malheureusement pas fait, contrairement aux États-Unis.

[*Français*]

M. René Villemure: Vous avez absolument raison.

Monsieur Juneau-Katsuya, j'ai été troublé par la révélation selon laquelle des élus pouvaient être recrutés par des gouvernements étrangers.

Auriez-vous un document à fournir au Comité ou quelques observations à faire pour que nous puissions creuser davantage cette question?

M. Michel Juneau-Katsuya: Je n'ai pas de documents officiels. Ce sont des analyses basées sur l'expérience que j'ai acquise au fil des années.

Pour obtenir de l'information plus précise, vous devriez vous adresser aux agences officielles, en particulier le Service canadien du renseignement de sécurité. M. Richard Fadden, l'ancien directeur de cet organisme, avait déjà mentionné lors d'une entrevue à la télévision que plusieurs élus de divers échelons avaient été compromis. Je crois que les agences auraient beaucoup de renseignements à ce sujet.

M. René Villemure: Je vous remercie beaucoup.

[*Traduction*]

Le président: Merci.

Nous passons maintenant à M. Green, qui aura cinq minutes et demie.

M. Matthew Green: Merci beaucoup.

Madame McPhail, vous avez mentionné la partie VI du Code criminel et rappelé qu'elle n'a pas été réexaminée depuis 20 ans. M. Deibert et vous avez longuement souligné, je crois, que la technologie outrepasse considérablement les garde-fous législatifs, et ce, de différentes manières. La partie VI a aussi été citée abondamment et très souvent par le ministre responsable et les témoins de la GRC.

Selon votre point de vue et votre opinion, quelles sont les grandes lacunes législatives actuelles de la partie VI en ce qui concerne les pouvoirs technologiques de ce genre?

Mme Brenda McPhail: La partie VI du Code criminel — je rappelle ici au Comité que je ne suis pas avocate, bien que je travaille pour un organisme de parrainage juridique — est généralement rédigée de façon à être neutre sur le plan technologique et à permettre des interrogations appropriées avec des garde-fous appropriés. Cela dit, étant donné les changements fondamentaux que connaît la technologie, je tenais simplement à dire qu'il faudrait, idéalement, que les experts de l'utilisation de cette partie puissent signaler les améliorations qui devraient y être apportées. Je ne suis pas bien placée pour me prononcer là-dessus; je tiens simplement à attirer l'attention du Comité sur cet élément important.

M. Matthew Green: Oui. Recommanderiez-vous au Comité de recommander au gouvernement d'examiner la partie VI pour s'assurer qu'elle tient compte de l'évolution de la technologie?

Mme Brenda McPhail: Oui, c'est ma recommandation.

M. Matthew Green: Professeur Deibert, êtes-vous du même avis?

M. Ronald J. Deibert: Oui, en effet.

M. Matthew Green: Je m'adresse maintenant à notre dernier témoin, dont le nom m'échappe, je m'en excuse.

Diriez-vous, vous aussi, que la partie VI ne tient pas nécessairement compte de l'évolution de la technologie et qu'elle pourrait, pour le bien et la santé de la démocratie et pour tout ce que vous avez exprimé dans votre témoignage, fournir les renseignements à jour et l'analyse juridique dont il est question?

M. Michel Juneau-Katsuya: C'est essentiel.

M. Matthew Green: D'accord.

Merci.

Le président: Merci.

Nous passons maintenant à M. Williams, qui dispose d'un maximum de cinq minutes.

M. Ryan Williams: Merci beaucoup.

Par votre intermédiaire, monsieur le président, j'adresse ma question au professeur Deibert et à Mme McPhail.

Les corps de police municipaux et provinciaux ne sont pas assujettis à la Loi sur la protection des renseignements personnels, n'est-ce pas?

● (1635)

Mme Brenda McPhail: C'est exact.

M. Ryan Williams: Pour ce qui est des recommandations à l'intention du Comité, je vous demanderais tous les deux ceci: quelles parties du Code criminel devrions-nous modifier ou recommander pour un examen dans le but de tenir compte, dès maintenant, de ces nouvelles techniques?

Mme Brenda McPhail: Comme nous venons de le dire, la partie VI du Code criminel est celle qui concerne la surveillance électronique et qu'il faudrait examiner.

M. Ryan Williams: Pardonnez-moi. J'aimerais aussi savoir ce qu'il en est pour les corps de police provinciaux et municipaux et leur utilisation de cette technologie.

Mme Brenda McPhail: Comme le maintien de l'ordre relève des provinces et des territoires, il y a en fait un ensemble hétéroclite de lois pertinentes. C'est l'un des problèmes fondamentaux qui se posent quand on veut arriver à ce que tous les services de police du pays se conforment à des normes optimales en matière d'utilisation des technologies de surveillance.

C'est pourquoi — au lieu d'adopter une approche hétéroclite et d'encourager les provinces à modifier une série de lois provinciales — je recommande d'avoir un organisme consultatif fédéral qui produira des bulletins d'information, que les provinces pourront alors utiliser et tenter de mettre en oeuvre dans leur propre juridiction, de manière à arriver à un résultat cohérent et fondé sur des pratiques exemplaires partout au pays.

M. Ryan Williams: Merci.

Monsieur le professeur, auriez-vous quelque chose à ajouter?

M. Ronald J. Deibert: Oui. J'ajouterais ceci: je ne suis pas avocat, mais s'il y a une chose que j'ai remarquée dans le cadre de mes recherches à l'échelle mondiale, c'est que l'industrie des logiciels espions est grandement intéressée à vendre ses produits aux forces policières locales, où les abus ont tendance à être particulièrement problématiques. Elle souhaite évidemment le faire dans le but d'accéder à de nouveaux clients. Je crains fortement que des agences autres que la GRC utilisent déjà ces techniques d'enquête, même si nous ne l'avons pas encore découvert.

M. Ryan Williams: Monsieur Juneau-Katsuya, vous avez parlé de l'utilisation par d'autres ministères de la technologie dont nous discutons aujourd'hui. J'aimerais savoir spécifiquement si vous connaissez d'autres technologies. La technologie dont nous parlons aujourd'hui existe depuis une décennie. Y en a-t-il de nouvelles?

Je suis conscient qu'il y a un certain temps que vous avez fréquenté certaines agences, mais êtes-vous au courant d'autres technologies qui existent, mais dont le Comité ne parle pas aujourd'hui?

M. Michel Juneau-Katsuya: Pourriez-vous préciser un peu votre question? À quelles fins...

M. Ryan Williams: Je m'en tiens au même thème, celui de la surveillance. Il pourrait s'agir de drones ou de satellites. Y a-t-il, à votre connaissance, des technologies dont nous ne parlons pas aujourd'hui, mais qui existent actuellement?

M. Michel Juneau-Katsuya: La surveillance aérienne au moyen de satellites, ou à partir de drones ou d'avions, est employée depuis des décennies. On tente de suivre l'évolution de la technologie autant que possible. Les drones sont utilisés par d'autres ministères, particulièrement par le ministère de la Défense nationale sur le théâtre des opérations. On utilise aussi d'autres méthodes que les téléphones cellulaires personnels pour suivre des véhicules et des personnes.

Bref oui, on utilise une multitude de technologies dans le but d'atténuer les menaces que posent les gens préoccupants que nous pistons.

M. Ryan Williams: Croyez-vous que la GRC utilise certaines de ces technologies? Sont-elles utilisées par divers ministères, ou par un ou deux d'entre eux?

M. Michel Juneau-Katsuya: Quand on parle de surveillance, il est important de noter que ce ne sont pas tous les outils de surveillance qui captent des renseignements; on ne recueille pas tous les renseignements. Parfois, il s'agit seulement de « marquer » une personne, un véhicule ou un objet pour pouvoir le suivre.

Donc oui, d'autres ministères utilisent des techniques et des technologies de surveillance.

M. Ryan Williams: Je reviens à ce dont nous avons discuté aujourd'hui, pour avoir votre point de vue général. Pensez-vous que nous devrions envisager des outils de protection des renseignements personnels ou voir à mener des évaluations des facteurs relatifs à la vie privée? Étant donné les technologies qui apparaissent, le commissaire à la protection de la vie privée a-t-il un rôle à jouer?

M. Michel Juneau-Katsuya: Oui, il a un rôle à jouer.

M. Ryan Williams: Très bien. Merci.

Le président: Votre temps est presque écoulé.

M. Ryan Williams: J'arrêterai ici.

Le président: Je donne donc la parole à Mme Hepfner pour le dernier tour de cinq minutes.

Madame Hepfner, à vous la parole.

Mme Lisa Hepfner: Merci, monsieur le président.

Monsieur Juneau-Katsuya, je me tourne de nouveau vers vous. Vous avez mentionné avoir l'impression que la GRC ne pourra plus utiliser sa technologie de logiciel espion si la source de cette technologie est révélée. Pourriez-vous nous expliquer plus précisément pourquoi?

● (1640)

M. Michel Juneau-Katsuya: Eh bien, contrairement au professeur Deibert, je crois — puisque nous avons nous-mêmes fait la même chose — que lorsqu'on réussit à déterminer quelle technologie un gouvernement étranger ou une cible utilise, on peut soit employer des contre-mesures, soit profiter des possibilités qu'offre cette technologie. Connaître cet élément relève du renseignement de sécurité. Il devient maintenant important de savoir quelle technologie utilise notre adversaire pour pouvoir la contrer ou en profiter, comme je l'ai dit.

C'est pourquoi le révéler ouvertement... Il n'existe pas une multitude d'entreprises qui produisent ce genre de technologie. Il y en a un bon nombre, mais pas une multitude. Donc quand on restreint le champ à partir du pays d'origine et d'autres détails du genre, on peut déduire ce qu'utilise la GRC ou n'importe quelle agence de sécurité, ce qui pourrait permettre de limiter ses capacités tactiques.

Mme Lisa Hepfner: Selon vous, pourquoi est-il dangereux que le Comité ait exploré à quelques reprises des accusations de surveillance de masse ou que l'idée de surveillance de masse, bien qu'infondée, revienne sans cesse? Pourquoi est-ce dangereux de la part du Comité, selon vous?

M. Michel Juneau-Katsuya: Il y a deux raisons. Premièrement, rien ne prouve qu'il existe une surveillance de masse. L'autre élément concerne le coût.

L'une des façons d'évaluer à quel point il est possible ou plausible qu'une technologie ait été déployée consiste à faire une analyse de coût. Une seule opération peut facilement coûter un demi-million de dollars; je parle ici d'une opération visant à faire une interception sur une cible, peut-être à partir d'un seul appareil. Il faut beaucoup de temps et de ressources pour installer le logiciel, assurer un suivi, fournir des renseignements à propos du logiciel, et parfois traduire ou expliquer l'information obtenue. Quand on additionne tous ces éléments, on voit le budget qui serait requis, et on constate qu'on ne peut pas déployer la méthode en question à grande échelle parce que cela coûterait trop cher.

Pour ce qui est de ce que M. Snowden a révélé à propos des capacités de l'agence de sécurité nationale des États-Unis, la NSA, ce serait comparer des pommes et des oranges. Le budget, les capacités et les intentions de la NSA sont fort différents de ce que la GRC, le SCRS ou le MDN seraient en mesure de déployer ici au Canada.

Mme Lisa Hepfner: Merci beaucoup.

C'est une transition parfaite, monsieur le président. Je souhaite profiter des quelques minutes qu'il me reste pour présenter une motion. Je souhaite le faire parce qu'il y a eu, au Comité, un peu trop de sous-entendus, trop d'accusations à propos d'une surveillance de masse, et même des comparaisons farfelues entre la GRC et la Stasi allemande. Nous devrions, en tant que comité, exprimer notre soutien envers le travail important qu'accomplit la GRC tout en veillant à ce qu'elle rende des comptes en vertu de la Charte canadienne des droits et libertés.

Je vais lire ma motion, et je la ferai aussi circuler parmi les membres du Comité dans les deux langues officielles. Elle se lit comme suit:

> Que le comité affirme qu'il est satisfait que la GRC n'utilise pas la technologie de Pegasus ou de l'organisme NSO; que l'utilisation des « outils d'enquête sur l'appareil » est réservée aux cas les plus graves; que l'approbation d'une demande d'utilisation des « outils d'enquête sur l'appareil » est assortie de conditions strictes et doit être approuvée en dernier ressort par un juge de la cour supérieure; que l'utilisation de ces outils sans autorisation judiciaire constituerait une infraction criminelle; et que le comité appuie la GRC dans son mandat de protéger les Canadiens contre le terrorisme, le trafic de personnes et de drogues, le blanchiment d'argent et le meurtre, tout en assurant la responsabilisation.

Il y a une petite répétition ici, je m'en excuse. La fin est répétée:

> le comité appuie la GRC dans son mandat de protéger les Canadiens contre le terrorisme, le trafic de personnes et de drogues, le blanchiment d'argent et le meurtre, tout en assurant la responsabilisation.

Je m'excuse de cette répétition. Nous enverrons le texte exact à tous les membres du Comité. J'attends avec intérêt les questions que mes collègues pourraient avoir.

● (1645)

Le président: Le greffier lira la motion avant que nous en débattions. La version électronique a-t-elle été envoyée? Parfait.

M. Matthew Green: Y a-t-il une liste d'intervenants?

Le président: Non, je ne suis pas encore rendu là.

Très bien, merci.

Je vous remercie, madame Hepfner.

La motion est recevable. Je sais que M. Green souhaite intervenir, puis Mme Khalid. Ce sont les deux noms que j'ai pour le moment.

Monsieur Green, vous avez la parole.

M. Matthew Green: Merci beaucoup, monsieur le président. Je propose que le Comité s'ajourne maintenant.

Mme Iqra Khalid: J'invoque le Règlement, monsieur le président.

Le président: Je ne peux pas entendre de rappel au Règlement si le...

Mme Iqra Khalid: J'ai levé la main tout à l'heure, pendant que Mme Hepfner lisait la motion. Je crois que personne n'avait levé la main avant moi.

Le président: J'ai donné la parole à M. Green. Je fais de mon mieux pour voir qui souhaite intervenir. M. Green cherchait aussi à attirer mon attention. En fait, je ne me prononcerai pas sur ce rappel au Règlement puisqu'une motion d'ajournement a été présentée. Lorsqu'une motion...

Mme Iqra Khalid: Je suis désolée, monsieur le président, mais j'aimerais que vous vous prononciez sur ce rappel au Règlement. La situation me semble très injuste.

M. Matthew Green: Il vient de le faire.

Mme Iqra Khalid: Je me suis déjà fait reprocher de ne pas être sur place en personne par des membres qui ne sont pas eux-mêmes sur place pour 75 % des réunions. J'apprécierais, monsieur le président, que vous vous montriez un peu plus équitable et judicieux pour ce qui est d'assurer le bon déroulement de nos réunions.

Le président: Nous continuons donc. Le greffier peut continuer.

Le vote est égal. Je vote en faveur de la motion d'ajournement.

(La motion est adoptée par 6 voix contre 5. [*Voir le Procès-verbal*])

Le président: La séance est levée.