



CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

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

ETHI • NUMÉRO 138 • 1^{re} SESSION • 42^e LÉGISLATURE

TÉMOIGNAGES

Le mardi 26 février 2019

Président

M. Bob Zimmer

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

Le mardi 26 février 2019

• (1530)

[Traduction]

Le président (M. Bob Zimmer (Prince George—Peace River—Northern Rockies, PCC)): Bonjour. La 138^e séance du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique est ouverte. Conformément à l'article 108(3)h)(iv) du Règlement, nous sommes réunis pour une séance d'informations sur le groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections.

Pendant la première heure, nous accueillons l'honorable Karina Gould, ministre des Institutions démocratiques.

Pendant la deuxième, ce sera le sous-ministre adjoint des Opérations au Centre canadien pour la cybersécurité M. André Boucher, et le chef adjoint, SIGINT, M. Dan Rogers. Nous accueillons aussi les représentants du Bureau du Conseil privé: le secrétaire adjoint au Cabinet, Appareil gouvernemental et Institutions démocratiques M. Allen Sutherland, et l'analyste principale des politiques, Institutions démocratiques Mme Ayesha Malette.

Madame la ministre, nous commençons par vous. Vous disposez de dix minutes. Vous avez la parole.

L'hon. Karina Gould (ministre des Institutions démocratiques): Je vous remercie de votre invitation. Je suis heureuse de comparaître devant votre comité et de vous expliquer en détail le plan du gouvernement pour protéger les élections de 2019.

Je suis ravie d'être accompagnée de mes adjoints, qui aborderont les aspects techniques de ce plan, c'est-à-dire, pour répéter les présentations M. Allen Sutherland, secrétaire adjoint du Cabinet, Appareil gouvernemental et Institutions démocratiques M. Daniel Rogers, chef adjoint, SIGINT, au Centre de la sécurité des télécommunications M. André Boucher, sous-ministre adjoint des Opérations au Centre canadien pour la cybersécurité Mme Ayesha Malette, conseillère principale au Secrétariat des institutions démocratiques du Bureau du Conseil privé.

[Français]

Avant de commencer, je voudrais exprimer ma gratitude aux membres du Comité pour leur contribution, au cours de la dernière année à l'étude sur la désinformation. Les témoins et les membres du Comité ont fourni de l'information et des points de vue qui se révéleront précieux à mesure que nous poursuivons nos efforts pour protéger les élections de 2019.

Les élections offrent aux Canadiens l'occasion de se faire entendre. Elles leur permettent d'exprimer leurs préoccupations et leurs opinions dans le cadre d'un des droits les plus fondamentaux qui soient: le droit de vote. Cependant, cette élection fera l'objet d'un examen minutieux sans précédent.

[Traduction]

Comme nous l'avons vu ces dernières années, les démocraties du monde entier sont entrées dans une ère nouvelle. Une ère de menaces accrues et de vigilance renforcée. L'année 2019 verra un certain nombre de pays se préparer à contrer toute une gamme de tentatives de perturbation! L'Inde, l'Australie, l'Ukraine, la Suisse, la Belgique, l'Union européenne et, bien sûr, le Canada. Les faits ont confirmé que les élections générales des plus récentes dans notre pays, en 2015, n'ont été entravées par aucun ingérence malgré des tentatives assez frustes, visant à perturber, à désinformer et à diviser. Ces tentatives peu nombreuses, probablement non coordonnées, ont eu aucun incidence visible sur l'électeur, que ce soit en ligne ou dans isoloir.

[Français]

La prochaine élection pourrait être bien différente. Nous avons constaté que les outils servant à renforcer la participation citoyenne étaient employés pour miner, perturber et déstabiliser la démocratie.

Nous nous attendons à ce que certains groupes dits «hacktivistes» utilisent leurs cybercapacités pour tenter d'influencer notre processus démocratique.

Nous pourrions également devoir faire face à des tentatives coordonnées d'ingérence de la part d'acteurs étatiques étrangers, comme cela s'est produit dans d'autres démocraties au cours des dernières années. Il peut s'agir de tentatives visant à influencer les candidats ou à abuser les médias sociaux pour diffuser de l'information faussée ou trompeuse.

[Traduction]

Ces dernières années, nous avons vu des acteurs étrangers chercher à compromettre des sociétés et les institutions démocratiques, les processus électoraux, la souveraineté et la sécurité. Nous devons nous préparer à la menace stratégique grave que posent leurs tactiques malveillantes, multiformes et en constante évolution. Voilà pourquoi, en 2017, j'ai demandé au Centre de la sécurité des télécommunications du Canada d'analyser les risques que les cybermenaces représentent actuellement ainsi que les risques de piratage des processus démocratiques du Canada et de rendre publiques son évaluation. Le rapport intitulé *Cybermenaces contre le processus démocratique du Canada* est la première évaluation publique des menaces de ce genre à être publié dans le monde. Il explique de quelle façon certains aspects clés du processus démocratique, comme les élections, les partis politiques, les politiciens et les médias, sont vulnérables aux cybermenaces et aux tentatives d'influence.

• (1535)

[Français]

Cette évaluation, la surveillance continue des services canadiens de renseignement ainsi que les expériences de nos alliés et des pays aux vues similaires dans le monde entier ont éclairé et guidé nos démarches au cours de la dernière année. Elles ont mené à l'établissement d'un plan d'action fondé sur quatre piliers.

Nous reconnaissons que la protection des institutions démocratiques du Canada exige l'adoption d'une approche qui touche tous les échelons de la société. Par conséquent, en plus de renforcer et de protéger l'infrastructure, les systèmes et les pratiques du gouvernement, nous veillons étroitement à préparer les Canadiens et à collaborer avec les plateformes numériques qui ont un rôle important à jouer pour favoriser un débat et un dialogue démocratique positifs.

[Traduction]

Les quatre piliers de notre plan sont d'améliorer la préparation des citoyens; de renforcer la préparation organisationnelle de lutter contre l'ingérence étrangère; d'encourager l'intervention des plateformes de médias sociaux.

Jevoudrais prendre quelques minutes pour souligner certaines des initiatives les plus importantes de notre plan.

Relativement au premier pilier, améliorer la préparation des citoyens, nous avons annoncé l'Initiative de citoyenneté numérique. Notre engagement comprend un investissement de 7 millions de dollars pour améliorer la résilience des Canadiens face à la désinformation en ligne. Nous tirons parti de l'expertise des organisations de la société civile qui travaillent directement dans les collectivités sur cette question.

Nous augmentons la portée et l'orientation de la campagne nationale de sensibilisation du public « Pensez cybersécurité » afin de sensibiliser les Canadiens à la cybersécurité et aux mesures simples qu'ils peuvent prendre pour se protéger en ligne.

Nous avons établi le Protocole public en cas d'incident électoral majeur. Il s'agit d'une procédure simple, claire et impartiale pour informer les Canadiens si un incident grave venait à menacer l'intégrité des élections générales de 2019.

Le protocole est appliqué par un comité constitué de cinq hauts fonctionnaires dont les décisions prises conjointement reposent sur le consensus.

[Français]

Il est important de souligner que c'est la raison pour laquelle un groupe de cinq hauts fonctionnaires a été constitué. Ce ne sera pas une seule personne qui décidera de ce que les Canadiens devraient savoir.

Le protocole ne sera mis en œuvre que pour répondre aux incidents qui surviennent pendant la période électorale et qui ne relèvent pas des responsabilités d'Élections Canada.

Le seuil d'intervention du groupe chargé d'informer la population sera très élevé et se limitera à exposer des circonstances exceptionnelles qui pourraient traverser notre capacité de tenir des élections libres et justes. À ce titre, le seuil d'intervention doit dépasser la rhétorique négative habituelle qui est parfois associée aux campagnes politiques.

Je suis reconnaissant du fait que, lors des consultations menées auprès des partis politiques sur l'élaboration de ce protocole, la partisanerie a été mise de côté dans un souci de justice. L'intégration des commentaires de tous les partis a permis l'élaboration d'un

processus équitable envers lequel les Canadiens peuvent avoir confiance.

[Traduction]

Grâce au deuxième pilier, renforcer la préparation organisationnelle, nos organismes nationaux de la sécurité et de renseignement préparent Élections Canada au moyen de conseils et de directives à toute ingérence possible dans l'administration des élections. Le Centre de la sécurité des télécommunications offre également aux partis politiques des conseils et des directives techniques en matière de cybersécurité.

Les organismes de sécurité offriront des séances d'informations sur les menaces aux principaux dirigeants des partis politiques afin de mieux les sensibiliser et de les aider à renforcer leurs pratiques et comportement en matière de sécurité interne.

[Français]

Dans le cadre du troisième pilier, qui est de lutter contre l'ingérence étrangère, le gouvernement a mis sur pied le Groupe de travail sur les menaces en matière de renseignements visant les élections, ou MSRE, afin de mieux faire connaître les menaces étrangères et d'appuyer l'évaluation et l'intervention. Cette équipe réunit le Centre de la sécurité des télécommunications ou CST, le Service canadien du renseignement de sécurité ou SCRS, la Gendarmerie royale du Canada, ou GRC, ainsi qu'Affaires mondiales Canada afin de bien comprendre des menaces qui pèsent sur le Canada et d'y réagir.

Permettez-moi de prendre quelques instants pour expliquer en quoi le Protocole public en cas d'incident électoral majeur et le Groupe de travail sur les MSRE sont des composantes distinctes mais connexes de notre approche.

Le Groupe de travail veille à ce que le travail des organismes chargés de la sécurité nationale du Canada se fasse de façon coordonnée et conforme aux mandats respectifs que la loi confère à chacun de ces organismes. Ces derniers ont leurs propres pratiques pour informer leurs structures organisationnelles internes y compris leurs dirigeants, dans le cadre de leurs pratiques opérationnelles régulières. Le Protocole ne changerait rien à cette situation.

• (1540)

[Traduction]

Le protocole ajoutera un mécanisme pour l'échange de l'information utile avec le comité de hauts fonctionnaires qui déterminera si l'incident dépasse le seuil d'intervention en gênant la tenue d'élections libres et justes au Canada.

Lorsque les dirigeants des organismes de sécurité nationale estiment qu'un incident ou des incidents pourraient menacer l'intégrité des prochaines élections fédérales du Canada, ils se concerteront avec le conseiller à la sécurité nationale et au renseignement pour informer en conséquence le comité de hauts fonctionnaires pendant une séance ordinaire ou spéciale d'information, selon les besoins.

Nous avons activé le mécanisme d'intervention rapide du G7, annoncé lors du sommet des dirigeants du G7 de Charlevoix, afin de renforcer la coordination entre nos alliés du G7 et d'assurer une collaboration et une coordination internationale au moment de faire face aux menaces à la démocratie venant de l'étranger.

Le quatrième pilier concerne les plateformes de médias sociaux.

Je n'ai pas besoin d'annoncer à votre comité que le visage des médias de masse est passé de l'ère de Gutenberg à celle de Zuckerberg en une génération. On ne saurait trop insister sur les répercussions qu'a eues cette transformation sur la société.

Il incombe aux médias sociaux et aux plateformes en ligne, qui sont les nouveaux arbitres de l'information, de gérer leurs utilisateurs. Nous savons aussi qu'on les a manipulés pour diffuser de la désinformation, créer la confusion et exploiter les tensions sociales. Les plateformes sont reconnues comme présentant une fausse information et la désinformation. J'ai rencontré leurs représentants afin de m'assurer que ces entreprises interviendront pour favoriser la transparence et l'authenticité de leurs plateformes.

Les entreprises de médias sociaux ont réagi aux incidents de 2016 en améliorant leurs plateformes. Pour commencer, notre gouvernement attend que ces améliorations soient mises à la disposition des utilisateurs au Canada comme elles l'ont été aux États-Unis et en Europe.

[Français]

Ce plan global est également soutenu par de récents efforts législatifs. Le projet de loi C-76, qui a reçu la sanction royale le 13 décembre 2018, prévoit des mesures importantes pour contrer l'ingérence étrangère et les menaces posées par les nouvelles technologies.

[Traduction]

Des dispositions de ce projet de loi interdisent notamment aux entités étrangères toute dépense visant à influencer sur l'électorat, alors qu'auparavant elles pouvaient dépense jusqu'à 500 \$ de façon non réglementée aux vendeurs d'espace publicitaires d'acceptation de publicités électorales provenant d'entités étrangères;

[Français]

ajouter une interdiction en lien avec l'« utilisation non autorisée d'un ordinateur » dans le but d'empêcher d'interrompre ou de gêner l'emploi légitime de données informatiques en période électorale et obliger les plateformes en ligne à divulguer l'identité des annonceurs en mettant à jour un registre accessible au public des annonces politiques publiées sur la plateforme pendant la période préélectorale et électorale.

[Traduction]

À remarquer que le Canada dispose d'un organisme solide et très respecté, l'administration des élections Élections Canada. Conjointement aux efforts législatifs, politiques et programmatiques que je viens de décrire, je crois que le Canada est dans la meilleure position possible pour contrer les ingérences dans nos processus démocratiques.

Bien qu'il soit impossible de prédire avec précision quel type de menaces, s'il y en a, nous verrons à l'approche des élections générales au Canada, je tiens à vous assurer que le Canada est doté d'un plan solide. Nous continuons de tester et d'évaluer notre état de préparation et nous continuerons de prendre toutes les mesures qui s'imposent pour assurer la tenue d'élections sûres, libres et justes en 2019.

[Français]

Je vous remercie,

[Traduction]

et je suis maintenant prête à répondre à vos questions.

Le président Merci, madame ministre.

Mme Vandenbeldentamerale premier tour. Les interventions durent sept minutes

Mme Anita Vandenbeld (Ottawa-Ouest—Nepean, Lib.): Madame ministre, je tiens à vous remercier de vous être déplacée et d'avoir consacré un travail incroyable pour doter le Canada de ce qui serait, d'après moi, l'un des premiers protocoles de ce genre dans le monde.

Récemment le caucus multipartite pour la démocratie a entendu Chris Walker, qui a écrit sur le « sharp power », le pouvoir qui perce, pénètre et perfore, de certains régimes autoritaires. On le distingue du pouvoir de velours parce qu'il est subversif et qu'il vise à modifier l'opinion publique à l'étranger ou à la diviser. Les menaces étrangères dont vous parlez ne sont pas uniquement dirigées contre nous. Elles visent des pays du monde entier.

Vous avez parlé du mécanisme de réaction rapide du G7. Je me demande si vous pourriez en dire un peu plus à ce sujet et, aussi, des autres formes de collaboration du Canada avec d'autres démocraties pour combattre cette menace.

• (1545)

L'hon. Karina Gould: Intéressante cette notion de « sharp power ». Je l'entends pour la première fois. Jem'informerais après la séance. Si vous avez des renseignements, n'hésitez pas à me les communiquer.

Dans le G7, nous dirigeons le secrétariat du Mécanisme d'intervention rapide, qui sera hébergé à Affaires mondiales Canada. Ce ministère, par l'examen de données de source ouverte, cherche d'abord à établir un point de comparaison pour déterminer comment les médias sociaux sont manipulés par l'ingérence étrangère. Relativement à des questions antérieures précises sur l'ingérence qui peut aussi toucher, par exemple, des éléments de la politique étrangère canadienne et réagir à des sauts d'activité.

Quand nous sommes entrés en rapport avec les Casques blancs en Syrie, par exemple, des acteurs étrangers se sont manifestement ingérés en essayant de polariser le débat ou de propager la désinformation à ce sujet.

Cela correspond aussi à notre travail de membre de l'OTAN. L'OTAN possède un centre de communications stratégique qui examine activement ces manifestations. L'automne dernier, le Canada l'a accueilli et il a invité nos partenaires des médias à le contacter à se renseigner auprès de lui sur certaines formes d'ingérence étrangère qui ont eu lieu. L'OTAN le fait dans tous ses pays membres et y invite les médias intéressés.

Membres également du Groupe des cinq, nous mettons en commun des renseignements sur les menaces et l'ingérence étrangère dans nos démocraties. Nous, les démocraties occidentales, et les pays attachés aux mêmes idées, nous en discutons beaucoup. J'ai personnellement eu des conversations avec mes homologues de France, du Royaume-Uni, d'Allemagne, d'Ukraine, de Lettonie, d'Australie et ainsi de suite, parce que nous prenons tous ces sujets très au sérieux. Nous avons constaté à maintes reprises différentes manifestations avérées d'ingérence étrangère dans les élections de notre groupe de pays.

Cela étant dit, nous continuons d'évaluer les effets de cette ingérence.

Mme Anita Vandenberg: Notre comité a entendu beaucoup de témoignages comme vous le savez, sur les méthodes par lesquelles les agrégateurs de données ont influé sur les plateformes de médias sociaux, particulièrement pour le Brexit, mais aussi dans les élections américaines.

Je remarque que vous avez mis en place le Protocole public en cas d'incident électoral majeur. Quels auraient été les effets, dans ces pays ou dans certains des autres que vous avez énumérés comme l'Ukraine ou l'Inde, de la mise en place d'un mécanisme semblable? Je sais qu'il est difficile de répondre à ce genre de question hypothétique mais par quel moyen auriez-vous pu atténuer certaines des manifestations qui se sont produites?

L'hon. Karina Gould: En fait, je pense pouvoir décrire une situation très réelle, qui n'est pas hypothétique c'est-à-dire que nous avons étudié nos alliés ou des pays qui partagent nos idées pour connaître des mécanismes qu'ils ont mis en place.

Un exemple frappant a été celui de la France, où le Conseil d'État s'est interposé après une fuite dans la campagne du candidat Macron, pour, essentiellement, la dénoncer comme une menace contre la démocratie française et conseiller aux médias de ne pas en parler.

C'est un pas de plus que ce que notre mécanisme prévoit. Nous avons essayé d'établir une marche à suivre respectueuse du contexte canadien. Le Conseil d'État, en France, existe depuis très longtemps. Il s'agissait d'éviter l'impass bureaucratique venue par exemple, aux États-Unis pendant les présidentielles de 2016 et d'éviter qu'un organisme chargé de faire respecter la loi ne fasse une déclaration publique. Il s'agissait aussi d'instituer un processus et de l'annoncer bien d'avance pour que les Canadiens comprennent ce qui conduirait à une telle annonce le cas échéant. Bien sûr, nous espérons que cela ne se produira pas et que nous ne serons pas obligés d'y recourir, mais il vaut toujours mieux se préparer au pire.

• (1550)

Mme Anita Vandenberg: Manifestement le seuil à franchir pour la mise en oeuvre sera très élevé.

Pouvez-vous donner des exemples des divers déclencheurs de ce mécanisme?

L'hon. Karina Gould: Je dois faire attention, parce que tout dépend beaucoup du contexte, et je ne voudrais pas préjuger des conclusions et de la décision du comité chargé d'appliquer le protocole.

Mais je pense qu'on peut sans crainte supposer que certains des incidents majeurs survenus dans le monde, par exemple les fuites dans la campagne de Macron ou les problèmes dans lesquels se sont débattus les États-Unis, à l'époque, suffiraient à informer les Canadiens. Mais, encore, cela dépendrait beaucoup du contexte et ce serait celui des élections canadiennes qui est différent.

Mme Anita Vandenberg: Très bien.

Dans ce cas, vu que plusieurs partis sont en cause, quels garde-fous assurent le caractère complètement politique et neutre du système et en rendent impossible la manipulation par un parti politique?

L'hon. Karina Gould: Depuis la publication du rapport du Centre de sécurité des télécommunications en juin 2017, nous nous réunissons avec les principaux partis politiques représentés à la Chambre des communes pour faciliter l'instauration d'un lien avec ce centre, pour qu'il puisse fournir des conseils techniques aux partis intéressés. Nous ignorons si les relations se poursuivent. Nous facilitons simplement les liens et nous avons rencontré régulièrement les représentants des partis politiques pour instaurer cette confiance.

Comme je l'ai dit dans ma déclaration j'ai été très encouragé par la participation des principaux partis politiques représentés à la Chambre, sur cette question. Nous élargirons aussi l'attestation de sécurité à tous les chefs élus à la Chambre ainsi qu'à trois de leurs principaux responsables de campagne, et nous les informerons continuellement.

Mme Anita Vandenberg: Merci.

Le président: Le prochain intervenant est M. Kent, qui dispose de sept minutes.

L'hon. Peter Kent (Thornhill, PCC): Merci, madame la ministre. Merci aussi à vos adjoints venus pour la deuxième heure.

Je me demande si vous avez eu le temps de lire d'abord le rapport provisoire que notre comité a déposé en juillet dernier, puis, dernière ment notre rapport définitif de décembre intitulé *Démocratie menacée: risques et solutions à l'ère de la désinformation et du monopole des données*. C'était un compte rendu très fidèle du scandale Cambridge Analytica-Facebook-Aggregate et de tentatives connexes d'ingérence dans les élections en Amérique du Nord et en Grande-Bretagne.

Je me demande quelles sont vos réactions aux recommandations de notre comité et à ses recommandations antérieures après l'étude du projet de loi sur la protection des renseignements personnels et les documents électroniques préconisant l'attribution de plus grands pouvoirs de prise de décret au commissaire à la protection de la vie privée et des sanctions plus rigoureuses plus sévères, pour les infractions portant atteinte à la vie privée des Canadiens y compris au processus électoral démocratique.

L'hon. Karina Gould: Oui, absolument. J'ai lu les deux. Comme je l'ai dit dans ma déclaration préliminaire, j'en remercie votre comité, parce que c'est vraiment du bon travail, qui, en plus, s'est fait même avant que le sujet ne devienne un enjeu vraiment accrocheur. Je vous en félicite.

Je ferais remarquer qu'on a répondu à plusieurs éléments des deux rapports et qu'on les a intégrés dans le projet de loi C-76 ainsi que dans notre annonce il y a quelques semaines sur la protection de la démocratie. Par exemple, la recommandation 5 du premier rapport est intégrée dans le projet de loi ainsi que les recommandations 8 et 8.

L'hon. Peter Kent: Le projet de loi C-76 ne vise pas le financement par des organismes étrangers de charité, par l'entremise de l'Agence du revenu Canada.

L'hon. Karina Gould: D'accord, mais pour prévenir le financement étranger et leur influence sur les élections dans notre pays... Eh bien, ça concerne le financement étranger de tiers ou de partis politiques ou de candidats à des élections.

L'hon. Peter Kent: Lead Now est financé par des organismes étrangers de charité passant par des organisations comme Tides Canada.

L'hon. Karina Gould: Je ne suis pas certaine que ce soit prouvé, mais ce serait...

L'hon. Peter Kent: Voyez le témoignage de Mme Vivian Krause, devant notre comité.

L'hon. Karina Gould: Encore une fois, le commissaire aux élections fédérales serait responsable de mener une enquête. Cet enjeu n'a pas été soulevé, et je vous encouragerais à traiter ces allégations avec prudence, mais je crois qu'il est important de souligner que dans le projet de loi C-76, qui a fait l'objet d'un examen par le Comité permanent de la procédure et des affaires de la Chambre — et j'aperçois Mme Kusie, qui a joué un rôle important dans ce dossier —, nous avons été en mesure d'obtenir un important consensus entre tous les partis pour interdire le financement étranger provenant de tierces parties dans nos élections. Cette discussion a été très productive.

• (1555)

L'hon. Peter Kent: En ce qui concerne le groupe de travail sur le Protocole public en cas d'incident électoral majeur, je me demande pourquoi on a omis la présence de deux personnes importantes à savoir le directeur général des élections et le commissaire à la protection de la vie privée, qui jouent tous les deux un rôle très pertinent, selon moi, en ce qui a trait à la protection de la vie privée et à la protection du processus électoral. Ces fonctionnaires sont certainement bien équipés pour lutter contre l'ingérence étrangère dans la sphère numérique et électronique. Étant donné les recommandations formulées par le commissaire à la protection de la vie privée ces dernières années je suis surpris qu'il ne fasse pas partie de ce groupe.

L'hon. Karina Gould: Si vous me permettez de répondre, ce groupe a été formé précisément pour traiter les menaces étrangères à l'égard de notre démocratie. Si les lois canadiennes sont enfreintes à l'échelle nationale, nous avons recours aux lois canadiennes et à des mécanismes par l'entremise du commissaire aux élections fédérales et la GRC. Dans le cas qui nous occupe, on parle spécifiquement de l'ingérence étrangère dans les élections. J'aimerais vous lire la déclaration du directeur général des élections qui, à la suite de l'annonce confirmée qu'il est un haut fonctionnaire du Parlement et qu'il ne fait donc pas partie du gouvernement du Canada :

En prévision de la prochaine élection fédérale, Élections Canada collabore avec les organismes responsables de la sécurité nationale et le commissaire aux élections fédérales. Grâce à leur expertise, il peut se concentrer sur son objectif premier : mener l'élection et veiller à ce que les Canadiens sachent où, quand et comment inscrire et voter.

En ce qui concerne la question d'une atteinte à la sécurité nationale, c'est à ce moment-là que le gouvernement du Canada et l'approche pangouvernementale par l'entremise de ce Protocole public en cas d'incident électoral majeur, entrent en jeu. Toutefois, en ce qui a trait à l'administration des élections, le directeur général des élections demeure manifestement la personne-ressource principale à laquelle les Canadiens peuvent faire confiance et sur laquelle ils peuvent compter.

L'hon. Peter Kent: En ce qui concerne les activités de ce groupe, si un incident se produit en période électorale, c'est-à-dire une situation comme l'exacerbation du scandale de SNC-Lavalin — la déclaration originale du premier ministre relative à la relation, dans les médias, d'allégations de tentatives d'obstruction à la justice, d'ingérence politique et de pressions sur l'ancienne procureure générale —, ce groupe, étant donné le témoignage du greffier la semaine dernière et si cette histoire faisait l'objet d'autres gazouillis électroniques se rangerait probablement du côté du gouvernement, comme vous l'avez dit, ce qui mettrait en doute ses compétences.

L'hon. Karina Gould: À des fins d'éclaircissement je n'ai jamais dit que le greffier se rangerait du côté du gouvernement dans une situation comme celle que vous venez de décrire. Ce qui est important, et ce que j'ai dit, c'est qu'il y aura un groupe composé de

cinq hauts fonctionnaires. Ces gens seront avisés par les dirigeants des organismes responsables de la sécurité nationale pertinents.

Si ces dirigeants d'organismes responsables de la sécurité nationale ont des motifs suffisants de croire qu'un incident mérite leur attention, et que cet incident a une portée suffisante pour nuire à la capacité de mener des élections libres et justes, et qu'il s'agit d'une menace étrangère ce groupe de cinq personnes devra prendre une décision collective, fondée sur un consensus sur la question de savoir si le public sera informé ou non.

En même temps, tous les grands partis politiques représentés à la Chambre des communes, leur leader et jusqu'à trois membres de leur personnel supérieur de leur choix recevront une autorisation de sécurité. À des fins de transparence ils seront tous informés en même temps de la situation et ils recevront donc tous les mêmes renseignements. C'est un élément très important de ce processus pour veiller à ce que tout le monde obtienne des mêmes enseignements au même moment.

L'hon. Peter Kent: S'il y a des différences d'opinion entre les représentants des partis et les recommandations du Comité, comment cette situation sera-t-elle résolue ?

L'hon. Karina Gould: Cette décision revient au groupe de travail, et non aux partis politiques, mais ils recevront tous l'information en même temps.

Le président: Merci, monsieur Kent.

La parole est à M. Angus. Il a sept minutes.

M. Charlie Angus (Timmins—Baie James, NPD): Merci, madame Gould, d'être ici aujourd'hui.

Quel représentant de Facebook avez-vous rencontré ?

L'hon. Karina Gould: J'ai rencontré Kevin Chan, de Facebook. Il faudrait que je trouve le nom des cinq autres intervenants car je ne me souviens pas...

• (1600)

M. Charlie Angus: Vous avez rencontré Kevin Chan, qui n'est pas inscrit au registre des lobbyistes, qui a rencontré plusieurs personnes au bureau du gouvernement et qui est un ancien membre qui travaillait pour les libéraux. Kevin Chan était-il votre voix ?

L'hon. Karina Gould: Je suis désolée, monsieur Angus, mais pourriez-vous me laisser parler ?

M. Charlie Angus: Je demande si c'était Kevin Chan ? Nous avons étudié ce dossier pendant plus d'un an et nous n'avons pas pu obtenir une réponse claire de Facebook. Si Kevin Chan était votre source, je veux que cela soit ajouté au compte rendu.

L'hon. Karina Gould: Monsieur Angus, j'ai dit que nous avions aussi rencontré cinq autres personnes de Washington et de Silicon Valley.

M. Charlie Angus: Ces personnes avaient-elles des postes plus élevés ou moins élevés que Kevin Chan ? Pourriez-vous nous donner leurs noms ?

L'hon. Karina Gould: Je serais heureuse de vous donner leurs noms, mais je ne les ai pas en ce moment.

M. Charlie Angus: Merci.

Je présume que je suis un peu sur les nerfs. Nous avons étudié ce dossier pendant plus d'un an. Nous avons mené des travaux à l'échelle nationale et internationale. Je vois le rapport que vous avez produit. Il fait tellement « guerre froide ». Nous avons le mécanisme d'intervention rapide du G7, nous avons le groupe d'évaluation critique. Tout ce que nous avons trouvé est exactement le contraire de ce que vous présentez.

Vous n'avez pas tenu compte de nos principales recommandations, dont celle qui concernait le rôle du directeur général des élections, qui sera maintenant sous Michael Wernick, du Conseil privé. Cependant nous avons toujours dit que le directeur général des élections jouait un rôle important. Pendant les élections, les esprits s'échauffent. Si l'équipe du mécanisme d'intervention rapide du G7 que vous avez formée annonce soudainement la présence d'une menace, cela pourrait réellement déstabiliser une élection. Nous avons besoin d'inspirer la confiance.

L'hon. Karina Gould: Il est important de préciser les rôles...

M. Charlie Angus: Il faudrait inspirer la confiance, n'est-ce pas ?

L'hon. Karina Gould: ... et de ne pas fusionner des enjeux différents.

M. Charlie Angus: C'est la raison pour laquelle je me demande pourquoi vous avez nommé Michael Wernick et non le directeur général des élections pour prendre cette décision pour les Canadiens.

L'hon. Karina Gould: Si vous me laissez parler, je serai heureuse de répondre à votre question.

Comme je viens littéralement de le dire à M. Kent il y a moins de deux minutes, je répéterai ce que le directeur général des élections a dit...

M. Charlie Angus: J'ai entendu cela...

L'hon. Karina Gould: ... et c'est...

M. Charlie Angus: ... mais je demande pourquoi M. Wernick n'est pas le...

L'hon. Karina Gould: ... qu'il est un haut fonctionnaire du Parlement, et qu'il ne fait donc pas partie du gouvernement du Canada. C'est une fonction distincte.

M. Charlie Angus: D'accord.

L'hon. Karina Gould: Dans le cas d'un enjeu lié à la sécurité nationale, c'est le gouvernement du Canada qui s'occupe.

M. Charlie Angus: D'accord.

L'hon. Karina Gould: En période d'élection, nous avons ce que nous appelons la convention de transition...

M. Charlie Angus: Oui.

L'hon. Karina Gould: ... qui prend la relève pour assurer la continuité des activités du gouvernement. Il est important que...

M. Charlie Angus: Oui, je comprends cela. Ce qui me préoccupe, c'est...

L'hon. Karina Gould: ... les intervenants politiques ne soient pas compromis à cet égard.

M. Charlie Angus: ... que comme M. Wernick, je suis préoccupé par la montée de l'extrémisme politique, mais j'étais très surpris qu'il parle d'assassinat politique au beau milieu d'une audience parlementaire qui servait à déterminer si le gouvernement avait mal agi.

Ne vous rendez-vous pas compte que cela va à l'encontre des règles selon lesquelles le Conseil privé ne doit pas intervenir dans les questions de conjoncture et de controverse ? Pourtant il a commencé à répondre à la question du groupe de travail qui cherchait à

déterminer si le gouvernement avait interféré avec la primauté du droit ou non et il a non seulement établi un lien avec l'assassinat politique, mais il a aussi dit ce qui suit:

Jem'inquiète au sujet de la réputation de personnes honorables qui ont servi leur pays avant d'être souillées et traînées dans la boue sur la place publique. Je m'inquiète au sujet des trolls, qui émergent des réseaux sociaux pour aller hanter l'arène des médias publics. Plus que tout, je m'inquiète du fait que des gens perdent foi...

Est-ce la position du gouvernement ou est-ce son opinion ?

L'hon. Karina Gould: Il faudrait que vous lui posiez la question.

M. Charlie Angus: D'accord.

L'hon. Karina Gould: D'après ce que je comprends c'était son opinion personnelle.

M. Charlie Angus: D'accord.

Parce que selon les lignes directrices à l'intention des fonctionnaires du Conseil privé — et je crois que les gens à côté de vous les ont lues —, et je cite: « Un fonctionnaire est habilité à donner des explications en réponse aux questions relatives à des aspects complexes de stratégie, mais il ne doit pas chercher à défendre une stratégie ni à participer à un débat. Pour les autres questions, surtout en ce qui a trait à l'administration du ministère et des programmes, cela doit être strictement limité. » Les questions de stratégie de politique qui risquent de soulever une controverse sont essentiellement réservées aux ministres, car si les fonctionnaires devaient rendre compte des politiques, ils seraient inévitablement entraînés dans des polémiques qui mettraient fin à leur utilité [politique] à long terme pour le système et mineraient l'autorité et la crédibilité de leur ministre. »

Ce qui me préoccupe, c'est que M. Wernick, en profitant d'une audience de comité pour présenter toutes sortes de conjectures politiques personnelles — premièrement pour parler de l'éthique du premier ministre, deuxièmement pour louer Mme Bennett, troisièmement, pour dénoncer les critiques dont elle a fait l'objet sur Twitter —, a utilisé sa position pour faire progresser une cause, ce qui met fin à son utilité à titre de personne à laquelle nous pouvons tous faire confiance en cas de tension politique.

Ne voyez-vous pas cela ?

L'hon. Karina Gould: Une personne responsable de superviser les activités de l'ensemble du gouvernement sera certainement dans une position unique relativement à ses impressions et aux menaces qu'elle voit se profiler à l'horizon.

Je crois qu'il est très important de reconnaître qu'en élaborant le Protocole public en cas d'incident électoral majeur, nous avons délibérément créé un groupe de travail composé de cinq hauts fonctionnaires afin qu'il ne revienne pas à un seul fonctionnaire de prendre cette décision...

● (1605)

M. Charlie Angus: Et je n'aurais rien eu à dire au sujet de M. Wernick avant son témoignage...

L'hon. Karina Gould: ... d'amorce une conversation et d'évaluer ces enjeux.

M. Charlie Angus: ... mais étant donné qu'à titre de chef du Conseil privé, il a des obligations liées aux sujets sur lesquels il peut donner son avis, il a tout de même dit, au sujet de Mme Bennett, qu'il était profondément blessé des atteintes à sa réputation, que des choses méchantes avaient été dites, et qu'aucun autre Canadien n'avait travaillé plus fort à la réconciliation avec les peuples autochtones que l'honorable Carolyn Bennett...

C'est peut-être le cas, mais les gens qui l'ont remise en question sur Twitter sont des représentants autochtones qui n'appuient pas la position. Donc, s'il pense que ces propos sont méchants, ce qui me préoccupe, c'est que lorsque des gens diront des choses qui soulèveront la controverse pendant une élection — et cela arrivera — et lorsque les gens nous attaqueront et qu'ils attaqueront le gouvernement, comment pouvons-nous avoir l'assurance que M. Wernick saura faire la différence entre les critiques justes et celles qui ne le sont pas?

Le fait qu'il se soit prononcé sur des questions qui soulèvent la controverse sans tenir compte de ses obligations me pousse à le remettre en question, alors que je ne mets pas en question le directeur général des élections. Mais je me pose certainement des questions au sujet de cette équipe sur les incidents que vous avez formés avec M. Wernick.

L'hon. Karina Gould: J'aimerais répéter, monsieur Angus, que les membres du groupe de travail que nous avons créé ne se réuniront pas à moins que les organismes responsables de la sécurité nationale soulèvent un problème de sécurité nationale qui doit être examiné par ce groupe, ce qu'ils pensent...

M. Charlie Angus: Ne serait-il pas préférable que le directeur général des élections confirme qu'il s'agit d'un problème grave, car Michael Wernick semble penser que le fait que des gens attaquent des ministres dépasse les bornes...

L'hon. Karina Gould: Donc, encore une fois, la réponse, c'est que le rôle du directeur général des élections consiste à agir à titre de fonctionnaire du Parlement et à administrer les élections.

M. Charlie Angus: Merci.

L'hon. Karina Gould: C'est un enjeu distinct et ils jouent tous les deux un rôle distinct.

En ce qui concerne le groupe de travail, il est extrêmement important de répéter que ses membres ne se réuniront que si l'un des dirigeants des organismes responsables de la sécurité nationale juge avoir observé une ingérence étrangère assez importante pour réunir les membres de ce groupe pour informer...

M. Charlie Angus: Nous devons gagner la confiance du public, et c'est ma question. Si M. Wernick n'a pas respecté ses obligations liées au Conseil privé, avons-nous cette confiance? Je ne suis pas certain que cette confiance existe actuellement.

Le président: Merci, monsieur Angus.

La parole est maintenant à M. Saini. Il a sept minutes.

M. Raj Saini (Kitchener-Centre, Lib.): Bonjour, madame la ministre. Je vous remercie beaucoup d'être ici aujourd'hui, surtout avec vos collègues.

J'aimerais d'abord poser une question sur l'un des piliers que vous avez mentionnés, c'est-à-dire le courage d'intervention des plateformes de médias sociaux. Je sais que vous avez parlé de transparence avec leurs représentants pour veiller à ce que les gens qui font de la publicité ou qui paient pour faire de la publicité — et nous savons de qui il s'agit — pour lutter contre la diffusion de renseignements erronés.

Toutefois, j'aimerais que votre ministère ou les fonctionnaires qui sont ici formulent des commentaires sur un certain point. Parfois, par exemple sur Reddit ou Facebook, il y a une section réservée aux commentaires. Parfois, cette section peut être infiltrée par des intervenants étrangers ou d'autres intervenants qui souhaitent perturber notre mécanisme électoral en disséminant des renseigne-

ments erronés dans la section des commentaires. Envisageons-nous d'adopter un protocole pour prévenir ce type de situation?

L'hon. Karina Gould: Le gouvernement envisage pas d'intervenir dans les conversations qui se déroulent sur les plateformes sociales et numériques. Ce n'est pas le rôle du gouvernement.

Toutefois, nous nous attendons à ce que les plateformes et les médias sociaux adoptent une attitude et des mesures plus responsables relativement à l'utilisation de leurs plateformes pour diffuser des renseignements erronés.

Manifestement, c'est plus compliqué dans le cas d'une section réservée aux commentaires que dans le cas d'une publication. Toutefois, nous nous attendons à ce que ces plateformes éliminent les comportements et les comptes non authentiques. Les représentants de Twitter et de Facebook nous ont parlé du nombre de comptes qu'ils ont éliminés. Dans les deux cas, il s'agit de millions de comptes et je pourrais vous envoyer les nombres précis que nous avons reçus si cela vous intéresse. Je ne connais pas tout à fait le mécanisme qui pourrait être utilisé par ces plateformes pour gérer la section réservée aux commentaires, mais si elles attaquent aux faux comptes ou aux comptes étrangers qui prétendent être des intervenants nationaux légitimes, cela pourrait contribuer à résoudre ce problème.

M. Raj Saini: Vous avez parlé du mécanisme d'intervention rapide du G7. Je ne connais pas le contenu des ententes de partage de renseignements, mais manifestement elles visent à solidifier le système dans tous les pays du G7. Je ne suis pas nécessairement inquiet à cet égard, car je pense que le G7 a suffisamment de ressources pour créer un système solide.

Ce qui me préoccupe, c'est plutôt le cas des démocraties naissantes ou même au-delà du G7, c'est-à-dire le G20. Récemment, des élections ont eu lieu au Nigeria et on a avancé l'hypothèse selon laquelle il y avait eu une ingérence étrangère dans ces élections. Une telle ingérence a déjà eu lieu au Nigeria avant cette élection. Vous avez mentionné d'autres pays.

Si vous renforcez les pays du G7, c'est excellent, mais cela ne fait rien pour les autres démocraties. Le gouvernement ou votre ministère a-t-il déjà réfléchi aux pratiques exemplaires ou aux pratiques éprouvées qui pourraient être communiquées à d'autres pays qui n'ont peut-être pas les mêmes ressources ou la même capacité que notre pays?

• (1610)

L'hon. Karina Gould: Je mets vraiment l'accent sur la démocratie au Canada. Quand j'ai eu des discussions avec des homologues étrangers, c'était vraiment pour tirer des leçons de leurs expériences et voir ce qui pouvait être appliqué ici, dans le contexte canadien.

Je dirais qu'en dehors de l'Union européenne et du Canada, on trouve la voie pour ce qui est de protéger notre démocratie contre les cybermenaces venant de l'étranger. Les éléments que nous avons annoncés le 30 janvier forment la base de cela.

Cela étant dit, je sais que des efforts sont déployés afin de garantir que tout ce que nous apprenons est transmis à nos homologues et alliés étrangers. J'ai appris que divers autres pays se tournent vers nous également pour savoir ce que nous faisons et pour voir comment appliquer cela sur leur propre territoire.

M. Raj Saini: Ma dernière question est plutôt personnelle. Comme vous le savez, nous serons bientôt en campagne électorale, et il se dira peut-être des choses vraies ou fausses sur les réseaux sociaux au sujet de certains candidats. Quel est le mécanisme qui permet de contrer les faussetés?

L'hon. Karina Gould: Dans le projet de loi C-76, il y a eu un resserrement conforme aux recommandations de l'ancien DGE d'Élections Canada. Il s'agissait de ressermer le libellé entourant les fausses déclarations relatives à des candidats. La disposition antérieure de la Loi électorale du Canada était trop vague et impossible à appliquer. Nous l'avons resserré afin qu'elle se fonde sur des énoncés qu'on pouvait prouver ou réfuter.

Par exemple, si quelqu'un accuse un candidat d'avoir un dossier criminel, il est possible de prouver ou de réfuter cela. Aux termes de la Loi électorale du Canada, le mécanisme est une plainte qu'on dépose auprès du commissaire aux élections fédérales, lequel doit ensuite répondre.

On a augmenté les ressources affectées au commissaire et il y a un autre élément très important, et c'est que le poste de commissaire est retourné au sein d'Élections Canada et qu'en plus, il est maintenant habilité à déposer des accusations et à contraindre des personnes à témoigner. Les pouvoirs du commissaire ont été affermis, ce qui lui permet d'appliquer la loi plus efficacement.

M. Raj Saini: Un de vos piliers est d'améliorer la préparation des citoyens, car plus les citoyens sont bien informés, plus le système sera robuste. Il y aura moins d'ambiguïté. Vous avez mentionné quelque chose dans votre déclaration liminaire au sujet de la création d'une initiative de citoyen numérique.

Pouvez-vous nous en dire un peu plus à ce sujet?

L'hon. Karina Gould: L'un des meilleurs conseils que j'ai entendus, mais surtout le plus pertinent, probablement, c'est que quand il est question de cybermenaces contre notre démocratie au bout du compte, c'est le citoyen qui est la cible. Partout dans le monde, nos homologues ont souligné le fait qu'une population résiliente représente la meilleure arme contre les campagnes de désinformation.

Nous avons annoncé pour notre initiative citoyenne numérique, un montant de 7 millions de dollars qui servira à financer des organisations de la société civile dans les domaines des médias numériques et des connaissances civiques. C'est une initiative d'une extraordinaire importance. Au cours des dernières années, et particulièrement dans le contexte des élections américaines de 2016, les démocraties occidentales ont été un peu secouées après avoir constaté que nous tenions notre démocratie pour acquise en quelque sorte. Il est important de veiller à ce que nous continuions de parler de démocratie et de valeurs démocratiques dans notre propre pays, sans quoi nous risquons de les perdre.

Le président: Merci, monsieur Saini.

Madame Kusie.

Mme Stephanie Kusie (Calgary Midnapore, PCC): Madame la ministre, c'est toujours un plaisir de vous voir. J'aime beaucoup votre collier, en passant il est magnifique.

L'hon. Karina Gould: Merci.

Mme Stephanie Kusie: Je veux également dire que j'ai vraiment aimé votre discours hier à l'événement relatif à l'IA. C'était très informel. Je crois que vous devriez d'ailleurs opter pour ce format, même quand vous comparez devant des comités. Vous le faites si bien. Je voudrais vous complimenter à ce sujet.

Vous avez beaucoup parlé des vulnérabilités. C'était un thème majeur pour vous. Bien entendu, au sein de l'opposition, nous prenons très au sérieux notre responsabilité de demander des comptes au gouvernement concernant la protection des élections. Je dirais qu'à presque chaque étape, nous avons l'impression que le gouvernement échoue et ne va pas assez loin dans les mesures qu'il devrait prendre pour protéger les élections.

Je donnerais des exemples tirés du projet de loi C-76.

Le registre des plateformes sociales, qui représente des renseignements des plus essentiels à mon point de vue, n'est peut-être pas allé assez loin concernant la protection des Canadiens et la diffusion de renseignements ainsi que la gestion des données.

Mon collègue a mentionné l'aspect de l'ingérence étrangère. C'est une chose que j'ai déjà dite plusieurs fois. Nous, de l'opposition, avons présenté plus de 200 amendements. Un grand nombre de ces amendements ont été rejetés. Comme je l'ai dit précédemment, je pense très fermement que ce que nous avons pour l'ingérence étrangère avec le projet de loi C-76, c'est une tape sur les doigts. C'est comme dire: « Ce n'est pas beau. Vous ne devriez pas faire cela. » Il aurait plutôt fallu inclure dans la loi des mécanismes précis, comme des comptes bancaires distincts, ce qui rendrait impossible l'ingérence étrangère sur le plan financier.

Concernant plus particulièrement que mon collègue, l'honorable Peter Kent, a mentionné il y a le financement en dehors des périodes électorales et préélectorales soit la période ouverte en fait. Commencez en sommes enus à le constater cela affecte d'autres aspects de notre démocratie dont l'immigration et l'approbation des oléoducs, dossier que j'ai particulièrement à cœur en tant qu'Albertaine.

Ce n'est que le début. Je ne vais certainement pas entrer dans les détails de nos points de vue concernant les vulnérabilités créées par le vote des non-résidents, les cartes d'électeur et les modifications apportées aux dispositions visant le recours à un répondant dans le projet de loi C-76. Vous avez dit que c'était très important pour vous-même et pour le gouvernement. Cependant, on ne prend pas les mesures qui seraient absolument nécessaires afin de faire vraiment tout ce qui est possible pour protéger ces processus électoraux. Cela a été abordé hier. Mon collègue, M. Saini, a mentionné cela brièvement dans ses questions tout à l'heure. Cela a été mentionné par un ancien membre du gouvernement libéral et du cabinet libéral, une personne que je respecte beaucoup et qui est un ancien collègue des Affaires étrangères Allan Rock. Il était question, encore une fois, de la gestion des plateformes de médias sociaux.

Bien entendu, nous recherchons toujours un équilibre dans la société. Comme je l'ai indiqué dans mon témoignage devant le comité PROC, la semaine dernière, nous devons faire confiance à ces sociétés dont l'objectif est de maximiser la valeur des actions, pour qu'elles assument la responsabilité de s'autoréguler. Cela suscite naturellement des questions et d'autres concernant la liberté d'expression et ainsi de suite. Il mentionnait une préoccupation au sujet de laquelle il faudrait peut-être faire plus que de l'encouragement. Je suis aussi préoccupé par votre réponse sur ce qui semble être votre réponse. Je vais vous donner la chance d'en parler. Vous semblez vouloir confier au comité PROC la réalisation d'une étude qui couvrirait vos arrières: si vous décidez d'opter pour des mesures législatives, vous pourriez dire que le comité a réalisé une étude et que c'est ce qu'il vous a dit.

Je vous demande si vous êtes prête, en ce qui concerne les plateformes de médias sociaux, à prendre des décisions difficiles et à adopter des mesures rigoureuses et ce, maintenant et non dans six mois.

• (1615)

L'hon. Karina Gould: Je vous remercie, madame Kusie. Je sais que vous avez en fait proposé une motion pour que le comité PROC se penche sur cet enjeu.

Mme Stephanie Kusie: En effet.

L'hon. Karina Gould: Oui, pour que ce comité prenne la décision.

Je veux éclaircir quelque chose d'important, parce que c'est la deuxième fois que vous le mentionnez et c'est que dans le projet de loi C-76, les tiers sont maintenant tenus d'avoir des comptes bancaires distincts de manière à pouvoir rendre compte de toutes les entrées d'argent. Je pense que c'était un enjeu très important à soulever, en particulier pour déterminer la provenance de l'argent.

En ce qui concerne des vulnérabilités que j'ai mentionnées hier et que j'ai souvent mentionnées à ce sujet, vous pouvez les trouver directement dans le rapport du CST sur les cybermenaces contre notre démocratie. Le rapport signale très clairement que les principales menaces relatives à l'ingérence informatique visent principalement des personnes politiques, les partis politiques et les médias — dans tous les cas où il y a des interactions humaines. Comme c'est souvent le cas, d'un côté, ces particuliers et intervenants n'ont pas nécessairement les pratiques qui leur permettent d'assurer la sécurité de leurs données comme l'authentification à deux facteurs et les mesures qui leur servent à protéger leurs comptes le mieux possible, mais en plus, ils sont vulnérables aux stratégies et aux campagnes d'influence. Ce sont les vulnérabilités dont je parlais.

En ce qui concerne le projet de loi C-76, je suis généralement très fière parce que je pense que son objectif premier est de garantir à tous les Canadiens la possibilité de voter. Je pense que c'était un facteur vraiment important dans le choix d'améliorer les modalités relatives au répondeur pour nos Canadiens les plus vulnérables, de veiller à ce que la carte d'information de l'électeur puisse servir comme preuve de résidence car nous savons par exemple que c'est souvent un obstacle pour les femmes âgées qui sont seules, parce qu'il arrive souvent qu'elles n'aient pas de pièces d'identité prouvant leur résidence.

• (1620)

Le président: Merci. Le temps est écoulé.

C'est maintenant au tour de M. Erskine-Smith. Vous avez cinq minutes.

M. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Je vous remercie de votre présence, madame la ministre.

Notre comité a recommandé d'imposer aux plateformes de médias sociaux l'obligation de retirer rapidement le contenu manifestement illégal, y compris les propos haineux, le harcèlement et la désinformation sans quoi elles risqueraient des sanctions pécuniaires. J'aimerais lire un commentaire. C'était en réponse à un article au sujet des propos haineux et des menaces venant du mouvement des gilets jaunes. Ce qui est intéressant, c'est que je pense que s'ils savaient que le mouvement des gilets jaunes en France réclame un impôt sur la richesse et un salaire minimum, le mouvement des gilets jaunes canadiens voudrait peut-être pas tant s'associer à eux. Quoi qu'il en soit, ils ont dit de M. Trudeau qu'il est un traître à notre pays et qu'il mérite d'être pendu pour trahison. Cela a été dit sur Facebook et c'est resté sur Facebook. Facebook ne retire pas cela. Est-

ce que nous devrions nous attendre à ce que les entreprises de médias sociaux agissent ou est-ce que nous devrions plutôt les obliger à agir?

L'hon. Karina Gould: Je devrais préciser que mes attentes doivent être liées au contexte électoral en ce moment, étant donné que je suis la ministre des Institutions démocratiques. Cela étant dit, je crois qu'à voir où vont les choses, nous allons devoir exiger des entreprises de médias sociaux qu'elles agissent. Cela ne relève pas de mon mandat particulier en ce moment, mais je pense que devant une preuve très claire de infractions qu'elles commettent ici au Canada, ces entreprises devraient agir de manière responsable.

M. Nathaniel Erskine-Smith: Je vous remercie. Donc, dans le cadre de votre mandat, nous avons le projet de loi C-76 qui crée comme il se doit un registre des annonces diffusées aussi bien en période électorale qu'en période préélectorale. Est-ce que les conversations que vous avez eues avec Facebook et d'autres entreprises vous permettent de croire avec assez de certitude qu'elles vont veiller à ce que la base de données soit aussi accessible que possible, en particulier pour les journalistes?

L'hon. Karina Gould: Facebook m'en a donné l'assurance. Je sais que toutes les entreprises de médias sociaux cherchent à parler avec les gens d'Élections Canada afin d'obtenir des éclaircissements, car au bout du compte, c'est Élections Canada qui va interpréter la loi et déterminer comment les choses se passent. Cependant, d'après ce que je comprends, elles essaient de rendre cela accessible aux Canadiens.

M. Nathaniel Erskine-Smith: En ce qui concerne le projet de loi C-76, l'accent est mis sur la transparence des activités publicitaires, et c'est vraiment important. Cependant, quand M. Zimmer et moi étions à Washington en juillet dernier pour une table ronde, quelqu'un a fait un commentaire intéressant. Le sénateur Warner dit que quand ils ont commencé à étudier cette question, leur attention se portait principalement sur la publicité, mais il s'est avéré que ce n'était que la pointe de l'iceberg. Le piratage des algorithmes eux-mêmes était le véritable problème, que ce soient les fermes à trolls de l'Internet Research Agency ou d'autres organisations. En quoi estimez-vous que les mesures prises par votre bureau représentent une solution à ce problème?

L'hon. Karina Gould: J'ai aussi lu le rapport du sénateur Warner. Il est très intéressant sur ce plan, et c'est probablement un des meilleurs rapports que j'ai lus.

J'ai tendance à voir les mesures que nous avons prises comme étant des mesures visant à résoudre des problèmes que nous avons connus jusqu'à maintenant. Il est entendu que c'est un domaine qui évolue et que notre compréhension des enjeux continue de s'améliorer.

En ce qui concerne la divulgation complète, à titre de ministre responsable de ce portefeuille, je vais vous dire que quand je me suis penché à-dessus, je pensais aux tentatives de piratage et aux fuites. Au cours des deux dernières années, notre compréhension de l'enjeu a radicalement changé. En ce moment, à l'échelle de la communauté internationale ainsi qu'ici même au Canada, nous essayons de comprendre profondément l'ampleur de l'enjeu et de trouver des solutions qui nous permettront de nous attaquer à la source du problème. Je remercie d'ailleurs le Comité de votre travail, parce qu'il est très important pour éclairer les prochaines étapes.

• (1625)

M. Nathaniel Erskine-Smith : Vous avez mentionné le piratage. J'ai lu le rapport du CST sur les cybermenaces, je crois comprendre qu'une nouvelle menace serait en train d'émerger, mais j'ai lu le dernier rapport. On y dit que l'intégrité du système électoral est excellente et qu'on ne s'inquiète pas tant du risque de piratage d'Élections Canada ou du système de vote, mais que ce sont les acteurs politiques qui représentent la plus grande faiblesse de tout cela. Nous avons déjà des députés et des sénateurs qui ont été victimes de piratage.

Par conséquent en ce qui concerne les 7 millions de dollars destinés à une initiative de citoyenneté numérique — et je crois que ce sont 7 millions de dollars à l'échelle du pays —, comment allons-nous éduquer les Canadiens ici au mois d'octobre ? Est-ce qu'il ne serait pas préférable de consacrer ces 7 millions de dollars à l'éducation des politiciens, du personnel politique, des bénévoles et des associations de circonscription — à mon éducation et à celle de mon personnel et de mes bénévoles, pour que nous sachions comment protéger nos comptes des pirates ?

L'hon. Karina Gould : Cela s'accompagne d'une question de privilège parlementaire en ce sens que le Parlement décide de l'information que vous choisissez d'utiliser et de ne pas utiliser. Dans l'annonce, nous avons inclus une série de graphiques et d'outils éducatifs que j'invite tous les parlementaires et les Canadiens à consulter et à utiliser pour savoir comment mieux se protéger.

Le centre de cybersécurité du CST, dont André pourra vous parler un peu tout à l'heure, est en place, mais il sera à la disposition des parlementaires ainsi que des politiciens et de leurs entités politiques s'ils le veulent, et nous allons raffermir la campagne de cybersécurité également. Nous allons ainsi assumer notre responsabilité de veiller à faire preuve de leadership dans ce domaine.

Cela étant dit, vous pourriez mettre les meilleures mesures en œuvre pour assurer votre cybersécurité et être quand même victime de piratage.

Le président : Merci.

À titre d'information, trois autres députés vont poser des questions. Nous avons commencé un peu tard. Nous espérons que ce n'est pas un problème pour la ministre.

C'est maintenant au tour de M. Gourde, qui a cinq minutes.

[Français]

M. Jacques Gourde (Lévis—Lotbinière PCC) : Merci, monsieur le président.

Merci d'être ici, madame la ministre.

Les Canadiens seront sans doute très préoccupés par ce qu'on a entendu au sujet des menaces numériques générées par Facebook. Ce qu'on a entendu à la dernière élection aux États-Unis pourrait sans doute se répéter au Canada.

Il est difficile de rattraper ou de dénoncer cette fameuse publicité et les fausses nouvelles qu'on publie sur Facebook, et cela prend énormément de temps. Une nouvelle annoncée sur Facebook peut faire la manchette pendant 24 ou 48 heures, même si elle est complètement fautive, peu importe le parti attaqué. Ensuite, on va entendre dire que ce n'était pas vrai, mais la nouvelle s'est déjà répandue dans le public ou a déjà pénétré dans la tête des Canadiens. Si cela se passe à répétition, on a beau avoir un comité de travail disant qu'il ne faut pas faire cela, ce n'est pas suffisant.

De quelle façon va-t-on annoncer publiquement que ce sont de fausses nouvelles ou de fausses allégations qui se retrouvent dans les médias, comme Facebook ?

L'hon. Karina Gould : Comme je l'ai dit, je ne crois pas que ce soit le rôle du gouvernement de décider quelles nouvelles sont fausses et lesquelles sont véridiques. C'est une problématique du XXI^e siècle. Nous habitons effectivement dans un monde médiatisé où les nouvelles voyagent très rapidement. Je pense que le rôle et la responsabilité des médias traditionnels sont aussi de s'assurer de ne pas rapporter de fausses nouvelles. De plus, bien sûr, les politiciens disposent de plateformes pour dire ce qu'ils pensent. Les propriétaires des plateformes numériques ont aussi une responsabilité de s'assurer qu'elles ne sont pas manipulées.

Je suis toujours optimiste, mais réaliste également, et je veux souligner que, pendant les élections présidentielles aux États-Unis, les responsables des plateformes numériques n'ont pas essayé de dévoiler ce genre de manipulations d'activités. Au moins, ils le font maintenant et tentent d'éviter ce type d'abus. Bien sûr, ce n'est pas suffisant. Ce n'est pas tout ce qu'ils pourraient faire, mais, au moins, les gens sont plus au courant de ce genre de désinformation. Comme je l'ai dit déjà, ce n'est pas la solution, mais l'une des choses qui pourraient être faites serait de sensibiliser les Canadiens à ces menaces pour qu'ils puissent prendre des décisions éclairées quand ils écoutent les nouvelles, qu'elles soient réelles ou fausses.

• (1630)

M. Jacques Gourde : Est-ce le rôle d'Élections Canada de faire une campagne de sensibilisation au début de la campagne électorale en vue de sensibiliser les Canadiens quant à cette réalité, de leur dire d'y porter une attention particulière et d'en faire part s'ils entendent de fausses nouvelles ou s'ils se sentent égarés par ce qui se passe dans les médias sociaux ?

L'hon. Karina Gould : C'est une excellente question. Comme Élections Canada est un organisme indépendant du gouvernement, ce serait peut-être une question à poser à son directeur général. Je peux dire cependant que, dans le projet de loi C-76, nous avons redonné au directeur général des élections le pouvoir d'informer les Canadiens sur les élections. Si c'est un sujet qui l'intéresse, il pourrait en parler aux Canadiens.

M. Jacques Gourde : Il est clair que la prochaine élection sera cruciale. Dans ce nouvel environnement médiatique, nous allons tous suivre cela de près, du moins en tant que législateur et acteurs dans le milieu politique. Devons-nous nous préparer à poser des gestes après l'élection de 2019 ?

L'hon. Karina Gould : Je crois que, après les prochaines élections, il sera nécessaire d'analyser ce qui se sera passé. Le rapport du CST, que j'ai mentionné, devrait être renouvelé après les prochaines élections. Une analyse sera faite de ce qui s'est passé. Je crois que ce serait vraiment approprié et important que le Parlement voie cela. En outre, j'imagine que le directeur général des élections va faire son rapport après les prochaines élections et, comme il le fait après chaque élection générale, il va formuler ses suggestions sur les façons d'améliorer la législation électorale dans ce pays.

Merci.

[Traduction]

Le président : Merci.

Nous passons maintenant à Mme Fortier, pour cinq minutes.

[Français]

Mme Mona Fortier (Ottawa—Vanier, Lib.) : Merci beaucoup.

[Traduction]

Madame la ministre, je vous remercie de votre présence aujourd'hui et de l'information que vous nous avez donnée. Je risquede me répéter, mais je sais que vous avez probablement plus de choses à dire en réponse à ma question.

[Français]

Nous prenons très au sérieux le travail entrepris pour protéger nos élections contre les menaces et l'ingérence extérieures. Comme vous le savez, nous avons étudié les violations commises notamment par la société Cambridge Analytica et Facebook. Depuis plusieurs mois, les membres de ce comité étudient la situation en profondeur en collaboration avec des comités parlementaires du monde entier; il s'agit d'une étape importante. Notre comité s'est employé à le faire de manière non partisane, sachant que les répercussions sur notre système électoral préoccupent grandement les Canadiens et les

[Traduction]

Dans quelle mesure les Canadiens peuvent-ils avoir la certitude que la lutte contre l'ingérence étrangère est prioritaire pour notre gouvernement que cette ingérence soit le fait d'organismes quasi gouvernementaux ou de particuliers travaillant seuls?

L'hon. Karina Gould: Ils devraient être tout à fait assurés que c'est une absolue priorité. J'ai adopté pour ce dossier une approche pangouvernementale. Mon annonce du 30 janvier réunissait les ministres de la Défense, de la Sécurité publique, de Patrimoine canadien, d'ISDE et de la Justice. Un groupe de travail composé de sous-ministres et adjoints se penche sur plusieurs aspects de cela. Le sujet qui est discuté aujourd'hui est pour lequel j'ai été invitée est le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections. Ce groupe réunit le SCRS, le CST, la GRC et Affaires mondiales Canada, ce qui permet de vraiment garantir que l'ensemble du gouvernement prend cette question au sérieux, car il n'y a rien de plus important que la merveilleuse démocratie que nous avons ici au Canada.

• (1635)

[Français]

Mme Mona Fortier: Le Comité aimerait mieux comprendre comment dans l'éventualité où serait détectée une ingérence lors des élections, les fonctionnaires pourraient alerter les Canadiens sur les conséquences d'une telle ingérence. Pouvez-vous expliquer aux Canadiens et aux Canadiennes comment ce processus fonctionnerait?

L'hon. Karina Gould: Bien sûr.

Comme je l'ai mentionné, il y a le Protocole public en cas d'incident électoral majeur. Je crois que nous avons transmis au Comité les documents infographiques qui sont disponibles sur notre site Web. Selon ce processus, les agences de sécurité nationale qui prendraient connaissance d'un incident informeraient le groupe formé de cinq hauts fonctionnaires suivants: le sous-ministre de la Justice et sous-procureur général du Canada, le sous-ministre d'Affaires mondiales Canada, le sous-ministre de la Sécurité publique, le conseiller à la sécurité nationale et au renseignement et le greffier du Conseil privé. Ces hauts fonctionnaires auront à décider ensemble s'il vaut la peine d'informer les Canadiens de l'incident. Le seuil d'intervention de ce groupe sera très élevé, c'est-à-dire dès que l'incident compromet la possibilité d'avoir des élections justes et libres. Si les Canadiens reçoivent un message de ce groupe, c'est qu'une ingérence étrangère réelle a une incidence sur les élections.

Mme Mona Fortier: J'ai une dernière question à vous poser. Croyez-vous qu'on devrait infliger des sanctions à ceux et à celles qui auront fait de l'ingérence dans le système électoral?

L'hon. Karina Gould: Ce sera à la ministre des Affaires étrangères d'en décider. Bien sûr, la Loi électorale du Canada prévoit déjà que l'ingérence étrangère dans les élections est illégale. La collusion entre un acteur canadien et un acteur étranger est aussi illégale. Ce sera au commissaire aux élections fédérales et à la GRC d'intervenir dans ce cas.

Mme Mona Fortier: D'accord, merci beaucoup.

[Traduction]

Le président Monsieur Angus, vous avez trois minutes.

M. Charlie Angus: Il y a exactement un an, le premier ministre a fait une mise en garde ferme à Facebook. Il a dit à la société de se prendre en main, sinon elle serait réglementée. Ensuite, rien n'est arrivé. Notre comité a commencé son étude, ce qui nous a permis de découvrir les agissements d'acteurs fort sombres. J'ai l'impression de rêver lorsqu'on entend parler d'acteurs d'agents et de pays étrangers qui, il semble, téléphonent aux citoyens sans cesse le jour des élections, alors que ce que nous avons découvert, c'est qu'il pourrait s'agir de deux gars dans un bureau au-dessus d'un cabinet d'optométrie avec des ensembles de données solides et la capacité de changer des votes, une centaine, une cinquantaine par là-bas, ce qui pourrait en fait faire dérailler le système démocratique.

Lorsque nous avons rencontré des représentants de 17 pays, ils ont tous exprimé leur frustration quant à l'absence de volonté de la part de Facebook d'assumer une responsabilité quelconque. Notre comité homologué du Royaume-Uni a même traité la société de « gangster numérique ».

Hier, le Toronto Star a publié un éditorial qui indiquait qu'Ottawa devrait confronter les géants du numérique sur la question de la protection de la vie privée et la démocratie. Je cite: « Et pourtant, notre gouvernement semble incertain, voire même paralysé face aux nombreux défis créés par les géants de la technologie... Les États-Unis... et l'Europe... prennent des mesures musclées pour contrer certains des pires effets de Facebook... alors qu'Ottawa semble... heureux de ne rien faire. » Ce n'est pas moi qui le dis; j'ai cité un article paru hier dans le Toronto Star, inspiré sans doute par votre rapport.

J'ai deux questions rapides. La première: quelles assurances avez-vous obtenues de Facebook qu'aucun autre pays ne semble avoir obtenues? La deuxième qui a déjà été posée, c'est de vous demander les noms des représentants de Facebook avec qui vous avez parlé afin que nous puissions les convoquer ici pour savoir quelles assurances seront offertes au peuple canadien.

• (1640)

L'hon. Karina Gould: Monsieur Angus, comme je vous l'ai déjà dit, je me ferais un plaisir de vous donner les noms de ces gens. J'en m'en souviens pas actuellement, mais je vous les ferai suivre.

M. Charlie Angus: D'accord. C'est parfait.

L'hon. Karina Gould: Pour ce qui est de réglementer les médias sociaux, j'aimerais vous préciser qu'ils seront encadrés par le projet de loi C-76, qui prévoit un registre obligatoire des messages de publicité en ligne pour les prochaines élections. J crois que c'est une mesure très importante et c'est la première à être adoptée au monde.

Pour ce qui est des assurances fournies par Facebook je ne suis pas entièrement convaincu que la société fera tout ce qui s'impose ni qu'elle comprend l'ampleur du problème, et c'est la raison pour laquelle je continue de m'entretenir avec ses représentants et que j'ai souligné...

M. Charlie Angus: Pourquoi vous entretenez-vous avec eux sur notre système démocratique ? Voilà mon inquiétude. Si vous n'êtes pas entièrement convaincu, moi non plus, et c'est vous qui les rencontrez.

Pourquoi ménageons-nous une société alors qu'elle se moque allégrement si elle perturbe des élections partout au monde ? Pourquoi ne parlons-nous pas de conséquences sérieuses comme celles qu'adoptera l'Allemagne et celles dont parle l'Europe ? Ne croyez-vous pas que notre système électoral est toujours compromis par la capacité d'acteurs tiers ici au pays de profiter de la plateforme de Facebook puisque Facebook ne respectera tout simplement pas ses obligations ?

L'hon. Karina Gould: Je crois qu'il faut tenir compte de la rigueur de notre loi électorale et du projet de loi C-76. C'est la raison pour laquelle nous avons inclus la disposition sur l'utilisation non autorisée d'un ordinateur et les interdictions connexes. Nous avons un système électoral bien établi et une loi solide ici au Canada. Nous avons également renforcé les règles qui régissent les activités des tiers et des parties touchant à la publicité et à la divulgation de leurs opérations financières, ce qui est très important, à mon avis.

J'ai confiance en notre loi électorale nationale.

M. Charlie Angus: Mais ce n'est pas Facebook.

L'hon. Karina Gould: Il m'en faut encore plus de la part des sociétés de médias sociaux. C'est la raison pour laquelle j'entretiens des discussions avec elles et je leur transmets nos exigences et je serai entièrement transparent avec les Canadiens quant au déroulement de ces discussions. Je me ferai un plaisir d'en parler plus tard avec vous à ce sujet, car il est d'une importance cruciale.

M. Charlie Angus: Merci.

Le président: J'ai quelques observations à faire à la ministre avant que nous ne terminions. La phrase qui m'est venue avant, lorsque j'ai vu le projet de loi C-76, c'est que nous sommes comme David avec une fronde face à Goliath. En fait, nous n'avons même pas de fronde; nous avons un pistolet à eau.

Je suis préoccupé du fait que malgré les recommandations ne peut plus claires contenues dans notre rapport, soit 26 recommandations précises, la ministre n'en a retenu que très peu. Le Comité se pose la question à savoir si votre tactique consistait à vous attendre à ce que les médias sociaux donnent suite à vos recommandations et devraient-ils pas vous prendre au sérieux ?

Je vais citer la commissaire de la protection de l'information du Royaume-Uni dont les propos ont été repris par notre commissaire à la protection de la vie privée. « Le temps de l'autoréglementation est terminé », a déclaré Mme Denham. « Il est trop tard. » Madame la ministre, je me demande pourquoi nous laissons toujours ces sociétés s'autoréglementer et nous nous attendons à ce qu'elles agissent correctement lorsqu'elles ne l'ont pas fait jusqu'à maintenant.

Le Comité ainsi que moi-même sommes inquiets du fait, comme cela a été dit avant, que nous soyons dans une guerre froide, mais dans un contexte numérique et que nous agissions comme si c'était un problème de la guerre froide.

À la lumière de tout cela, pensez-vous en avoir fait assez ?

L'hon. Karina Gould: Vous verrez de nombreux éléments pas tous mais quand même beaucoup, de vos deux rapports sur les élections dans le projet de loi C-76 et l'annonce qui a été faite concernant la protection de la démocratie.

Quant aux autres éléments qui ne relèvent pas de mon mandat, sachez que mon collègue, le ministre Bains, mène des consultations publiques et publiera un rapport qui portera précisément sur la protection de la vie privée et les données et la façon dont les sociétés s'enservent. Si j'ai bien compris, cela se fera prochainement.

Comme je l'ai dit à maintes reprises, nous avons un grand défi à relever. Pendant longtemps, à bien des égards, nous n'avons retenu que les avantages énormes des médias sociaux et du monde numérique. Je crois que les gens partout au monde sont aperçus en 2016 de ce qui se passait.

Comme à bien des moments dans l'histoire, nous devons trouver la façon d'aborder un problème. Nous voulons continuer à encourager les aspects positifs des médias sociaux, comme la capacité de communiquer d'une façon qui était impossible auparavant et les aspects positifs pour la démocratie puisqu'ils permettent d'échanger des opinions et des points de vue, ce qui est extraordinairement positif à mon avis. Nous voulons également atténuer les risques et les méfaits sociaux que nous constatons.

Au cours des deux dernières années et surtout l'année dernière, lorsque de plus en plus de problèmes ont été révélés, j'ai réfléchi au fait qu'il y a eu très peu de fois où une seule industrie a exercé tellement d'influence dans tant d'aspects de nos vies et il est difficile de s'y attaquer à partir d'un seul point de vue, qu'il s'agisse de la démocratie, de la protection de la vie privée, de la sécurité publique, du maintien de l'ordre ou quel que soit l'enjeu. Nous devons commencer à réfléchir de façon plus globale à la façon d'aborder ces géants du numérique.

C'est la raison pour laquelle je pense que le travail de votre comité nous a beaucoup aidés à réfléchir à ces problèmes et à la façon de les gérer d'une façon qui sera conforme à nos valeurs et normes sociales dans l'avenir.

• (1645)

Le président: Merci, madame la ministre.

Nous prendrons une pause de quelques minutes pour vous laisser partir, madame, et nous entendons ensuite les autres témoins pendant la dernière heure de notre réunion.

L'hon. Karina Gould: Merci de m'avoir reçue.

Le président: Prenons une pause.

• (1645)

_____ (Pause) _____

• (1645)

Le président: La réunion reprend.

Tout d'abord, M. Angus souhaite faire un rappel au Règlement.

M. Charlie Angus: Monsieur le président, je voulais tout simplement exprimer ma préoccupation. Après notre réunion tenue la semaine dernière, des représentants de Waterfront Toronto nous ont envoyé des lettres. La première était une lettre de Jim Balsillie, dans laquelle il indique que le secrétaire parlementaire a menti sur ce qui avait été dit et a déformé les faits, et qu'il voulait corriger cela.

Nous avons également reçu une lettre, je ne sais pas si nous l'avons ici, de Julie Di Lorenzo, qui affirme que de fausses déclarations ont été faites.

Je suis inquiet. Nous avons effectué notre travail d'une certaine façon. Je crains que les choses ne s'enveniment entre M. Vaughan et M. Balsillie, mais je pense que ce dernier a le droit de comparaître. Je pense également que Mme Di Lorenzo, si elle dit que de fausses déclarations ont été faites pendant l'audience, devrait aussi avoir la possibilité de prendre la parole.

Nous devons trouver un cadre qui leur permettrait de s'exprimer, et ensuite nous pourrions aller de l'avant.

• (1650)

Le président: D'accord, je vais en parler.

La présidence a bien reçu la lettre et je crois que nous attendons tout simplement la traduction. Mike a dit qu'elle devrait être prête d'ici demain après-midi.

De plus, nous avons invité M. Balsillie à revenir témoigner devant le Comité. Il ne peut venir jeudi, et nous cherchons une date propice. Selon les conversations que j'ai eues avec les vice-présidents, je puis affirmer que cela a déjà été fait.

Le Comité attend juste la lettre qui devrait nous parvenir demain.

M. Charlie Angus: Il y a également Mme Di Lorenzo, qui, je crois, a siégé au comité immobilier ou avait un lien quelconque avec Waterfront Toronto. Elle a dit qu'elle travaillait avec son avocat pour rédiger une lettre et j'aimerais que le Comité communique avec elle pour savoir si nous recevons une lettre officielle ou si elle fera une déclaration.

Je veux être fixé sur ce qui s'est passé avec les témoignages.

Le président: Oui, la présidence peut s'en occuper. Je vais m'assurer que les analystes ont cette demande.

M. Maxime-Olivier Thibodeau (attaché de recherche auprès du comité): Bien sûr.

Le président: Parfait.

Il n'y a aucune déclaration de prévu de la part de témoins, alors nous allons passer directement aux questions.

Les premières sept minutes reviennent à M. Erskine-Smith.

M. Nathaniel Erskine-Smith: Merci aux gens qui comparaissent pour la première fois aujourd'hui, ainsi qu'à ceux qui reviennent.

Pour commencer, je vais m'adresser au CST au sujet d'une évaluation de la menace antérieure. Est-ce que des choses ont évolué depuis que nous devrions savoir?

M. André Boucher (sous-ministre adjoint, Opérations Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications): La publication de la mise à jour de l'évaluation de la menace est imminente. Mon équipe prend le temps nécessaire pour élaborer des conseils et des directives ciblés en fonction de la teneur du rapport. Je ne veux pas vendre la mèche aujourd'hui, mais je vous assure que nous n'attendons pas la publication du rapport pour prendre des mesures à l'égard de facteurs dont nous sommes déjà au courant.

Lorsque j'ai parlé de la publication imminente, il est question de quelques jours ou semaines au maximum.

M. Nathaniel Erskine-Smith: La ministre a dit qu'elle rencontrait les représentants des médias sociaux. En ce qui concerne la sécurité, dans quelle mesure travaillez-vous directement avec les sociétés de médias sociaux pour vous assurer que leurs plateformes ne se font pas pirater?

M. André Boucher: Du point de vue du centre de la cybersécurité, il y a beaucoup de sociétés qui sont présentes dans l'écosystème. Moi je suis préoccupé par les appareils dont nous nous servons tous, les logiciels qui sont installés et la façon dont nous utilisons les appareils sur les réseaux sociaux.

À mon avis, les médias sociaux sont un facteur dans un écosystème complexe et nous leur accordons un traitement égal. Nous nous entretenons avec les sociétés et nous avons les mêmes attentes quant à leurs pratiques en matière de cybersécurité ainsi que leur comportement et leurs réactions dans l'écosystème. Cela ressemble au traitement accordé aux autres sociétés, que ce soit celles qui fabriquent les appareils ou les systèmes d'exploitation ou encore les applications qui sont installées.

M. Nathaniel Erskine-Smith: Êtes-vous d'accord avec le Comité pour ce qui est de nos inquiétudes quant au contenu haineux, incendiaire ou encore qui incite à la violence et qui reste sur ces plateformes et n'est pas retiré rapidement?

M. André Boucher: Le centre de la cybersécurité n'a pas comme fonction d'analyser ou de faire des commentaires sur l'information véhiculée par les ordinateurs, les courriels ou le contenu des médias sociaux, mais nous nous attendons à ce que toutes les sociétés se comportent comme de bons citoyens canadiens et veillent à leur présence et leurs responsabilités au Canada.

Si nous pouvions nous écarter de la question des médias sociaux pendant une seconde, j'aimerais dire que si une société de logiciels ne se comporte pas en bonne citoyenne, nous aurons les mêmes inquiétudes.

M. Nathaniel Erskine-Smith: Oui. Je trouve toujours drôle que Facebook s'appuie sur la liberté d'expression. J'en suis un grand défenseur et je ne pense pas que les gens devraient nécessairement être incarcérés pour avoir dit des choses absurdes. Toutefois, l'idée selon laquelle ils peuvent les dire sur la plateforme de Facebook sans qu'elles soient retirées nous incite à nous demander quelle sorte de communauté Facebook veut construire.

En ce qui concerne le piratage des algorithmes, et prenons l'exemple de l'Internet Research Agency, on parle seulement d'un certain nombre de robots, mais aussi de gens qui gèrent un certain nombre de comptes pour renforcer un message. Souvent, il s'agit de désinformation. Votre organisme se penche-t-il là-dessus?

• (1655)

M. André Boucher: Nous commençons certainement une discussion en disant « je m'attends à ce que tous les produits de mon écosystème soient de la meilleure qualité possible », de sorte que si nous constatons que quelque chose cloche dans le logiciel ou le matériel, ou qu'une personne nous le signalait, est-ce que nous essayerions d'aller au fond des choses? Absolument, et nous ferions assurément quelque chose à propos de l'entreprise, mais il y a aussi une possibilité dans le volet étranger et je vais laisser Dan en parler.

M. Dan Rogers (chef adjoint, SIGINT, Centre de la sécurité des télécommunications): Sur le plan du renseignement étranger, nous nous intéressons aux acteurs étrangers qui sont à l'extérieur du Canada et à leurs possibles intentions à l'égard du Canada. Ce que nous pouvons faire, entre autres pour aider le centre de cybersécurité ou d'autres éléments du gouvernement du Canada à intervenir, c'est de voir ces acteurs étrangers. Si nous pouvons déterminer quels sont leurs comportements — si nous pouvons voir leur infrastructure en ligne ou les types de réseaux de zombies ou de techniques ils utilisent —, voilà un avantage que nous pouvons fournir au centre de cybersécurité et à d'autres personnes au gouvernement qui, dans le cadre de leur mandat, peuvent intervenir.

M. Nathaniel Erskine-Smith: Y a-t-il des mesures que peuvent prendre les plateformes et qu'elles ne prennent pas déjà pour contrer le problème de piratage de logiciels?

M. André Boucher: L'information me serait fournie par cette équipe. Nous n'avons jamais hésité à communiquer avec les entreprises canadiennes ou étrangères pour parler de la qualité et du comportement de leurs appareils ou de leurs logiciels. Nous ferions exactement la même chose dans ce cas.

M. Nathaniel Erskine-Smith: J'ai parlé du mouvement des gilets jaunes, et j'ai lu un commentaire haineux incitant à la violence. Évidemment on peut trouver beaucoup de commentaires de ce type en naviguant sur Internet si l'on peut supporter de regarder les commentaires dans les sections réservées à cette fin.

Dans son témoignage, Michael Wernick a dit qu'il était très préoccupé par les risques de violence aux prochaines élections. Est-ce que cela va au-delà de ce type de commentaires en ligne? Y a-t-il des évaluations de menaces réelles, crédibles, et devrions-nous craindre que des actes de violence soient commis au cours des prochaines élections?

M. Dan Rogers: Ce que je peux dire, sur le plan de la sécurité nationale et du renseignement étranger, c'est que bien qu'une bonne partie de ce dont nous avons parlé aujourd'hui est dans le cyberspace, bien entendu, nous surveillons des menaces de toutes sortes dont les Canadiens pourraient faire l'objet, qu'il s'agisse de terrorisme, de cyberattaque ou d'autres types d'activités étrangères pernicieuses qui pourraient être menées contre le Canada ou les Canadiens. Dans cet espace, il y a déjà des mécanismes. Ce n'est pas un nouveau défi pour nous. Si nous voyons ce type de choses nous allons les signaler. Le SCRS, la GRC et d'autres organismes ont le mandat d'enquêter sur les activités qui sont menées au Canada le cas échéant. La fonction de renseignement que nous et d'autres aurons leur fournira toute information, de sorte que si cela arrive, nous serons vigilants et nous nous assurerons qu'ils ont l'information.

M. Nathaniel Erskine-Smith: Monsieur Sutherland je ne sais pas si vous pouvez parler de l'observation de M. Wernick et peut-être nous donner un peu plus de détails. Se base-t-elle seulement sur les commentaires dans les médias sociaux et la mesure dans laquelle ils sont méchants ou y a-t-il une menace réelle à laquelle c'est lié?

M. Allen Sutherland (secrétaire adjoint au Cabinet, Appareil gouvernemental et Institutions démocratiques, Bureau du Conseil privé): Je crois que M. Wernick donnait son point de vue personnel. Il a commencé ses remarques de cette façon. Je dirais que la préoccupation qu'il a exprimée est largement partagée par les gens qui se penchent sur les questions d'inclusion sociale, non seulement au Canada mais partout dans le monde.

M. Nathaniel Erskine-Smith: Ma dernière question portait sur les initiatives d'éducation numérique. Nous savons qu'il y a un investissement de 7 millions de dollars. Je pose une question ouverte. Dans quelle mesure pouvons-nous sensibiliser les Canadiens à la désinformation sur Internet en peu de temps? D'après l'expérience du Centre de la sécurité des télécommunications, compte tenu du fait que des acteurs politiques comme nous sont les maillons faibles, en quelque sorte, pensez-vous qu'il vaudrait mieux utiliser les fonds pour veiller à ce que les bénévoles de nos équipes, nos associations, le comité et les gens qui participent aux campagnes dont nous-mêmes faisons tout ce que nous pouvons pour ne pas être victimes de piratage et ne pas être vulnérables?

M. André Boucher: Je vais en parler un peu. Concernant l'investissement de 7 millions de dollars qui a été annoncé, il s'agit de fonds supplémentaires destinés à des activités précises. Je crois que nous ne pouvons pas oublier que nous avons commencé... même avant la publication du premier rapport intitulé *Cybermenaces contre le processus démocratique du Canada*, nous avons collaboré avec tous les participants mentionnés dans le rapport. Cela fait des années que des activités visant à sensibiliser les gens sont menées et que l'on parle de prévention, et il s'agit d'un investissement important.

Le président: Merci.

C'est maintenant au tour de M. Kent, qui dispose de sept minutes.

• (1700)

L'hon. Peter Kent: Je remercie tous encore une fois chacun de comparaître à nouveau devant notre comité.

Messieurs Rogers et Boucher, je crois que votre dernière comparaison devant nous remonte au 18 octobre.

L'une des questions que je vous ai posées portait sur la façon dont vous géreriez une situation comme le coup Beyoncé au cours des dernières élections fédérales aux États-Unis. Une entité russe — ou un individu russe — a créé un faux site Web d'admirateurs de la vedette populaire Beyoncé et a attiré des millions d'abonnés simplement au moyen de potins, d'informations, de photos, etc. Ensuite, deux ou trois jours avant les élections, cette bombe à retardement a explosé avec toutes sortes de déclarations et d'instructions semblant provenir de Beyoncé. L'objectif, selon l'un de nos témoins précédents M. Ben Scott, était de dissuader les électeurs noirs américains de voter.

À l'époque, nous parlions de théories. Je ne veux pas que vous dévoiliez des processus et des tactiques, mais je veux parler de la capacité de la collectivité du renseignement et de ce nouveau comité de réagir, dans les jours, voire les heures qui précèdent des élections, à une situation comme le coup Beyoncé.

M. Dan Rogers: Je peux essayer de répondre à la question.

Je soulignerais deux ou trois éléments. Tout d'abord, il est beaucoup plus facile de réagir lorsque nous avons de bonnes informations à l'approche de la date. Nous continuons de collaborer avec le Groupe de travail sur les menaces en matière de sécurité et de renseignement, et le SCRS, la GRC, le CST et Affaires mondiales essayeront de déterminer si des acteurs étrangers essaient d'établir de faux comptes et de communiquer cette information.

L'hon. Peter Kent: Évidemment, les gens qui s'attaqueraient au système électoral actualiseraient leurs stratégies au fur et à mesure. Ils pourraient très facilement infiltrer un mauvais acteur au Canada à l'aide d'une adresse ou d'une identité Web légitime et pourraient faire le même type de choses au Canada.

Comment le découvririez-vous?

M. Dan Rogers: C'est une bonne question, et elle est en partie hypothétique. Ce que je peux dire notamment, c'est que si nous devons regarder du côté de l'étranger si nous pouvons découvrir les intentions, les plans ou toutes sortes de capacités pour ce qui est de créer ce type de comptes au Canada et voir le volet étranger, cela donnera un avantage au centre de cybersécurité et à d'autres éléments au Canada. Voilà ce que nous cherchons à faire, et nous améliorons notre collecte de renseignements. Comme vous pouvez le comprendre, je ne peux pas parler des détails ou des techniques et des outils que nous utiliserons, mais d'ici à l'élection de 2019, notre tâche consistera à améliorer nos capacités de découvrir de telles choses.

L'hon. Peter Kent: En ce qui concerne la publication *Évaluation des cybermenaces nationales 2018*, compte tenu de son contenu, en cette année électorale le Canada considère-t-il la Russie comme un adversaire?

M. André Boucher: Ce qui constitue la base de notre analyse, c'est une tendance à la hausse à l'échelle mondiale de menaces qui planent sur nos institutions démocratiques. Nous ne consacrons pas un temps démesuré à essayer de déterminer d'où viennent les comportements. Nous utilisons nos ressources pour les découvrir, trouver des solutions et passer à la prévention le plus vite possible. Je pense qu'il est important de comprendre que, comme notre rapport l'indique, ces menaces sont de plus en plus importantes et puisque le Canada est un acteur clé dans le monde, il est susceptible d'être ciblé par les mêmes menaces.

L'hon. Peter Kent: La ministre a répété que le gouvernement s'attend à ce que les entreprises de médias sociaux prennent des mesures concrètes pour que les élections de l'automne prochain soient protégées. Les membres de notre comité, peu importe leur allégeance, ne croient pas que les entreprises de médias sociaux le feront. Comme on l'a dit ici aujourd'hui, leur priorité, c'est de faire croître leurs activités et leur rentabilité, et non de protéger la vie privée. C'est ce qu'ont dit les commissaires à la protection de la vie privée du Canada de la Colombie-Britannique et du Royaume-Uni, et bon nombre d'autres personnes. La mauvaise foi dont certaines des entreprises de médias sociaux ont fait preuve dans le cadre de leur comparution devant notre comité nous pousse, je crois, à nous demander pourquoi la ministre doit attendre six mois alors que nous ne nous attendons pas vraiment à ce qu'elles fassent mieux.

Je vous donne un exemple. L'an dernier, lorsque M. Chan a comparu devant nous pour la première fois, j'ai posé une question. Au cours de la réunion, un téléspectateur abonné a envoyé un courriel et a posé une question au sujet de la fausse publication russe en Lettonie, où l'on a utilisé de vieilles photos d'un Canadien, un officier, portant un bikini. Le message dans le courriel, c'était qu'on prévenait les Lettons que des soldats canadiens à la tête du groupement tactique en Lettonie essaieraient d'encourager l'homosexualité. M. Chan a dit qu'il ne savait rien à ce sujet. Plus d'un mois plus tard, mon bureau a communiqué le nouveau avec lui et lui a dit que la publication dont nous avions parlé lorsqu'il avait témoigné devant le Comité était encore là. Bien que M. Chan — et certainement les employés de Facebook qui regardaient les nombreux moniteurs dont il parle —, évidemment, n'a rien fait jusqu'à ce que nous revenions à la charge un mois plus tard, elle a été

retirée trois jours plus tard. Encore une fois, est-ce que quiconque d'entre vous à cette table fait vraiment confiance aux médias sociaux, ce qui, je crois, n'est pas le cas des membres de notre comité, et croit qu'ils empêcheront le type de choses que nous craignons voir arriver durant le processus électoral de se produire?

● (1705)

M. Allen Sutherland: J'ai deux ou trois observations à faire à cet égard. Je crois que dans sa déclaration préliminaire, la ministre a dit très clairement qu'elle des attentes envers les entreprises de médias sociaux et que les discussions sont en cours. Ce qui me semble clair, c'est que votre comité a des attentes envers les sociétés de médias sociaux et qu'il est d'écouter ce qu'il a constaté jusqu'à maintenant et qu'il s'attend mieux de leur part. C'est un message que la ministre peut certainement transmettre dans ses prochaines discussions avec elles.

Le président: Merci.

Très rapidement.

L'hon. Peter Kent: La ministre a parlé des élections en Europe qui, comme celles au Canada, auront lieu cette année, mais elle n'a pas parlé des recommandations qu'a faites notre comité dans un certain nombre de rapports. Nous recommandons que le gouvernement canadien envisage de mettre en oeuvre certaines des mesures très concrètes que l'Union européenne a adoptées avec le Règlement général sur la protection des données en mai de l'an dernier, qui va bien plus loin. Le Canada est loin d'avoir le type de mesures de protection de la vie privée dont disposent les Européens présentement.

M. Allen Sutherland: Je peux vous assurer que la ministre est au fait de ce qui se passe dans l'Union européenne.

Le président: Merci.

C'est maintenant au tour de M. Angus, qui dispose de sept minutes.

M. Charlie Angus: Merci beaucoup monsieur le président.

Nous avons parlé en quelques sortes des acteurs étrangers, mais nous nous concentrons beaucoup sur la menace nationale et la facilité avec laquelle il est possible de manipuler la plateforme. Du point de vue du renseignement, observez-vous une augmentation de l'utilisation du langage extrémiste, une montée des groupes extrémistes et des comportements extrémistes dans le débat politique au Canada?

M. Dan Rogers: Du point de vue du Centre de la sécurité des télécommunications, je peux dire que comme le prescrit la loi, nous avons le mandat de nous pencher exclusivement sur les acteurs étrangers qui se trouvent à l'extérieur du Canada. C'est exclusivement ce sur quoi porte notre mandat en matière de renseignement étranger à moins que nous travaillions à la demande du SCRS dans le cadre de notre mandat de soutien. Je peux dire que les menaces que nous verrons seront publiées dans le contexte électoral dans le rapport dont André a parlé plus tôt.

M. Charlie Angus: Je suppose que c'est ce qui m'inquiète. Vous examinez les menaces étrangères. Or, il y a au pays Les Fils d'Odin et des gens qui ne sont pas capables de se trouver quelque part avec qui sortir, qui haïssent les femmes et qui se décrivent comme des célibataires involontaires. Nous avons au pays des nationalistes blancs. Il y a toutes sortes de gens. Il y en a qui croient à des complots de lézards géants ou qui croient que la Terre est plate. Ce ne sont pas des menaces étrangères mais ils dominent le discours au pays.

Nous nous sommes concentrés sur la capacité de renverser ce type de conversations au pays. Si cela ne provient pas d'une source étrangère, comment allons-nous savoir si la menace nationale est comprise, calculable et que nous pouvons, en fait, élaborer une solution crédible sans porter atteinte aux droits qu'ont les gens de dire ce qu'ils veulent au sujet des politiciens?

M. Dan Rogers: Je peux répondre à cette question également.

Jedois dire que le Groupe de travail sur les menaces en matière de sécurité et de renseignements lors des élections dont a parlé le ministre réunit le CST, le SCRS, la GRC et Affaires mondiales Canada et, bien entendu, le SCRS et la GRC auront le mandat national d'enquêter sur des menaces dans les limites de leur mandat. Cela continuera d'ici à 2019, et toute activité constituant des menaces sera examinée.

M. Charlie Angus: J'ai défendu publiquement notre premier ministre actuel contre certaines attaques vraiment abominables, car je crois qu'il nous faut avoir une norme dans les conversations et lorsque le premier ministre fait quelque chose que nous n'approuvons pas, on ne devrait pas dire qu'il devrait être pendu. Ce n'est pas un traître. Il a été élu démocratiquement et c'est notre premier ministre. Je crois que nous devons appliquer cette norme partout.

J'ai été très choqué lorsque le greffier du Conseil privé, Michael Wernick, a laissé entendre qu'un assassinat politique pourrait être commis. Du point de vue des activités de renseignement, s'agit-il pas de quelque chose qu'on ne dit pas publiquement?

• (1710)

M. Dan Rogers: Je ne peux pas me prononcer sur les opinions générales du greffier, mais ce que je peux vous dire, c'est qu'en ce qui concerne la sécurité nationale nous examinons les menaces de ce genre.

J'ajouterais aussi, à titre de précision, que nous n'avons certainement pas la responsabilité de décider ce qui est vrai et ce qui est faux, ou quel type de discours les Canadiens considéreraient comme approprié. Nous nous concentrons sur les aspects de la question relatifs au renseignement étranger et à la sécurité nationale.

M. Charlie Angus: Je vous lis un autre extrait des directives du Conseil privé à l'intention des fonctionnaires qui présentent des témoignages: « Les fonctionnaires doivent comprendre et respecter l'obligation qu'ils ont [...] de s'abstenir de divulguer des renseignements scotés ou de transmettre des documents confidentiels à toute personne qui n'est pas autorisée à en prendre connaissance. Je trouve inquiétant que quelqu'un ait mis la possibilité d'un assassinat politique. À mes yeux, cela ouvre une porte qui devrait rester close. Je vous suggérerais de revenir là-dessus, sur le plan du renseignement, car je pense qu'il faut faire très attention à ce qui est dit.

Ce qui me frustre, c'est que nous avons vu que des tierces parties — pas des menaces étrangères mais bien des tierces parties à l'intérieur même du Canada — peuvent bouleverser les élections au moyen de très bons ensembles de données. Nous avons parlé des contrefaçons profondes basées sur de fausses informations. Il faudra des mesures très souples pour répondre à ces malfaiteurs, mais l'approche que vous adoptez ne semble très militaire. Pourtant nous avons affaire à des gangsters numériques.

Pouvez-vous nous assurer que les préoccupations que nous avons soulevées en nous fondant sur le travail de notre comité, ont été entendues et qu'il sera possible d'intervenir lestemment rapidement pour empêcher que les élections soient bouleversées?

M. Allen Sutherland: Je pourrais peut-être répondre en parlant du Protocole public en cas d'incident électoral majeur. Il est plus

probable que la menace qui dépasserait le seuil et ferait en sorte que les Canadiens soient informés de quelque chose vienne d'une source étrangère. Je pense que c'est vrai aussi du point de vue du renseignement. C'est la tendance.

En France, aux États-Unis et au Royaume-Uni, l'ingérence est venue d'acteurs étrangers, mais le protocole ne se limite pas à l'ingérence étrangère. Le facteur clé, c'est que l'incident pose une menace à la tenue d'une élection libre et juste. Si, comme vous le dites, il se passe quelque chose à l'intérieur du pays d'une envergure telle que la tenue d'une élection libre et juste est menacée, le protocole sera suivi.

M. Charlie Angus: Je suis un peu surpris que vous pensiez que la menace est étrangère alors que nous avons vu à maintes reprises, dans les 17 pays que nous avons étudiés... Facebook a reçu de nombreux avertissements concernant la menace intérieure de génocide au Myanmar et les propos extrémistes attaquant les musulmans Rohingyas.

Facebook n'a rien fait. Elle a ignoré la situation. Elle a été condamnée à l'échelle internationale. Malgré tout, elle n'a toujours pas pris de réelles mesures.

Au Sri Lanka, c'était la même chose. Nous avons aussi reçu des avertissements de la part des représentants du Brésil durant la séance du comité international. Au Nigeria, ce sont des acteurs nigériens et non des acteurs étrangers qui ont utilisé ces plateformes pour propager la haine. Dans chaque de ces cas, Facebook n'a rien fait.

Pour les élections de 2019, nous nous préparons à mener une guerre froide alors qu'en réalité, ce que nous devons savoir, c'est comment lutter contre les tierces parties qui cherchent à influencer sur les élections — 100 votes par-ci, condamner des gens par-là, s'en prendre aux immigrants, et ce, en manipulant très efficacement des algorithmes de Facebook. C'est par rapport à cela que nous devons être rassurés et je n'entends rien à ce sujet.

M. Allen Sutherland: Je comprends et ma réponse était peut-être pas très claire. La source n'importe pas. S'il arrive quelque chose qui pose une menace à la tenue d'une élection libre et juste, le protocole sera suivi.

M. Charlie Angus: Il faudrait que vous exerciez une surveillance très étroite. Ce que j'essaie de dire et ce que nous avons vu, c'est que l'ingérence se fait au moyen d'un vote par-ci, d'une annonce par-là, puis d'un message négatif par-ci et d'un commentaire sur un site par-là; or, une tendance commence à émerger et tout est fait par un petit nombre d'intervenants. Il faudrait que vous ayez une bonne compréhension du mode de fonctionnement de ces intervenants.

• (1715)

M. Allen Sutherland: Je tiens à vous rassurer il peut s'agir d'un incident unique, de l'aboutissement de nombreux incidents ou encore d'une accumulation d'incidents. Je pense que cela répond à votre préoccupation.

M. Charlie Angus: Merci.

Le président: Le prochain intervenant est M. Picard. Vous avez sept minutes.

[Français]

M. Michel Picard (Montarville, Lib.): Merci, monsieur le président.

L'un des aspects dont on n'a pas encore discuté, c'est l'après-attaque. Je m'explique.

Disons que, un jour, nous sommes envahis par une quantité industrielle de messages haineux, que nous réagissons de façon efficace et que, le lendemain, nous défaisons ces messages haineux en apportant une correction ou en affichant une publicité positive, peu importe la stratégie. Il reste que le dommage est fait. Nous sommes dans un environnement de liberté d'expression où certaines choses sont un peu moins tangibles. Bref, le dommage est social, d'une certaine façon.

Il existe un problème en ce qui concerne des attaques de systèmes par des pirates informatiques au cours desquelles il est possible de s'attaquer aux algorithmes, aux codes et aux systèmes de gestion. Même si l'attaque a eu lieu et que, selon le meilleur scénario possible, vous l'avez détecté et vous y avez réagi au cours de la journée même, il reste que les données du système sont dès lors compromises. La nature compromise des données est-elle réparable?

Dans le cas contraire, si on constate que, à la suite d'une attaque des données ou des algorithmes, notre système est compromis, cela enlève toute légitimité à l'élection en cours. Cela entraînerait une perte de légitimité du processus électoral, dans la situation actuelle de celui de l'élection prochaine, au mois d'octobre.

La nature compromise des données et des systèmes à la suite d'une attaque est-elle maintenue ou est-elle capable de garantir que, après la prise de mesures pour corriger le tir, on peut à nouveau faire confiance aux données ou aux systèmes? Autrement, il serait impossible de reconnaître l'élection de façon légale et légitime.

M. André Boucher: Je vais donner quelques éléments de réponse.

Dans le cas précis où un individu remarque que son compte a été piraté par quelqu'un et que de la mauvaise information a été diffusée, il peut aller sur notre site Web, où nous indiquons quoi faire en cas de piratage. L'une des premières choses est de reprendre le contrôle et d'enlever l'information. Selon le type d'attaque, on a la possibilité d'enlever cette information.

La rapidité d'intervention est importante parce qu'il y a un effet de vague dans la propagation de l'information. Je pense que c'était ce sur quoi portait votre commentaire. Je ne pense pas qu'on puisse arrêter cette vague à l'aide des outils présents.

[Traduction]

M. Michel Picard: Je comprends.

[Français]

C'est une attaque à la réputation. Si quelqu'un pirate mon compte personnel et y écrit des choses non fondées, il s'agit d'une question de réputation, mais ce sont des mots.

Si quelqu'un entre dans le système de gestion des données de l'élection pour faire une attaque, ce n'est plus la réputation qui est en jeu. C'est un vrai piratage du système. On touche les données, le programme, l'algorithme ou la ligne de code. En compromettant la ligne de code, cela met en doute la légitimité de l'élection. Même si nous réussissons à bloquer le signal, nos données qui sont à la base de la gestion de notre système électoral viennent d'être compromises.

La nature compromise des données est-elle ce point important que l'on pourrait déclarer nulle l'élection?

M. André Boucher: La première réponse que j'ai donnée était dans le contexte de piratage de médias sociaux.

Votre deuxième question, si je comprends bien, est au sujet du piratage des systèmes électoraux, n'est-ce pas?

M. Michel Picard: Oui.

M. André Boucher: Il est important de nous rassurer. Cela fait déjà plusieurs années que nous travaillons avec Élections Canada afin de mettre en place les mesures de protection nécessaires pour éviter ce genre d'événements. Si quelqu'un est en train de pénétrer dans nos systèmes, il faut détecter cette activité le plus tôt possible pour stopper le piratage. Dans le cas peu probable mais possible d'une pénétration, il faut être capable de retourner en arrière, c'est-à-dire de repérer l'activité, de fermer la porte, de remettre des copies de sauvegarde et de rétablir l'intégrité de l'information.

Je crois qu'il faut saluer le travail qui a été fait, de même que le partenariat et la collaboration. J'ai une confiance très élevée dans nos systèmes en ce qui concerne des élections qui s'en viennent.

• (1720)

M. Michel Picard: On peut donc qualifier la donnée corrigée comme étant intègre.

M. André Boucher: Absolument.

M. Michel Picard: Je m'adresse maintenant à M. Rogers.

Ceci est un peu hors de mon expertise. Est-ce qu'un signal étranger peut être converti en un signal local pour passer inaperçu, sous le radar? J'imagine que les signaux étrangers s'arrivent pas avec un accent au Canada.

M. Dan Rogers: Merci de la question.

Je veux être clair, alors je vais répondre en anglais, si vous me le permettez.

[Traduction]

Si je comprends bien, vous voulez savoir si un acteur étranger peut entrer au Canada et se faire passer pour un Canadien. La technologie...

M. Michel Picard: [Inaudible] ... signal. SIGINT.

M. Dan Rogers: Oui.

La réponse est oui, la technologie permet aux acteurs étrangers de se faire passer pour des Canadiens ou autres. Notre rôle est d'examiner l'acteur étranger et de tenter de déterminer si c'est ce qu'il essaie de faire. Ainsi, nous pouvons envoyer l'information, par exemple au Centre pour la cybersécurité qui peut alors prendre des mesures défensives ou transmettre d'information à d'autres victimes potentielles.

M. Michel Picard: Votre responsabilité est d'examiner ces signaux étrangers. Êtes-vous en mesure non seulement d'arrêter un signal, mais aussi de contre-attaquer afin d'en détruire la source?

M. Dan Rogers: Selon le mandat actuel du CST, nos pouvoirs se limitent à la collecte de renseignements. Le projet de loi C-59 contient certaines dispositions. Le Sénat l'étudie actuellement. S'il est adopté, nous aurons peut-être plus de pouvoirs à l'avenir.

M. Michel Picard: C'est ce que nous attendons.

M. Dan Rogers: Oui.

M. Michel Picard: Merci.

Le président: Il nous reste environ neuf minutes. Les prochains intervenants auront donc environ trois minutes chacun.

Nous commencerons par Mme Kusie, qui aura droit à trois minutes. Nous passerons ensuite à M. Erskine-Smith, pour trois minutes. Ensuite, la séance sera presqu'terminée.

Madame Kusie.

Mme Stephanie Kusie: Étant donné les préoccupations que vous avez entendues de ce côté-ci de la table aujourd'hui concernant l'impartialité ou l'indépendance des cinq personnes formant le groupe qui prendra la décision de déclencher le protocole en cas d'incident majeur, je demanderai à M. Boucher et à M. Sutherland de nous garantir qu'ils feront tout ce qu'ils pourront, en leur qualité de fonctionnaires pour soutenir la communication et être à l'égal de l'information à l'ensemble des partis politiques.

M. Allen Sutherland: Je tiens à être précis. Dans le cas où un incident dépasse le seuil, il est obligatoire d'en informer le premier ministre, les chefs des partis de l'opposition et Élections Canada. Je peux vous assurer que c'est ce qui se produira. Toutes les parties concernées recevront les mêmes renseignements. On aura décidé que le seuil a été franchi. Ce n'est pas le premier ministre, le chef de l'opposition et Élections Canada qui décident. La décision aura été prise, et ils recevront tous les mêmes renseignements le vous le garantis.

Mme Stephanie Kusie: Merci, monsieur Sutherland.

[Français]

Monsieur Boucher, voulez-vous ajouter un commentaire?

[Traduction]

M. André Boucher: Oui, absolument.

Il est probable que la majorité des incidents ne dépasseront pas le seuil. Le Centre pour la cybersécurité a toujours informé les personnes touchées ou potentiellement touchées lorsqu'il détecte des incidents ou des événements importants, et il continuera à le faire. Contrairement aux échanges concernant le seuil, nos échanges ne contiennent jamais de noms. Ils concernent la présence d'un problème, et ils visent à fournir des outils aux personnes touchées ou potentiellement touchées afin qu'elles puissent se défendre ou résoudre le problème.

Nous ne déclarerions pas : « Tel groupe a tel problème. » Nous dirions simplement qu'un groupe impliqué dans le processus connaît un problème et nous fournirions des conseils et des indicateurs aux autres groupes pour les aider à déterminer s'ils ont le même problème. Nous les aiderions aussi à le régler. C'est ce qui arriverait dans toute situation en deçà du seuil.

Mme Stephanie Kusie: Monsieur Rogers, vous en avez peut-être assez de m'en entendre parler, mais je suis membre de la Commission trilatérale. En novembre, nous avons eu la chance de nous rendre à la Silicon Valley pour obtenir une vue d'ensemble de l'état actuel de la cybersécurité avec certains des plus grands esprits au monde. J'avais l'impression qu'au lieu d'être chez Facebook et Google, nous aurions dû nous trouver dans le bureau principal de Fortnite.

J'aimerais que vous nous parliez, très brièvement, de la façon dont vous trouvez, vous engagez et vous employez les personnes les plus hautement qualifiées pour sécuriser notre système électoral.

M. Dan Rogers: C'est une très bonne question, merci.

Nous recrutons actuellement, alors nous invitons quiconque nous écoute à nous envoyer leur CV.

• (1725)

M. Charlie Angus: J'avertis mes collègues il n'y a rien de mieux que l'éthique. Je vous poursuivrai.

Desvoix: Ha, ha!

M. Dan Rogers: C'est une excellente question, car c'est difficile de trouver les personnes les plus qualifiées et les plus brillantes pour les intégrer à notre équipe. C'est un travail que nous accomplissons

avec grand soin. Nous avons beaucoup recours aux programmes de sensibilisation et d'emploi pour étudiants pour recruter, dans les universités, des personnes exceptionnelles qui travailleront sur ces problèmes.

Le président: Merci.

Le dernier intervenant est M. Erskine-Smith. Vous avez trois minutes.

M. Nathaniel Erskine-Smith: Je vais poser une question puis je vais céder la parole à Anita.

Lorsque certains d'entre nous étions à Washington, nous avons échangé à ce sujet avec des membres du Congrès. L'un d'eux nous a dit que ce qu'ils font chez eux, c'est qu'ils opposent l'équipe des bleus à l'équipe des rouges: leurs comptes sont piratés, soit par les membres du personnel politique, soit par les membres du Congrès eux-mêmes. On essaie de les pirater, puis on leur explique comment on s'y est pris et comment se protéger contre de futures attaques.

Prévoit-on entreprendre des tentatives de piratage dans le but d'améliorer notre démocratie?

Desvoix: Ha, ha!

M. André Boucher: Je serais ravi d'être invité à le faire.

Non, mais nous offrons des conseils aux partis politiques. Comme vous le savez peut-être, une des mesures que nous utilisons avec les directeurs de campagne et d'autres, c'est la simulation. Les courriels d'hameçonnage sont un bon exemple. Encore aujourd'hui, les courriels d'hameçonnage ont la menace plus courante que nous recevons toutes et tous dans nos boîtes de réception. Une campagne de sensibilisation visant à montrer aux gens à quoi ressemblent les courriels et comment y réagir, puis...

M. Nathaniel Erskine-Smith: Je le dis moins sérieusement, mais je vous encouragerais à communiquer avec vos homologues américains. Je pense que ce serait une bonne idée de procéder régulièrement à une simulation pareille au Canada.

Anita.

Mme Anita Vandenberg: Merci.

J'aimerais revenir sur le Protocole public en cas d'incident électoral majeur. Qu'arriverait-il sans ce protocole? Que fait-on en ce moment? Si je comprend bien, les partis politiques ne seraient pas du tout mis au courant. Si le protocole n'existait pas, n'importe quel membre du groupe pourrait s'adresser seul aux médias. Pire encore, un incident pourrait survenir, et aucun des membres n'en informerait la population ou les partis politiques.

Dites-moi, sans le protocole, qu'existe-t-il en ce moment? Qu'arriverait-il aujourd'hui si le protocole n'avait pas été mis en place?

M. Allen Sutherland: C'est une question très intéressante. Heureusement, elle est hypothétique.

En l'absence d'un protocole durant la période électorale, je pense que les fonctionnaires et même les ministres et le premier ministre seraient placés dans une position intenable: il leur incomberait de décider si un incident avait dépassé le seuil. Évidemment, on serait confronté à un dilemme partisan.

Le président: Merci à toutes et à tous.

J'ai seulement une question. Elle concerne le voyage à Washington que certains d'entre nous ont fait il y a environ un an et demi pour parler d'Equifax. J'ai trouvé alarmant de découvrir que nos bureaux de crédit ne sont passés sous une réglementation au Canada. Cela dit, la raison pour laquelle l'atteinte à la sécurité des données chez Equifax a été découverte, c'est parce que le département de la Sécurité intérieure, un organisme global, a averti Equifax que la sécurité de ses données était peut-être menacée. Il l'a averti plusieurs fois, mais Equifax n'a pas répondu et n'a pas réglé le problème. C'est ce qui a causé l'atteinte à la sécurité des données de quelque 150 millions d'Américains et d'environ 19 000 Canadiens.

Le Canada a-t-il un système semblable? Si la réponse est non, je préfère que vous ne répondiez pas. Vous me le direz plus tard. Avez-vous un processus semblable?

Ce qui me préoccupe, c'est une des déclarations de M. Rogers. Vous avez le mandat de mener une enquête en cas d'incident. Faut-il que l'incident soit allumé pour que vous l'éteigniez ou prenez-vous des mesures pour prévenir que l'incident se déclenche?

M. Dan Rogers: Permettez-moi d'apporter une correction avant de céder la parole à André, qui vous donnera une très bonne réponse. Nous menons des enquêtes sur les acteurs étrangers dans le but de découvrir leurs intentions, et ce, passeulement si quelqu'un porte le dossier à notre attention. Je suis désolé si je me suis mal exprimé.

Je vais céder la parole à André. Un des avantages de notre système, c'est que les capacités relatives au renseignement que nous mettons à contribution dans le domaine du renseignement électromagnétique étranger permettent de détecter les activités des auteurs de cybermenaces. Ces renseignements peuvent être transmis au Centre pour la cybersécurité afin que la détection soit faite dès le départ.

Le président: Il nous reste environ 30 secondes.

M. André Boucher: Vous faites bien de m'en avertir, si vous connaissez la relation avec le microphone.

Ce que M. Rogers vient de dire est une très bonne nouvelle: le fait que l'équipe du Canada est conjointement représentée est une grande force.

Il existe certainement un équivalent canadien du département de la Sécurité intérieure des États-Unis. En fait, le département de la Sécurité intérieure a aussi un centre pour la cybersécurité: la Cybersecurity and Infrastructure Security Agency, ou la CISA. Nos pratiques sont très semblables.

Je vous donne un exemple théorique: M. Rogers et son équipe découvrent qu'un Canadien est la cible d'une menace étrangère et ils en informent mon centre. Nous nous adressons alors directement à la personne concernée et, pour des raisons de réputation et autres, nous commençons par lui dire très discrètement: «Nous pensons que telle menace pesait sur vous; vous devriez faire quelque chose.» Toutefois, si c'est nécessaire, nous prenons des mesures plus publiques.

• (1730)

Le président: Avant de conclure je vous rappelle que le 28 mai, notre comité tiendra ici même la 2^e séance du Grand Comité international.

Le Canada et huit autres pays se réunissent à Londres pour parler des mêmes dossiers que nous avons abordés aujourd'hui, des menaces étrangères à la démocratie etc. La deuxième séance aura lieu au Canada. La liste d'invités sera semblable, nous inviterons des représentants de différentes plateformes à se joindre à nous.

Si vous avez des témoignages à nous recommander ou des conseils à nous donner, nous vous remercions à l'avance de nous en informer.

Merci de vous être joints à nous aujourd'hui.

Je souhaite à toutes et à tous une bonne fin de journée. La séance est levée.

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

PERMISSION DU PRÉSIDENT

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

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

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

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

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

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

SPEAKER'S PERMISSION

The proceedings of the House of Commons and its Committees are hereby made available to provide greater public access to the parliamentary privilege of the House of Commons to control the publication and broadcast of the proceedings of the House of Commons and its Committees, notwithstanding that all copyright herein are also reserved.

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

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

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

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