



CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

44^e LÉGISLATURE, 1^{re} SESSION

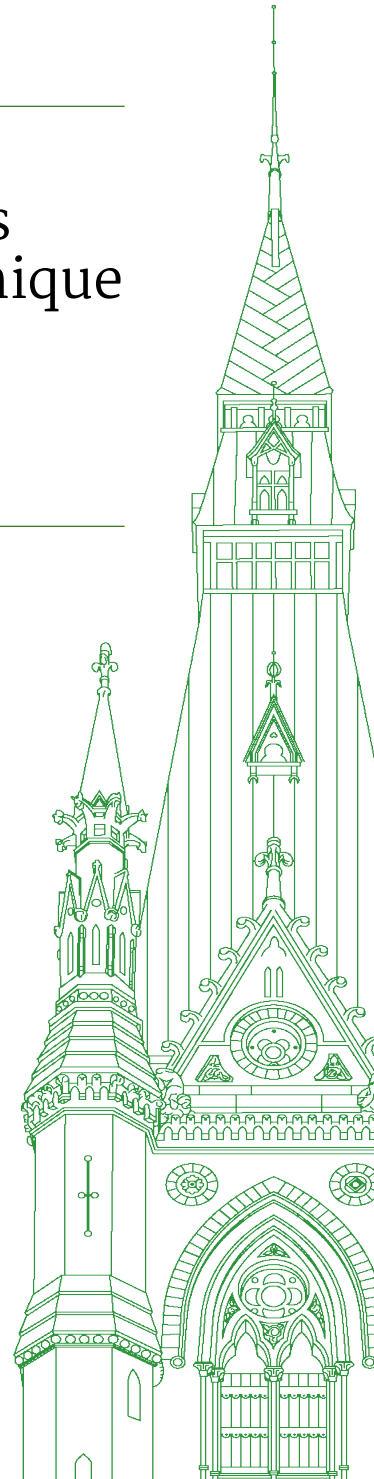
Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

TÉMOIGNAGES

NUMÉRO 132

Le mardi 8 octobre 2024

Président : M. John Brassard



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

Le mardi 8 octobre 2024

• (1545)

[Traduction]

Le président (M. John Brassard (Barrie—Innisfil, PCC)):
Bonjour à tous.

La séance est ouverte.

[Français]

Je vous souhaite la bienvenue à la 132^e réunion du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique.

Conformément à l'article 108(3)h) du Règlement et à la motion adoptée par le Comité le mardi 13 février 2024, le Comité reprend son étude sur l'incidence de la désinformation et de la mésinformation sur le travail des parlementaires.

[Traduction]

J'aimerais souhaiter la bienvenue à nos témoins pour la première heure de notre séance d'aujourd'hui.

De la Gendarmerie royale du Canada, nous accueillons M. Richard Baylin, directeur général, Cybercriminalité, et surintendant principal, Police fédérale, Opérations criminelles.

Bienvenue.

[Français]

Nous accueillons également M. Denis Beaudoin, directeur général de la sécurité nationale et surintendant principal de la police fédérale.

Monsieur Beaudoin, je vous souhaite la bienvenue au Comité.

[Traduction]

Nous recevons aussi M. Greg O'Hayon, directeur général, Police fédérale, Renseignement de sécurité et police internationale.

Bienvenue à vous également, monsieur O'Hayon.

Vous disposez de cinq minutes pour nous présenter votre déclaration préliminaire.

[Français]

Monsieur Beaudoin, vous avez la parole pour cinq minutes.

Surintendant principal Denis Beaudoin (directeur général, sécurité nationale et surintendant principal, Police fédérale, Gendarmerie royale du Canada): Merci, monsieur le président.

Je m'appelle Denis Beaudoin. Je suis surintendant principal et directeur général assumant la responsabilité de l'ingérence étrangère pour le Programme de sécurité nationale de la Police fédérale, à la Gendarmerie royale du Canada, ou GRC. Aujourd'hui, je suis accompagné de M. Richard Baylin, surintendant principal des en-

quêtes criminelles sur la cybercriminalité de la Police fédérale, ainsi que de M. Greg O'Hayon, directeur général du renseignement de sécurité de la Police fédérale.

D'abord, j'aimerais vous remercier de nous donner l'occasion d'aborder cette question. L'intrusion malveillante d'acteurs étrangers hostiles dans les processus démocratiques du Canada est l'une des principales priorités de la GRC.

Soyons clairs: l'ingérence étrangère touche toutes les sphères de la société, que ce soit les fondements de notre démocratie, les droits fondamentaux et les valeurs qui nous définissent en tant que société, notre prospérité économique, les infrastructures essentielles qui assurent notre bien-être, ou notre souveraineté.

Les acteurs étrangers ont recours à plusieurs tactiques pour atteindre leurs objectifs, notamment le harcèlement et l'intimidation des communautés au Canada, soutenus par un État étranger, la manipulation du discours à tous les niveaux de notre système politique et l'utilisation de tactiques malveillantes et trompeuses pour influencer sur notre démocratie.

Ne vous y trompez pas: des gouvernements étrangers mènent des campagnes de désinformation en ligne pour saper nos processus et institutions démocratiques et pour éroder la confiance des citoyens envers la démocratie.

La GRC est investie d'un vaste mandat lié à la sécurité nationale et à la cybercriminalité. Elle assure la sécurité publique en enquêtant sur l'ingérence étrangère, en contrant cette dernière et en la prévenant. Elle s'appuie sur les dispositions de diverses lois, y compris celles récemment adoptées dans le cadre du projet de loi C-70, ainsi que sur d'autres infractions visées par le Code criminel. Lorsque la GRC enquête sur des campagnes de désinformation, elle travaille en étroite collaboration avec ses partenaires nationaux et internationaux afin de déterminer les éléments de preuve pertinents, mais il arrive que des campagnes de désinformation ne constituent pas un acte criminel.

En gardant cela à l'esprit, j'exposerai brièvement le rôle que joue la GRC dans la protection du Canada, des citoyens, des résidents canadiens et des élus quant à l'ingérence étrangère.

[Traduction]

En 2019, le gouvernement du Canada a divulgué son plan pour protéger la démocratie canadienne. Ce plan visant à défendre nos institutions démocratiques comprend notamment des mesures pour renforcer le système électoral face à diverses menaces, y compris les cybermenaces et l'ingérence étrangère. Dès le départ, la GRC s'est engagée à contribuer à ces efforts pangouvernementaux.

Les élus et les titulaires d'une charge publique sont des figures centrales du système politique de notre démocratie, car ils façonnent nos politiques et nos lois. Ce rôle en fait des cibles de choix pour les États étrangers, qui peuvent tenter de les influencer ou de les contraindre à adopter des positions politiques servant leurs intérêts. C'est à ce titre que la GRC, en partenariat avec d'autres organismes gouvernementaux, a récemment tenu à l'intention des parlementaires des séances d'information sur la menace que représente l'ingérence étrangère. La GRC pilote également des initiatives visant à sensibiliser les services de police de tout le pays à la nouvelle loi instituée par le projet de loi C-70, ainsi qu'à la menace d'ingérence étrangère.

La GRC est aussi un membre actif du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections, qui coordonne les efforts de collecte et d'analyse de données au sujet des menaces pesant sur les processus électoraux fédéraux au Canada. Ce groupe est le principal mécanisme canadien de surveillance des menaces d'ingérence d'États hostiles pendant les élections. Il est composé d'experts du Service canadien de renseignement de sécurité, ou SCRS, du Centre de la sécurité des télécommunications du Canada, ou CST, et d'Affaires mondiales Canada.

À l'échelon fédéral, la GRC concentre ses efforts d'enquête sur les niveaux les plus élevés de cybercriminalité et travaille en étroite collaboration avec des partenaires nationaux et internationaux pour détecter au sein de l'écosystème de la cybercriminalité les menaces les plus sérieuses ayant des répercussions économiques ou d'autres impacts graves sur les intérêts canadiens au pays et à l'étranger, et prendre les mesures nécessaires pour contrer ces menaces et tenter des poursuites contre leurs auteurs. Les équipes d'enquête sur la cybercriminalité et les agents de liaison en cybercriminalité à l'étranger de la GRC se concentrent sur la prévention, l'application de la loi et la neutralisation des acteurs à l'origine des menaces les plus sérieuses et des principaux catalyseurs de la criminalité sophistiquée, tels que les logiciels malveillants, les rançongiciels, l'espionnage, l'ingérence étrangère, ainsi que les attaques contre les institutions gouvernementales, les actifs commerciaux clés et les infrastructures essentielles d'importance nationale.

Comme les membres du Comité le savent très bien, les menaces ciblant les titulaires d'une charge publique se sont multipliées ces dernières années. Comme nous sommes conscients des répercussions de cette tendance dans la vie des gens, ainsi que des préjudices causés à notre démocratie, cet enjeu demeure une priorité pour la GRC. Nous continuerons donc à lutter contre ces menaces dans le cadre de nos responsabilités à titre de police fédérale, en mobilisant d'autres forces policières et les différentes diasporas.

Compte tenu de l'ampleur des menaces, la collaboration entre la population, les services de police compétents et les partenaires du gouvernement du Canada continuera d'être un aspect important de la protection de notre pays contre l'ingérence étrangère.

La protection des processus démocratiques du Canada et la sécurité de ses citoyens et de ses résidents sont primordiales pour la GRC. Il sera important que toutes les sphères de la société conjuguent leurs efforts pour se protéger contre l'ingérence étrangère dans ce contexte.

Merci.

• (1550)

Le président: Merci, monsieur Beaudoin.

Je tiens aussi à remercier votre organisation. Plus tôt cette année, le Comité a eu l'occasion de visiter l'École de la GRC à Ottawa. Le sous-commissaire Larkin nous a alors fourni un large éventail de renseignements sur les outils utilisés pour l'extraction de données, la surveillance de la cybercriminalité et l'ingérence étrangère.

Est-ce que l'un d'entre vous était présent à ce moment-là? Non? D'accord. M. Fisher y était; je vois sa main à l'arrière.

Nous allons commencer notre première série de questions. Chaque parti disposera d'une période de six minutes. Nous allons commencer par M. Barrett.

À vous la parole, monsieur Barrett.

M. Michael Barrett (Leeds—Grenville—Thousand Islands et Rideau Lakes, PCC): La GRC reçoit-elle un financement suffisant pour contrer les cybermenaces qui pèsent sur le Canada?

Surintendant principal Richard Baylin (directeur général, Cybercriminalité et surintendant principal, Police fédérale, Opérations criminelles, Gendarmerie royale du Canada): C'est le sous-commissaire Flynn, si je ne m'abuse, qui soulignait la semaine dernière qu'il est impossible de parler à un chef de police n'importe où au Canada sans que la question des ressources vienne sur le tapis. Je peux toutefois vous dire que la GRC a des équipes de cybersécurité partout au pays. Nous avons travaillé à la constitution de ces équipes, à leur dotation et à leur formation en vue de l'adaptation aux menaces, et nous y affectons des ressources supplémentaires. J'estime que nous sommes effectivement en mesure de déployer des moyens permettant de contrer la criminalité à un niveau correspondant à celui d'une véritable menace.

M. Michael Barrett: Je vois.

D'autres corps policiers ont besoin de plus de ressources, mais pas la GRC. C'est ce que j'extrapole de votre réponse.

Disposez-vous des ressources nécessaires pour faire face aux menaces qui pèsent sur le Canada? Un oui ou un non rapide serait grandement apprécié.

• (1555)

Surint. pr. Richard Baylin: Il vaudrait certainement la peine d'avoir une discussion au sujet des ressources nécessaires.

Oui, je dirais que nous disposons actuellement de ressources suffisantes pour faire face à la menace.

M. Michael Barrett: D'accord.

Le gouvernement pourrait-il en faire davantage pour prévenir l'ingérence étrangère et protéger les Canadiens contre l'intimidation exercée par des États étrangers hostiles?

Surint. pr. Denis Beaudoin: Il est difficile pour la GRC de commenter les actions du gouvernement, monsieur le président.

Ce que nous pouvons dire, c'est que nous accueillons favorablement les nouvelles mesures législatives découlant du projet de loi C-70, qui a été adopté récemment, soit le 19 août dernier. Nous avons hâte de travailler avec nos partenaires du Service des poursuites pénales du Canada pour voir ce que cette nouvelle loi pourra nous permettre de faire.

Votre question précédente portait sur la cybercriminalité, la sécurité nationale et l'ingérence étrangère. Nous avons récemment reçu du financement par l'entremise d'un mémoire au Cabinet sur les activités hostiles des acteurs étatiques. Il n'en demeure pas moins que la montée de l'extrémisme violent au Canada va certes mettre nos capacités à l'épreuve.

M. Michael Barrett: Dans quelle mesure y a-t-il l'interopérabilité entre la GRC et le CSTC dans les dossiers de cet ordre? Suivant sa propre description, le CSTC est l'organisme national « responsable du renseignement électromagnétique étranger, des cyberopérations et de la cybersécurité ». Existe-t-il une entité chargée de contrer les cybermenaces d'États étrangers hostiles qui ciblent les Canadiens?

J'aurais besoin d'une réponse très brève.

Surint. pr. Richard Baylin: La réponse courte est oui, il y en a une.

M. Michael Barrett: D'accord. Et comment s'appelle cette entité?

Surint. pr. Richard Baylin: Il s'agit du GNCC, le Groupe national de coordination contre la cybercriminalité. Lorsque de nouvelles menaces se pointent à l'horizon, on en discute en outre au sein de différents comités et sur d'autres tribunes.

M. Michael Barrett: Si un Canadien était ciblé par un État étranger hostile — par exemple, au moyen d'un malicieux parrainé par cet État ou d'un piratage intercepté par vos services ou vos partenaires du CSTC —, comment ce Canadien apprendrait-il ce qui s'est passé? Lui diriez-vous qu'un État étranger l'a ciblé?

Surint. pr. Richard Baylin: Cela dépend de la nature de ce qui a été mis au jour et de qui l'a détecté.

C'est au sein de ce groupe que les discussions ont lieu en vue d'harmoniser les efforts. Une décision est alors prise quant à la nature de la menace et aux moyens à mettre en oeuvre pour la contrer.

M. Michael Barrett: Nous avons bien évidemment eu droit à un exemple où des parlementaires de tous les partis ont été la cible d'une attaque parrainée par un État étranger, via le groupe APT31. C'est ce que nous avons appris plus tôt cette année. Les individus ciblés étaient tous des législateurs. Aucune des personnes visées n'en a été informée par vos services. Il est intéressant de savoir que l'on a effectivement discuté de cette problématique. Le document en question aurait été transféré à la Chambre des communes. Cela n'est guère rassurant tant pour les personnes touchées que pour les autres Canadiens qui continuent à se demander ce qui leur arriverait s'ils étaient ciblés. En seraient-ils informés directement, ou devraient-ils compter sur le fait que leur employeur en serait avisé pour les mettre au courant par la suite? Devraient-ils attendre que le FBI les en informe? C'est ce qui s'est passé en l'espèce. C'est ainsi que les Canadiens ont appris que cela s'était produit.

Il y a deux ou trois questions sur lesquelles la police fédérale se penche en ce moment — des enquêtes dans quelques dossiers concernant le gouvernement.

Êtes-vous en mesure de faire le point avec nous sur l'enquête relative à l'arnaque ArriveCAN de 60 millions de dollars?

Surint. pr. Denis Beaudoin: Nous n'allons pas commenter une enquête. De plus, cela ne relève pas du portefeuille de la sécurité nationale, alors je ne suis certainement pas la bonne personne pour répondre à ces questions.

M. Michael Barrett: A-t-il indiqué qu'il n'était pas en mesure de répondre à la question? Je n'entends pas bien ce qu'il dit.

Le président: C'est ce que j'ai entendu.

Monsieur Beaudoin, si vous pouviez parler un peu plus fort, ce serait utile.

J'ai du mal à l'entendre, mais c'est bien ce qu'il a dit, monsieur Barrett.

Surint. pr. Denis Beaudoin: Je suis désolé.

La seule chose que j'ai dite, c'est que nous n'allons pas commenter une enquête. Cette question ne relève pas de ma responsabilité, alors je ne suis certainement pas la bonne personne pour y répondre.

• (1600)

Le président: Merci, monsieur Beaudoin.

Merci, monsieur Barrett.

Monsieur Housefather, vous avez six minutes.

M. Anthony Housefather (Mont-Royal, Lib.): Merci, monsieur le président.

Merci, messieurs, d'être avec nous aujourd'hui.

La GRC mène-t-elle actuellement une enquête pour savoir si des pays étrangers sont impliqués dans les campements établis l'an dernier sur des campus universitaires, les manifestations qui visent à glorifier le terrorisme et l'Iran et les actions du réseau Samidoun? Faites-vous enquête à ce sujet?

Surint. pr. Denis Beaudoin: Encore là, il ne nous est pas possible de faire des commentaires sur quelque enquête que ce soit.

M. Anthony Housefather: Je ne vous demande pas de faire des commentaires. Je veux juste savoir si vous vous penchez sur la question.

Surint. pr. Denis Beaudoin: Eh bien, vous me demandez de parler de nos enquêtes, et je viens d'expliquer à votre collègue que nous ne pouvons pas vous fournir de détails à ce sujet.

M. Anthony Housefather: Je ne pense pas qu'une réponse par oui ou par non à la question de savoir si... Est-ce que ces situations vous préoccupent?

Surint. pr. Denis Beaudoin: Oui. Nous surveillons certainement ce qui se passe au Canada, et nous avons des gens qui suivent l'évolution des choses.

M. Anthony Housefather: Lorsque se tiennent des manifestations comme celle que nous avons eue hier à Montréal, alors que des bâtiments de l'Université McGill ont été endommagés et que nous savions que ces manifestations allaient avoir lieu, quel est le rôle de la GRC en ce qui concerne la coordination avec la police locale?

Surint. pr. Denis Beaudoin: Nous communiquons avec les autorités policières dès que nous savons que certains événements vont avoir lieu, et nous demeurons en contact avec elles. Lorsque les choses se concrétisent, nous assurons la liaison pour voir si l'incident met en cause notre sécurité nationale.

M. Anthony Housefather: Avant que quelque chose ne se produise, faites-vous enquête pour voir s'il y a des liens entre la sécurité nationale et la manifestation prévue, et en avisez-vous les services policiers locaux?

Surint. pr. Denis Beaudoin: Oui.

M. Anthony Housefather: D'accord.

Pour revenir à la question de M. Barrett, je comprends qu'il peut y avoir des situations où vous devez déterminer si une personne devrait être mise au courant d'une menace étrangère parce que vous soupçonnez cette personne d'être de connivence avec une source étrangère ou d'être un agent de cette source étrangère. En revanche, si la GRC en arrive à la conclusion que la personne en question n'a rien à se reprocher, pour quelle raison ne l'avertirait-on pas qu'elle est exposée aux menaces d'une source étrangère?

Surint. pr. Denis Beaudoin: Il y a diverses raisons, y compris lorsque nous devons traiter avec des États étrangers dans le cadre d'une telle enquête. Il pourrait y avoir des limitations quant à l'utilisation des renseignements en notre possession. Il est possible qu'un autre organisme nous demande de ne pas donner suite à l'affaire. Il y a un large éventail de raisons pour lesquelles nous pourrions choisir de ne pas aviser la personne dans un cas particulier.

M. Anthony Housefather: Vous comprenez, bien sûr, que pour un parlementaire, il est très effrayant de penser qu'une telle menace puisse peser sur nous sans que nous le sachions, alors que vos services sont au courant.

Je ne connais pas le jargon policier, mais il semble y avoir un décalage entre ce que la personne menacée par cette source étrangère voudrait savoir et ce que vous pourriez ou voudriez lui dire.

Comment protégez-vous quelqu'un s'il n'est pas au courant de cette menace imminente d'une source étrangère, ou d'une menace continue d'une source étrangère, si vous ne pouvez pas le lui dire parce que, par exemple, votre source dans un autre pays vous a demandé de ne pas le faire?

Surint. pr. Denis Beaudoin: Comme je l'ai dit, nous avons à cœur la sécurité de tous les Canadiens, y compris les parlementaires. J'ai moi-même transmis de l'information à tous les partis au mois de juin afin de m'assurer que tous les parlementaires sont au fait des menaces qui pourraient peser sur eux. La GRC prend cette question très au sérieux.

En ce qui concerne des cas précis, comme je l'ai dit, nous ne faisons pas de commentaires sur les enquêtes, mais en général, il y a un certain nombre de questions qui entrent en jeu et dont nous devons nous occuper. Il arrive que nous déterminions qu'il est possible d'aviser la personne concernée. Il y a parfois des raisons opérationnelles pour lesquelles nous ne le faisons pas et d'autres occasions où nous ne le savons pas nous-mêmes.

M. Anthony Housefather: Me reste-t-il du temps, monsieur le président?

Le président: Il vous reste une minute et demie.

M. Anthony Housefather: Je veux donc en venir aux communications, car d'après ce que je comprends, aux États-Unis, les forces de l'ordre, le FBI, sont beaucoup plus disposées à divulguer des renseignements plus rapidement et plus clairement que la GRC. C'est ce que je constate au sujet de la tentative d'assassinat de Trump, par exemple, pour laquelle on a divulgué des renseignements qui, à mon avis, n'auraient pas été divulgués au Canada avant longtemps, mais qui, aux États-Unis, après la tentative d'assassinat en Pennsylvanie, l'ont été très ouvertement. Les organismes d'application de la loi diffusaient l'information ouvertement.

Je pense que les gens au Canada ont l'impression que la GRC devrait communiquer de façon beaucoup plus ouverte et claire, en particulier en ce qui concerne les menaces. Qu'en pensez-vous?

• (1605)

Surint. pr. Denis Beaudoin: Les lois sur la protection de la vie privée dans nos deux pays sont extrêmement différentes. Nous devons en tenir compte dans la communication de l'information. Cependant, nous allons sur le terrain. Nous diffusons de l'information. Nous menons de nombreuses campagnes d'information pour aider les Canadiens à tous les niveaux à comprendre les menaces qui pèsent sur différentes diasporas. Nous veillons à ce que les gens soient au courant de ce qui se passe et des menaces provenant d'États étrangers.

M. Anthony Housefather: Merci, monsieur le président.

Le président: Merci, monsieur Housefather.

[Français]

Avant de donner la parole à M. Trudel, je veux dire aux témoins que chaque député a six minutes ou moins pour poser ses questions. Si un député vous interrompt, ne vous sentez pas personnellement visés. C'est parce que le temps s'écoule très vite lors des questions et des réponses.

Monsieur Trudel, vous avez la parole pour six minutes.

M. Denis Trudel (Longueuil—Saint-Hubert, BQ): Merci, monsieur le président.

Merci infiniment, messieurs, d'être ici aujourd'hui.

Je vais revenir à la dernière question posée par mon collègue, M. Housefather, car je l'ai trouvée intéressante. Il parlait de l'attentat perpétré contre Donald Trump. Il a mentionné que l'on avait obtenu des renseignements plus rapidement aux États-Unis qu'on ne les aurait obtenus ici, au Canada. Vous avez répondu que les lois étaient différentes aux États-Unis.

En quoi cela concerne-t-il ce dossier en particulier? Quelles modifications le Canada pourrait-il apporter à sa législation pour qu'il puisse avoir accès à de tels renseignements?

Surint. pr. Denis Beaudoin: Tout d'abord, je ne peux pas faire de commentaires sur le temps que le Federal Bureau of Investigation, ou FBI, prend pour donner des renseignements sur une situation ou une autre. Toutefois, en général, la législation du Canada sur la protection de la vie privée est beaucoup plus restrictive que celle adoptée aux États-Unis.

Si les parlementaires veulent débattre là-dessus, c'est une chose, mais présentement, il n'est pas possible de rendre publics certains renseignements à cause de la législation sur la protection de la vie privée.

M. Denis Trudel: Il semble que, aux États-Unis, le FBI ne sent pas le besoin de cacher de l'information, alors que c'est le cas ici.

Que pouvez-vous nous dire là-dessus?

Surint. pr. Denis Beaudoin: Je ne pense pas qu'il s'agit de cacher de l'information, monsieur Trudel.

D'abord, je ne peux pas vous parler de ce que le FBI veut faire ou non. La question devrait être adressée à ses représentants. À la GRC, nous ne sommes pas là pour cacher de l'information. Comme je l'ai dit, nous menons plusieurs campagnes de sensibilisation auprès du public pour informer les gens concernant... Comment dire « *threat* »?

M. Denis Trudel: La menace.

Surint. pr. Denis Beaudoin: C'est le mot que je cherchais. La nature de la menace a changé au cours des dernières années.

À la GRC, nous essayons d'être le plus transparents possible, mais, quand il y a des enquêtes en cours, nous ne pouvons pas communiquer certains renseignements.

M. Denis Trudel: Dites-moi si je fais erreur, mais vous semblez dire que la menace est pire maintenant qu'elle ne l'était il y a cinq ou dix ans.

Laissez-vous entendre aussi que vous n'avez pas, en ce moment, les outils nécessaires pour lutter contre cette menace?

Surint. pr. Denis Beaudoin: Comme je l'ai dit, la nature de la menace a changé. Nous devons composer avec le caractère idéologique de la violence exercée par des personnes, ce qui est nouveau. L'ingérence étrangère est certainement une nouvelle menace, et nous le constatons depuis une dizaine d'années.

Tout investissement de la part du gouvernement dans les programmes relatifs à ces menaces est bienvenu, et la GRC lui en sera toujours reconnaissante. Cela nous aide certainement à en faire davantage pour les Canadiens.

M. Denis Trudel: Y a-t-il, en ce moment même, des enquêtes actives concernant des parlementaires au Canada?

Surint. pr. Denis Beaudoin: Je ne peux pas faire de commentaires là-dessus aujourd'hui, monsieur Trudel.

M. Denis Trudel: Tantôt, dans vos remarques préliminaires, vous avez dit que l'ingérence n'était pas toujours criminelle.

Pouvez-vous m'expliquer exactement ce que vous vouliez dire?

Selon ce que j'ai compris, il pourrait y avoir de l'ingérence légale et de l'ingérence criminelle. Or, j'imagine que vous intervenez seulement quand c'est criminel. Il faut donc faire la différence entre les deux.

Surint. pr. Denis Beaudoin: Nous avons été invités à comparaître devant vous afin de parler de désinformation et de désinformation. C'est pourquoi je m'exprimerai uniquement sur ce sujet.

Si quelqu'un a une opinion qui diverge de celle d'autres personnes, ce n'est pas nécessairement criminel. Selon la législation qui est entrée en vigueur au mois d'août, un acte criminel est commis quand l'objectif de la désinformation est d'influer sur un processus électoral ou gouvernemental. Il faut donc prouver que certains éléments sont présents pour enquêter sur une infraction criminelle.

• (1610)

M. Denis Trudel: Tantôt, vous avez dit que les nouvelles menaces avaient un caractère plus violent qu'auparavant.

À quoi faisiez-vous allusion?

Surint. pr. Denis Beaudoin: Je faisais allusion à la menace motivée par l'idéologie, c'est-à-dire la menace que représente l'extrémisme violent à motivation idéologique, ou EVMI.

M. Denis Trudel: Vous ne parlez pas de violence physique.

N'est-ce pas?

Surint. pr. Denis Beaudoin: Non, il s'agit d'extrémisme violent qui est motivé par une idéologie. Ce type de menace a aussi augmenté. Nous devons réorienter certaines ressources existantes à la Sécurité nationale en fonction du type de menace et des renseignements qui nous sont communiqués.

M. Denis Trudel: D'accord.

Le Globe and Mail a publié ce matin un article dans lequel on dit qu'en ce moment, la GRC a du mal à répondre à la menace d'ingérence étrangère de pays tels que la Chine, l'Inde, l'Iran, la Russie, et ainsi de suite, parce qu'elle doit agir en fonction d'un mandat confus.

Selon vous, votre mandat est-il confus?

Quel serait le mandat qui devrait vous être confié pour que vous puissiez lutter efficacement contre les menaces provenant de ces pays?

Que manque-t-il dans la législation actuelle et de quels outils avez-vous besoin dans ce contexte?

Surint. pr. Denis Beaudoin: Nous avons obtenu de nouveaux outils, il y a environ six semaines. Nous avons hâte d'étudier leur fonctionnement et de les utiliser. Il est certain que nous allons toujours avoir besoin d'accroître nos ressources.

Pour ce qui est de l'affirmation selon laquelle notre mandat est confus, je ne crois pas que ce soit le cas. Au fur et à mesure que la menace change, il faut assurément s'adapter. Nos enquêteurs doivent étudier toute nouvelle menace, et nous devons offrir de la formation en conséquence. La situation étant en constante évolution, il faut aussi sensibiliser la population de façon continue à cet égard.

M. Denis Trudel: Il y aura peut-être des élections bientôt.

Vous préparez-vous de façon particulière à cette éventualité?

M. Greg O'Hayon (directeur général, police générale et renseignements de sécurité, Renseignements et Police internationale, Gendarmerie royale du Canada): Je représente la GRC au sein du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections. Cela doit faire au moins huit mois que nous nous préparons en vue de la prochaine élection, parce que nous nous attendons justement à ce qu'il y ait de l'ingérence.

Pour ce qui est de la question relative aux menaces...

Le président: Je vous demanderais d'être bref, M. O'Hayon.

M. Greg O'Hayon: À l'époque, on pensait que...

Le président: Malheureusement, le temps de parole est écoulé.

Monsieur Trudel, vous aurez un autre tour de paroles de deux minutes et demie plus tard.

[Traduction]

Monsieur Green, allez-y, s'il vous plaît. Vous avez six minutes, et peut-être un peu plus.

M. Matthew Green (Hamilton-Centre, NPD): Merci.

Dans le cadre de l'étude du Comité sur l'utilisation des plateformes de médias sociaux pour la collecte de données et le partage non éthique ou illicite de renseignements personnels avec des entités étrangères, Brigitte Gauvin, commissaire adjointe par intérim de la Police fédérale pour la sécurité nationale à la GRC, a mentionné que le programme de sécurité nationale de la GRC enquête sur les activités criminelles, et que si ces activités ont trait à l'ingérence étrangère, il y a enquête. Cependant, elle a souligné que la GRC n'enquête pas sur les médias sociaux pour savoir s'il y a désinformation, désinformation ou tentative d'influence. Elle enquête seulement s'il y a une activité criminelle.

Pourquoi la GRC n'enquête-t-elle pas sur la mésinformation, la désinformation ou les tentatives d'influence sur les plateformes de médias sociaux?

Surint. pr. Denis Beaudoin: Comme je l'ai dit plus tôt, certains cas de mésinformation et de désinformation peuvent ne pas être illégaux en soi. La GRC doit donc vérifier si une infraction criminelle a été commise. Si c'est le cas, nous allons bien sûr mener une enquête. Cela relève de notre mandat en matière de sécurité nationale. Lorsqu'il s'agit de cybercriminalité, mon collègue, M. Baylin, mène une enquête.

M. Matthew Green: Merci.

Pour la gouverne du Comité, compte tenu de l'étude dont nous sommes saisis, dans quel contexte, le cas échéant, la diffusion de désinformation en ligne pourrait-elle faire l'objet d'une enquête criminelle de la GRC?

Surint. pr. Denis Beaudoin: Comme je l'ai mentionné plus tôt, c'est si cela visait à influencer les processus gouvernementaux. Cela la rendrait illégale.

• (1615)

M. Matthew Green: À quand remonte la dernière enquête de ce genre? Vous n'avez pas à donner de détails, mais donnez-nous une idée de la fréquence à laquelle cela peut se produire.

Surint. pr. Denis Beaudoin: L'un des nouveaux articles est entré en vigueur il y a quelques semaines à peine.

M. Matthew Green: Depuis que ce nouvel article est entré en vigueur, il y a déjà eu une enquête en vertu des nouveaux paramètres. Est-ce exact?

Surint. pr. Denis Beaudoin: Non, je dis simplement qu'il s'agit d'une loi très récente. À l'heure actuelle, je ne pense pas qu'elle ait été utilisée, mais encore une fois, il y a de nombreuses enquêtes en cours partout au pays.

M. Matthew Green: Avant cela, il n'y en a pas eu. Ai-je bien compris?

Surint. pr. Denis Beaudoin: En ce qui concerne la désinformation, elle ne s'accompagne pas nécessairement de menaces, mais si c'était le cas, nous pourrions utiliser le Code criminel. Nous devons examiner tous les faits et ne pas nous limiter au terme « désinformation ». Nous avons beaucoup de dispositions dans le Code criminel que nous pourrions utiliser.

M. Matthew Green: Je suis désolé. J'ai besoin d'éclaircissements parce que je ne comprends pas la réponse, si on veut. Si j'ai bien compris, vous avez dit que le seuil pour que ce soit criminel est qu'il y ait des preuves d'une campagne d'influence ou d'une ingérence étrangère pour modifier la politique du gouvernement. N'est-ce pas exact?

Surint. pr. Denis Beaudoin: Oui, c'est l'ingérence dans les processus gouvernementaux.

M. Matthew Green: D'accord. Cela dit, au cours de votre carrière, avez-vous déjà mené une enquête qui atteignait ce seuil?

Surint. pr. Denis Beaudoin: Comme je l'ai dit, pas personnellement, parce qu'il s'agit d'une nouvelle loi; elle est entrée en vigueur il y a environ six semaines.

M. Matthew Green: Encore une fois, je suis désolé; je ne cherche pas à m'obstiner ici. Pour être clair, il n'y a pas eu, avant cela, d'enquête de ce genre.

Surint. pr. Denis Beaudoin: En ce qui concerne les processus gouvernementaux... Non. Cependant, ce que j'essayais d'expliquer,

c'est qu'un acteur étranger étatique pourrait avoir commis une infraction liée à d'autres articles dans le Code criminel — pas nécessairement liée à la désinformation en soi — que nous pourrions utiliser.

M. Matthew Green: D'accord. Encore une fois, dans le cadre de notre étude sur les plateformes de médias sociaux, Bryan Larkin, sous-commissaire des Services de police spécialisés de la GRC, a déclaré que la GRC entretient « des relations suivies avec toutes les plateformes de médias sociaux » par l'entremise de son Centre national de coordination en cybercriminalité et que la GRC a également « mis en place des protocoles, notamment en ce qui concerne l'exploitation des enfants et les préjudices causés aux jeunes ».

Compte tenu de la nouvelle loi, la GRC a-t-elle maintenant un protocole précis en place en ce qui concerne les États étrangers qui diffusent de la désinformation en ligne au Canada?

Surint. pr. Denis Beaudoin: Je ne suis pas certain de comprendre la question, monsieur. Demandez-vous si nous avons des contacts au sein des plateformes de médias sociaux concernant la désinformation?

M. Matthew Green: M. Larkin a dit que c'était le cas.

Surint. pr. Denis Beaudoin: Oui, nous en avons.

M. Matthew Green: Voici donc ma question: avez-vous des politiques ou des protocoles précis en place en ce qui concerne les États étrangers qui diffusent de la désinformation en ligne au Canada, que ce soit au Centre national de coordination en cybercriminalité ou ailleurs à la GRC?

Surint. pr. Denis Beaudoin: Nous sommes en contact — surtout dans le cas des grandes plateformes — avec leur service de sécurité pour un large éventail d'enquêtes, parce que les médias sociaux sont utilisés par tous les criminels, pas seulement à des fins de désinformation, alors nous sommes en contact avec elles pour obtenir de l'information...

M. Matthew Green: Monsieur...

Surint. pr. Denis Beaudoin: ... lorsque c'est nécessaire, alors...

M. Matthew Green: Je suis désolé. Je vais vous poser la question suivante, et c'est aux fins de notre étude. Pouvez-vous fournir au Comité les protocoles précis que vous avez mis en place et qui concernent les États étrangers qui diffusent de la désinformation en ligne au Canada? Pouvez-vous le faire pour nous?

Surint. pr. Denis Beaudoin: J'essaie de répondre à la question, monsieur. Ce que j'essayais d'expliquer, c'est que nous n'avons pas... Nous ne patrouillons pas dans Internet. Nous n'avons pas de... Il faut qu'il y ait une victime. Lorsque des gens communiquent avec nous pour des allégations de désinformation et d'infractions criminelles qui se seraient produites sur une plateforme, nous avons alors des protocoles pour communiquer avec les entreprises de médias sociaux afin de nous assurer de recueillir cette désinformation.

M. Matthew Green: Pouvez-vous nous donner des exemples de la façon dont la GRC interagit avec la population ou les entités privées que vous venez d'énumérer, ou avec les communautés vulnérables, pour les sensibiliser aux risques d'activités d'ingérence étrangère?

Surint. pr. Denis Beaudoin: Oui. Vous demandez des exemples. Si nous recevons une plainte d'une personne qui a reçu des menaces en ligne de la part d'un État étranger ou d'acteurs d'un État étranger, nous communiquons alors avec la plateforme de médias sociaux, parfois de façon urgente si la vie de la personne est en danger, pour obtenir des renseignements sur l'auteur de la menace, assurer la sécurité publique et mettre fin aux menaces qui pèsent sur la personne.

• (1620)

Le président: Vous aurez une autre occasion, monsieur Green. Nous allons revenir à vous dans quelques minutes.

Cela met fin à notre première série de questions. M. Cooper va commencer notre deuxième série de questions de cinq minutes.

Allez-y, monsieur Cooper.

M. Michael Cooper (St. Albert—Edmonton, PCC): Monsieur le président, le 10 avril dernier, le *Globe and Mail* a rapporté qu'en 2019, le candidat libéral de l'époque, et maintenant député de Don Valley-Nord, avait été averti par un membre du Parti libéral qu'il était surveillé par le SCRS.

Il a été confirmé lors de l'enquête publique sur l'ingérence étrangère que seuls quelques libéraux haut placés, étroitement liés au premier ministre, étaient présents à une séance d'information classifiée du SCRS pendant laquelle cette information a été communiquée. Trois libéraux haut placés ont assisté à la séance d'information, y compris Azam Ishmael, le directeur national du Parti libéral. M. Ishmael a ensuite informé Jeremy Broadhurst, qui avait la cote de sécurité requise, Broadhurst étant un conseiller principal du premier ministre. Broadhurst a ensuite informé le premier ministre.

Ce que nous savons, c'est que cinq libéraux haut placés, y compris le premier ministre lui-même, ont été informés. Cette information a donné lieu à une fuite dans le cadre de laquelle un candidat, maintenant député, a été averti qu'il était surveillé par le SCRS.

Pouvez-vous confirmer que le fait de divulguer sciemment des renseignements classifiés constitue une infraction au titre des articles 13 et 14 de la Loi sur la protection de l'information?

Surint. pr. Denis Beaudoin: Oui. Le fait de divulguer des renseignements classifiés constitue une infraction criminelle.

M. Michael Cooper: Serait-il juste de dire qu'il s'agit d'une infraction grave passible d'une peine d'emprisonnement pouvant aller jusqu'à 14 ans?

Surint. pr. Denis Beaudoin: Oui. Je crois que vous avez raison.

M. Michael Cooper: À la suite de l'article du *Globe and Mail*, j'ai envoyé une lettre au commissaire de la GRC, datée du 12 avril de cette année, pour porter à son attention cette apparente atteinte grave à la sécurité nationale dont les preuves pointent vers cinq libéraux haut placés, dont un ou plusieurs ont peut-être trahi leur serment du secret et divulgué des renseignements classifiés, en compromettant ainsi des opérations de sécurité nationale en cours. Le 3 mai 2024, j'ai reçu une lettre du commissaire accusant réception de ma lettre.

Depuis ce temps, la GRC a-t-elle ouvert une enquête?

Surint. pr. Denis Beaudoin: Monsieur le président, je ne peux pas faire de commentaires sur le fait qu'il y ait ou non une enquête.

M. Michael Cooper: D'accord. Je comprends que vous ne puissiez pas faire de commentaires si une enquête a été ouverte, mais le

commissaire a dit dans sa lettre que la GRC examinerait cette information.

La GRC a-t-elle examiné l'information entourant les allégations très sérieuses mentionnées dans l'article du *Globe and Mail* au sujet d'une atteinte grave à la sécurité nationale impliquant de hauts dirigeants libéraux proches du premier ministre, peut-être même le premier ministre lui-même?

Surint. pr. Denis Beaudoin: Monsieur le président, encore une fois, je ne peux pas faire de commentaires à ce sujet.

M. Michael Cooper: Eh bien, la GRC a-t-elle communiqué avec l'un ou l'autre de ces libéraux hauts placés?

Surint. pr. Denis Beaudoin: Monsieur le président, encore une fois, je ne vais pas commenter...

M. Michael Cooper: Eh bien, je pense qu'il doit y avoir un certain niveau de transparence. Je sais que vous ne pouvez pas faire de commentaires sur une enquête en cours. Je comprends cela. Je respecte cela.

Je vais vous poser la question ainsi: le premier ministre a-t-il communiqué avec la GRC? A-t-il porté cette atteinte à la sécurité nationale à l'attention de la GRC?

Surint. pr. Denis Beaudoin: Monsieur le président, c'est la même réponse: je ne vais pas faire de commentaires à ce sujet.

M. Michael Cooper: Eh bien, il est intéressant que vous ne puissiez pas faire de commentaires.

Il est également intéressant de noter que le premier ministre n'a rien dit à ce sujet. Il n'a certainement pas dit qu'il avait porté l'affaire à l'attention de la GRC.

Nous avons vu les libéraux au Comité tenter de faire obstruction aux efforts pour faire toute la lumière sur cette atteinte grave à la sécurité nationale. Franchement, le silence du premier ministre et l'obstruction des députés libéraux — sans aucun doute à la demande du premier ministre — s'inscrivent dans une tendance chez ce premier ministre.

Cela s'inscrit dans une tendance chez un premier ministre qui ne cesse de faire passer ses intérêts politiques personnels et partisans avant notre sécurité nationale, et qui protège des libéraux haut placés impliqués dans un crime grave, soit la divulgation de renseignements classifiés qui pourraient avoir compromis une enquête du SCRS sur les activités d'ingérence de Pékin.

Les Canadiens méritent mieux.

Merci, monsieur le président.

• (1625)

Le président: Merci, monsieur Cooper.

Nous passons maintenant à M. Bains, pendant cinq minutes.

Allez-y, monsieur.

M. Parm Bains (Steveston—Richmond-Est, Lib.): Merci, monsieur le président.

Je remercie les directeurs généraux respectifs d'être avec nous aujourd'hui.

Je veux parler du projet de loi C-70. Vous avez dit, je pense, que ces modifications législatives étaient les bienvenues. Pouvez-vous nous parler de la cybersécurité et de la façon dont elle recoupe la sécurité de l'information et le renseignement électromagnétique? Pensez-vous que suffisamment d'améliorations ont été apportées grâce à ce projet de loi? Cela vous donne-t-il plus de pouvoirs et plus de marge de manœuvre pour cibler, en particulier, la désinformation, la désinformation ou toute menace étrangère?

Surint. pr. Richard Baylin: Je peux vous parler d'un élément du point de vue de la cybersécurité. Il est certain que nous sommes mieux outillés qu'auparavant. Comme mon collègue, M. Beaudoin, l'a mentionné, il est encore très tôt. Nous verrons où cela nous mènera et quelle marge de manœuvre supplémentaire cela nous apportera, mais il est certain que nous sommes mieux outillés qu'auparavant.

M. Parm Bains: Ces modifications ont été apportées après des décennies passées à appliquer les mêmes mesures. Au sujet des nouvelles infractions, disposez-vous actuellement des ressources nécessaires pour répondre à vos besoins? Je comprends que c'est nouveau, et vous y travaillez probablement. Je crois que vous avez dit que certaines dispositions sont entrées en vigueur la semaine dernière. Pouvez-vous nous parler des processus qui ont été mis en place et de ce qu'il vous reste à faire pour vraiment mettre cela en œuvre?

Surint. pr. Richard Baylin: Je peux en parler, dans une certaine mesure. Au cours des 18 derniers mois, voire des deux dernières années, la menace liée à la cybersécurité a évolué. Au départ, il s'agissait principalement de menaces tactiques ou de menaces criminelles. Nos équipes d'enquêtes sur la cybersécurité se concentraient principalement sur ces aspects de la cybercriminalité. Ce n'est que plus récemment que nous avons commencé à examiner des éléments comme ceux dont nous parlons ici aujourd'hui — la désinformation — en tant que menace stratégique à la sécurité nationale.

C'est ce qui a mené à ce projet de loi. Nous continuerons de travailler dans ce cadre pour voir où cela nous mènera, mais oui, absolument, nous sommes mieux outillés qu'auparavant.

M. Parm Bains: Cela vous permet-il de mieux collaborer avec d'autres pays lors de campagnes de désinformation transnationales, de les surveiller avec nos alliés, etc.? Est-ce que cela vous donne plus de moyens pour le faire?

Surint. pr. Richard Baylin: Nous pouvons nous pencher sur plus d'aspects de la criminalité, parce que nous allons au-delà, comme je l'ai mentionné, de la menace tactique, de la menace criminelle, de ces éléments. Oui, ce sont des discussions que nous avons actuellement avec nos forces de l'ordre et les communautés ayant des vues similaires aux nôtres.

L'« écosystème » de la cybersécurité auquel la GRC aime faire référence, tout comme nos partenaires, est composé de nombreux éléments. Bon nombre de ces éléments du côté criminel et du côté sécurité nationale se croisent. Il peut s'agir parfois des mêmes auteurs de menaces, des mêmes écosystèmes et infrastructures sur lesquels nous nous concentrons, mais nous examinons maintenant cela sous un angle différent, sous l'angle de la sécurité nationale, et cela nous est également utile.

M. Parm Bains: En ce qui concerne les auteurs de menaces, avez-vous cerné des plateformes particulières? Nous avons vu à quel point X est devenu toxique. Surveillez-vous davantage les médias sociaux? Je sais que vous avez dit que vous ne les patrouillez

pas, mais avez-vous remarqué une augmentation des menaces dans certains espaces, comme le Web clandestin et d'autres espaces, auxquels les gens ont accès? De plus, quelles mesures avez-vous prises pour les inclure dans vos processus?

• (1630)

Surint. pr. Richard Baylin: Nous avons certainement constaté, au cours des dernières années, une évolution à cet égard. La GRC, mais aussi les forces de l'ordre en général, en ont beaucoup parlé publiquement et, encore une fois, c'est l'un des nombreux éléments que nous surveillons.

Vous avez parlé du Web clandestin. Les criminels utilisent de nombreux outils différents, et les individus qui ne disposaient pas d'outils perfectionnés auparavant pour se livrer, par exemple, à des activités comme les rançongiciels et les menaces, etc., peuvent maintenant se les procurer facilement pour mener des activités criminelles.

Je ne sais pas si cela répond à votre question.

Le président: Merci, monsieur Baylin.

Merci, monsieur Bains.

[Français]

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

M. Denis Trudel: Merci.

Monsieur O'Hayon, nous allons reprendre notre discussion sur l'élection qui s'en vient, même si elle pourrait aussi bien être déclenchée dans six mois que dans deux semaines ou un mois.

Vous ne pouvez pas faire de commentaires sur les enquêtes en cours, mais de quoi avez-vous peur?

Vous dites que vous vous préparez depuis huit mois. Quelle est la chose la plus probable qui pourrait arriver pendant la campagne électorale? Qu'est-ce que des États comme l'Iran, la Chine et la Russie pourraient faire, concrètement?

M. Greg O'Hayon: La raison pour laquelle cela fait des mois que nous nous préparons, c'est qu'il y a une panoplie de menaces, qu'il s'agisse d'extrémisme violent, comme mon collègue l'a dit, ou d'ingérence étrangère.

M. Denis Trudel: Pouvez-vous donner un exemple concret?

M. Greg O'Hayon: C'est tout simplement parce que le volume d'information qu'il va falloir absorber et analyser, pour ensuite y réagir, va être plus grand qu'il ne l'a été lors des élections générales des 44^e et 43^e législatures.

Je ne suis pas vraiment en mesure de vous dire ce qui est le plus probable, mais, étant donné que nous sommes ici pour parler de désinformation et de mésinformation, je dirais qu'il va certainement y en avoir.

M. Denis Trudel: D'accord.

Qu'est-ce qu'on pourrait voir comme désinformation?

Quel serait l'avantage d'intervenir sur les réseaux sociaux, pour un pays comme la Chine? Serait-ce pour avantager les conservateurs, les libéraux, le NPD ou le Bloc québécois? Comment cela fonctionne-t-il?

M. Greg O'Hayon: La stratégie et les objectifs varient d'un pays à l'autre. Dans les documents qui ont été publiés dans le cadre de l'Enquête publique sur l'ingérence étrangère, on parle justement des divers buts stratégiques des pays comme la Chine, la Russie, l'Iran, le Pakistan et l'Inde.

Il faut se mettre dans la peau de l'adversaire et se demander ce qu'il recherche. Par exemple, dans les résumés qui ont été publiés pour cette enquête, on dit que le but de la Russie est de fomenter des troubles, de semer le désarroi et de susciter la polarisation sociale. Le but de la Chine, par exemple, est bien différent.

M. Denis Trudel: Merci.

Le président: Merci, monsieur O'Hayon et monsieur Trudel.

[Traduction]

Monsieur Green, vous avez deux minutes et demie. Allez-y, je vous prie.

M. Matthew Green: Merci beaucoup.

J'aimerais revenir en arrière afin de mieux comprendre comment la GRC s'est préparée en vue de cette réunion, sachant que nous parlons d'ingérence étrangère.

Nous venons d'avoir, je pense, des révélations majeures au sujet du CPSNR. Je me demande si, en prévision de cette réunion, l'un ou l'autre des témoins a eu l'occasion de réfléchir à des comparateurs mondiaux, à d'autres services de police nationaux semblables à la GRC qui pourraient également être confrontés à des situations de ce genre.

Surint. pr. Denis Beaudoin: Monsieur le président, la question est-elle de savoir comment nous nous sommes préparés pour le Comité?

M. Matthew Green: La question est la suivante: dans votre préparation pour le Comité, pour ce travail et cette étude, avez-vous examiné les pratiques exemplaires d'autres pays?

Surint. pr. Denis Beaudoin: Oui, nous le faisons toujours, et pas seulement pour ce comité, monsieur le président. Nous faisons partie du Groupe des cinq.

M. Matthew Green: Pouvez-vous, s'il vous plaît, donner des exemples venant d'autres administrations que vous incluriez à titre de recommandations pour cette étude?

• (1635)

Surint. pr. Denis Beaudoin: Je ne connais pas l'étude, mais nous mettons en œuvre diverses pratiques exemplaires. À titre d'exemple, par rapport à l'ingérence étrangère, nous cherchons actuellement à briser les cloisonnements entre les corps policiers. Lorsque je parle de « cloisonnements », il s'agit essentiellement de faire de la sensibilisation à la répression transnationale, car il est possible que les policiers patrouilleurs ne se rendent pas compte qu'ils ont affaire à ce crime et qu'ils considèrent simplement cela comme une menace. Par exemple, nous essayons d'utiliser certains comités existants pour diffuser cette information, y compris le projet de loi C-70, à l'ensemble de nos collègues au Canada. C'est un exemple de partage d'informations.

M. Matthew Green: Selon vous, quelles sont les leçons à retenir du rapport du CPSNR?

Le président: Je suis désolé de vous interrompre, monsieur Green. J'ai arrêté votre chronomètre; je veux m'assurer que nos témoins comprennent bien la question et ce que vous cherchez à sa-

voir. Je pense qu'il est important, pour cette étude, d'obtenir une réponse. Voulez-vous reformuler votre question?

J'ai arrêté le chronomètre pour vous en donner l'occasion.

M. Matthew Green: Merci.

Étant donné le temps limité dont nous disposons, je demanderais aux témoins de la GRC de fournir au Comité, par écrit, l'ensemble des notes qu'ils ont prises ou des documents d'information qu'ils ont reçus et qui traitent d'exemples d'autres administrations confrontées à cet enjeu.

Ils ont indiqué être constamment à la recherche de pratiques exemplaires. J'aimerais vraiment que les témoins qui sont ici aujourd'hui formulent des recommandations aux fins de notre étude. Je ne suis pas certain d'avoir entendu des recommandations jusqu'à maintenant. Je veux simplement leur donner l'occasion de nous transmettre leurs recommandations par écrit, en fonction de pratiques exemplaires d'organismes d'application de la loi d'autres pays.

Le président: Plusieurs personnes au bout de la table me semblent acquiescer de la tête. Je pense qu'ils comprennent ce que vous demandez.

Je demanderai, par l'intermédiaire de la greffière, que l'on fasse un suivi auprès des responsables des affaires parlementaires de la GRC pour nous assurer d'obtenir réponse à cette question.

Monsieur Beaudoin, aviez-vous quelque chose à ajouter?

Surint. pr. Denis Beaudoin: Non. Je voulais simplement m'excuser si ma réponse n'est pas à la hauteur de vos attentes. Ce n'est certainement pas notre intention.

Le président: Très bien.

Surint. pr. Denis Beaudoin: Nous serons ravis de fournir une réponse écrite lorsque nous aurons une question claire et que nous aurons bien compris l'impact...

Le président: C'est exactement pourquoi je tenais à avoir cette discussion, afin que tout le monde sache clairement ce qui était demandé.

Monsieur Green, il vous reste 40 secondes. Avez-vous terminé?

M. Matthew Green: Ça va. Cela me satisfait.

Je vous remercie de votre intervention, monsieur le président.

Le président: Je suis désolé. Ce n'est pas dans mes habitudes, mais je tenais à m'assurer que nous obtenions ces informations. Merci.

Nous passons maintenant à M. Caputo, suivi de Mme Shanahan.

Allez-y, monsieur Caputo. Vous avez cinq minutes.

M. Frank Caputo (Kamloops—Thompson—Cariboo, PCC): Merci, monsieur le président.

Surintendant principal Baylin, surintendant principal Beaudoin et directeur général O'Hayon, je vous remercie.

J'aimerais reprendre là où mon collègue, M. Barrett, s'est arrêté. Il a parlé des ressources appropriées. La vérificatrice générale a publié un rapport en juin dernier. Je ne sais pas si vous l'avez lu ou si vous le connaissez.

Surintendant principal Baylin, je vois que vous acquiescez de la tête.

Surint. pr. Richard Baylin: Je pense que nous parlons du même rapport, mais je vais attendre que vous poursuiviez la question.

M. Frank Caputo: Ce rapport de juin est assez important. Il traite de la GRC et des ressources. On y traite des ressources en général, et mon collègue, M. Barrett, a posé une question à ce sujet.

J'aimerais vous citer un extrait de ce rapport, monsieur. On lit ce qui suit:

Dans l'ensemble, la Gendarmerie royale du Canada [...], le Centre de la sécurité des télécommunications Canada et le Conseil de la radiodiffusion et des télécommunications canadiennes [...] n'avaient ni la capacité ni les outils requis pour appliquer efficacement les lois visant à protéger la population canadienne contre les cyberattaques ou pour s'attaquer à la quantité croissante de cybercrimes, qui deviennent de plus en plus sophistiqués..

Il s'agit d'une citation directe, je crois, du rapport de la vérificatrice générale. Que répondez-vous à cela?

Surint. pr. Richard Baylin: Je vous remercie de la question, monsieur le président.

Ce que je répondrais, c'est que la leçon que nous retenons de ce rapport, c'est que l'évolution de la cybercriminalité nous a obligés à concentrer nos efforts à un niveau supérieur. Plus tôt, j'ai employé le mot « écosystème ». Nous faisons évoluer nos techniques. Nous faisons évoluer nos outils.

J'ai également mentionné que je suis toujours prêt à discuter des ressources et des façons de mieux aborder et traiter les questions de cybercriminalité. Cependant, j'ai aussi dit, plus tôt, vous vous en souviendrez, que le rapport de la vérificatrice générale remonte sur un certain nombre d'années. Considérant notre approche initiale à l'égard de la cybercriminalité, des crimes facilités par l'informatique et des fraudes, notamment, et considérant l'évolution de cette approche, il faut poursuivre ce travail, mais en s'éloignant d'une approche réactive aux incidents de cybercriminalité pour intervenir à un autre niveau afin de démanteler un système qui facilite la cybercriminalité.

Nous recentrons une bonne partie de nos efforts à cet égard pour veiller à régler le problème comme il se doit.

● (1640)

M. Frank Caputo: J'en suis conscient, monsieur. En tant qu'ancien procureur qui s'est occupé de poursuites dans de nombreuses affaires de cybercriminalité, je pense, étant donné les propos de la vérificatrice générale et connaissant la lenteur de l'appareil gouvernemental et le temps que prennent les choses, que la vérificatrice générale a très clairement indiqué que les ressources posent problème. Les ressources sont un problème. Dans ce cas-ci, la vérificatrice générale souligne un cas précis lié au CRTC qui, pour éviter de faire l'objet d'un mandat, a essentiellement effacé ou détruit un appareil, je crois.

Quoi qu'il en soit, je vais passer aux surintendants de la GRC.

Pouvez-vous confirmer qu'il n'y a aucun poste de police de la RPC en activité actuellement au Canada?

Surint. pr. Denis Beaudoin: Encore une fois, je ne ferai aucun commentaire sur l'enquête en cours. Il a été dit clairement que cela fait actuellement l'objet d'enquêtes, alors je ne ferai pas d'autres commentaires.

M. Frank Caputo: En tout respect, je crois que lorsqu'il était ministre de la Sécurité publique, M. Mendicino a commenté publiquement cette affaire en 2023, en disant que les postes de police avaient été fermés. Je pense que c'est une question qui préoccupe

beaucoup les Canadiens, en particulier les groupes qui sont ciblés. Franchement, je suis un peu surpris qu'on ne puisse pas nous dire, au Parlement, s'il y a des postes de police ou non. Je comprends que des enquêtes sont en cours ou qu'il pourrait y avoir des enquêtes. J'ignore si c'est le cas. Pourquoi ne peut-on pas simplement avoir un oui ou un non, nous dire si ces choses sont en activité ou non? En quoi cela compromet-il une enquête?

Surint. pr. Denis Beaudoin: Une enquête est en cours. Quant à la possibilité d'une enquête, comme vous l'avez dit, je pense qu'il a été confirmé qu'une enquête est en cours. Encore une fois, je ne ferai pas d'autres commentaires à ce sujet.

M. Frank Caputo: D'après ce que je comprends, la GRC a dit qu'elle a fermé ces postes de police en 2023. Si la situation a changé en 2024, je pense qu'à titre de parlementaires, dans le cadre de notre étude sur l'ingérence étrangère, nous devrions savoir si cela a changé ou non. Avez-vous un commentaire à ce sujet?

Surint. pr. Denis Beaudoin: Je n'ai pas de commentaires, monsieur le président.

Le président: Merci, monsieur Caputo.

Madame Shanahan, vous avez la parole pour cinq minutes.

[Français]

Mme Brenda Shanahan (Châteauguay—Lacolle, Lib.): Merci beaucoup, monsieur le président.

Je remercie les témoins qui sont avec nous aujourd'hui.

Dans ma circonscription de Châteauguay—Lacolle, qui sera bientôt appelée Châteauguay—Les Jardins-de-Napierville, les réseaux sociaux, Facebook et d'autres groupes, sont très populaires. Tout le monde les utilise.

Notre étude porte sur la mésinformation et la désinformation. La définition de ces deux termes peut porter à confusion.

Monsieur Beaudoin, pourriez-vous nous donner, dans vos propres mots, une définition de chacun de ces termes?

Surint. pr. Denis Beaudoin: La mésinformation, c'est de l'information erronée.

La désinformation, c'est de l'information erronée, mais il y a une intention sous-jacente.

Mme Brenda Shanahan: La mésinformation, c'est donc comme un malentendu, alors que la désinformation se distingue par le fait qu'il y a une intention qui se cache derrière une information.

Peut-il arriver qu'il y ait une mauvaise intention rattachée à la mésinformation? Autrement dit, on pourrait penser qu'une mésinformation est involontaire alors qu'en réalité, elle ne l'est pas.

Surint. pr. Denis Beaudoin: Oui, c'est possible.

On dirait que chaque personne a une définition différente de ces termes. Ces termes ne se trouvent pas dans le Code criminel, et la désinformation et la mésinformation ne sont pas des infractions criminelles à proprement parler. La définition que chacun leur donne peut donc être différente.

● (1645)

Mme Brenda Shanahan: J'aimerais que ce problème soit soulevé dans notre rapport. Les gens ne sont pas bien informés. Même nous, qui travaillons dans le domaine public, nous avons du mal à bien cerner le sens de ces deux termes. Des acteurs malveillants peuvent donc nous jouer des tours.

Monsieur Beaudoin, la sensibilisation, c'est très important non seulement pour le public en général, mais aussi pour des entreprises privées et dans tous les secteurs d'activité. Cela a aussi de l'importance pour les communautés vulnérables. Je pense aux communautés ethniques et aux communautés qui sont susceptibles d'être visées par de la désinformation mal intentionnée.

Pouvez-vous nous donner des exemples de programmes de sensibilisation que la GRC met en place?

Surint. pr. Denis Beaudoin: Prenons le cas d'activités de désinformation visant des communautés ethniques. Comme je l'ai mentionné, de telles activités qui seraient entreprises avant une élection ou pendant un processus électoral pourraient être considérées comme criminelles.

Nous avons rendu publics certains de nos engagements auprès des communautés. Nous essayons de les sensibiliser et de leur montrer l'ouverture dont font preuve les services de police canadiens. À l'étranger, il arrive que les policiers soient mal vus ou moins bien vus au sein de la population.

Nous essayons de briser un peu la culture de cloisonnement au sein des communautés. Nous essayons aussi de les informer au sujet des nouvelles lois et de la criminalité. Elles peuvent être victimes de telles activités. Nous cherchons aussi à informer les communautés au sujet du projet de loi C-70.

Mme Brenda Shanahan: Comment faites-vous cela? Offrez-vous des ateliers? Allez-vous rencontrer les gens dans les centres communautaires?

Dans le cas de l'industrie, rencontrez-vous des représentants de chambres de commerce?

Surint. pr. Denis Beaudoin: Vous avez bien répondu à ces questions à ma place. Tout ce que vous avez dit est pertinent.

Je peux vous donner quelques exemples. Nous nous sommes rendus à Montréal, au mois de mai ou juin dernier, pour sensibiliser des communautés établies dans cette ville.

Nous faisons aussi des présentations auprès des corps policiers partout au Canada pour les sensibiliser à l'ingérence étrangère.

Les gouvernements étrangers engagent parfois des firmes de sécurité privées. Nous avons donc fait plusieurs présentations auprès de ces firmes pour qu'elles soient vigilantes et qu'elles sachent reconnaître les signes d'ingérence, y compris ce qui se fait par le truchement des réseaux sociaux.

Nous essayons de toucher un vaste public. C'est sûr que nous n'avons pas les ressources nécessaires pour faire tout ce que nous voudrions faire pour les communautés. Nous essayons de cibler certains groupes pour avoir le plus d'impact possible. Nous faisons des présentations en personne dans certaines communautés.

Nous collaborons actuellement avec la GRC, Sécurité publique Canada et d'autres organismes pour faire sept ou huit présentations auprès de certaines communautés dans de grandes villes canadiennes. Nous essayons de nous rendre un peu partout afin d'atteindre le plus de Canadiens possible.

Le président: Merci, madame Shanahan et monsieur Beaudoin.

[Traduction]

J'ai une question liée à celle de Mme Shanahan. Vous avez parlé de désinformation et de mésinformation, et nous avons entendu diverses définitions de ces termes durant notre étude. Je suis un peu

de la vieille école. Je me souviens de l'époque où cela s'appelait un mensonge, pour parler franchement. Vous avez mentionné le Code criminel, le fait qu'il n'y a pas de distinction ou que ces termes ne se trouvent pas dans le Code criminel.

Dans le Code criminel, quel est l'équivalent auquel les services de police pourraient avoir recours pour les cas de propagation de mensonges, etc.? Est-ce que cela serait considéré comme un méfait en vertu du Code criminel? Que feriez-vous pour faire appliquer cela?

Surint. pr. Denis Beaudoin: Je ne suis pas certain que la désinformation soit une infraction criminelle en soi, monsieur le président.

Le président: Cela pourrait être un désaccord ou d'une divergence d'opinions. Ce sont les définitions que vous avez données plus tôt et que nous avons entendues lors de témoignages précédents.

● (1650)

Surint. pr. Denis Beaudoin: Exactement. La plus grande différence, avec le projet de loi C-70, c'est que cela peut devenir une infraction criminelle s'il s'agit d'une campagne de désinformation visant à influencer les processus gouvernementaux. Vous ne trouverez pas ces termes dans la Loi sur la protection de l'information; ils n'y sont pas définis.

Comme le député l'a laissé entendre, il revient au Comité de déterminer s'il est utile de définir, ces termes, mais il faut savoir que les corps policiers traitent des cas de harcèlement, d'intimidation et de menaces. Quant à la désinformation, si quelqu'un fait de la désinformation et finit par franchir le pas et que cela représente une menace, nous enquêtons alors sur la menace, mais pas nécessairement sur le « mensonge », comme vous l'avez appelé, car dans bien des cas, ce n'est pas nécessairement un crime.

Le président: Je tiens à tous vous remercier d'être venus aujourd'hui pour nous fournir de précieux renseignements.

M. Green a fait une demande. Je veillerai donc à ce que la greffière fasse un suivi auprès des responsables des affaires parlementaires. J'essaie habituellement de fixer un délai pour les réponses. Je vous demanderais donc, si possible, de faire parvenir votre réponse au Comité dans une semaine, disons à 17 heures. Je suis conscient que c'est la fin de semaine de l'Action de grâces, mais cela laisse amplement de temps pour répondre aux questions de M. Green.

Messieurs, merci de votre présence aujourd'hui.

Je vais suspendre la séance pour quelques minutes, le temps de nous préparer à accueillir le prochain groupe de témoins.

La séance est suspendue.

● (1650)

(Pause)

● (1659)

Le président: Je vous remercie de votre patience pendant que nous passons au deuxième groupe de témoins.

J'aimerais souhaiter la bienvenue à nos témoins pour la deuxième heure de la séance d'aujourd'hui.

Nous accueillons Mme Heidi Tworek, professeure d'histoire et de politiques publiques à l'Université de la Colombie-Britannique. Elle témoigne à titre personnel. Bienvenue, madame Tworek.

De CIVIX — que je connais bien en raison de certains programmes locaux à Barrie, comme d'autres députés, j'en suis sûr —, nous accueillons M. Kenneth Boyd, qui est directeur de l'éducation.

En personne, de l'Alliance démocratique des Canadiens russes, nous avons Mme Maria Kartasheva, la directrice, et M. Guillaume Sirois, qui est avocat.

Nous allons commencer par vous, madame Tworek. Vous avez cinq minutes pour votre déclaration préliminaire.

Allez-y, s'il vous plaît. Merci.

Mme Heidi Tworek (professeure, Histoire et politiques publiques, University of British Columbia, à titre personnel): Je vous remercie, monsieur le président, mesdames et messieurs les députés, de m'avoir invité à discuter de ce sujet important.

Je suis professeure d'histoire et de politique publique à l'université de la Colombie-Britannique, où je dirige le Centre d'étude des institutions démocratiques. Notre objectif est de comprendre le passé, d'analyser le présent et de préparer l'avenir. Je ferai donc trois remarques aujourd'hui: une sur le passé, une sur le présent et une sur l'avenir.

Tout d'abord, le passé. La désinformation et la mésinformation sont une caractéristique, et non une erreur, du système international. Il en va de même pour l'ingérence étrangère dans les élections. Les États-Unis ont craint l'ingérence de la France dès 1796. Au cours de la seconde moitié du XX^e siècle, les deux superpuissances de la guerre froide, les États-Unis et l'Union soviétique, sont intervenues dans environ 11 % de l'ensemble des élections nationales dans le monde.

La question n'est pas de savoir si l'ingérence étrangère se produira, mais plutôt pourquoi certains États s'engagent dans cette pratique à des moments particuliers.

Une partie de mes recherches a porté sur les raisons pour lesquelles les Allemands ont essayé d'utiliser la nouvelle technologie de la radio pour influencer la politique mondiale entre 1900 et 1945. Les Allemands voulaient interférer dans les environnements d'information étrangers parce qu'ils se sentaient coincés politiquement et économiquement. La perte de la Première Guerre mondiale a accéléré ce sentiment. Cela ne s'est évidemment pas bien terminé. Les nazis se sont appuyés sur des décennies d'expérimentation pour diffuser des contenus racistes et antisémites, ce qui a débouché sur une guerre mondiale des mots et des armes.

Sans entrer dans les détails historiques, cela montre que l'analyse des relations internationales permet de prévoir les campagnes de désinformation étrangères potentielles. Ce phénomène ne disparaîtra pas, mais ira en s'amplifiant et en diminuant. Nous avons donc besoin d'interventions systémiques pour renforcer la résilience par le biais d'initiatives éducatives, d'interventions au niveau des plateformes, de la transparence, de la recherche et d'autres mesures visant à renforcer la démocratie.

Deuxièmement, le présent. L'environnement actuel des médias sociaux et de l'IA a créé de nouvelles incitations économiques à la désinformation. Pour des raisons compréhensibles, les réunions de ces commissions sont axées sur la politique, mais l'argent alimente également le problème.

Nous devons renforcer l'application de la réglementation électorale sur les plateformes pour éviter ce genre de situation pendant les élections. Le Canada pourrait également se coordonner avec

d'autres démocraties confrontées au même problème. Par exemple, un groupe de travail intergouvernemental pourrait se concentrer sur des questions telles que la démonétisation de la désinformation. Il pourrait s'inspirer d'autres institutions multilatérales telles que le Groupe d'action financière sur le blanchiment de capitaux.

De manière plus générale, le Canada a beaucoup à apprendre d'autres pays, comme la Finlande en matière d'éducation aux médias ou Taiwan en matière de transparence et de lutte contre la désinformation tout en préservant la liberté d'expression.

L'IA générative est évidemment au cœur des préoccupations de la plupart des gens. J'ai récemment co-rédigé un rapport publié par CSDI sur le rôle de l'IA générative dans les élections à travers le monde en 2024. Nous avons constaté que l'IA générique est actuellement omniprésente, mais pas nécessairement persuasive, et qu'elle crée encore des problèmes. Nous constatons que l'IA générique menace les processus démocratiques tels que les élections de trois manières principales.

Premièrement, il permet la tromperie en abaissant la barrière à l'entrée pour la création de contenus problématiques. Cela accélère les problèmes qui existaient déjà sur les plateformes de médias sociaux.

Deuxièmement, l'IA générique pollue l'environnement informationnel en détériorant la qualité des informations disponibles en ligne.

Troisièmement, l'IA générique intensifie le harcèlement. Il est beaucoup plus facile de créer des cas d'hypertrucage qui peuvent être utilisés pour harceler les candidates politiques en particulier. Nous devrions nous inquiéter de cette amplification du harcèlement en ligne des candidates politiques, que j'étudie au Canada depuis 2019. Cela pourrait cibler des individus spécifiques ou des groupes sous-représentés pour les forcer à quitter la politique.

À ce jour, rien ne prouve que l'utilisation bénéfique de l'IA générique dans les élections l'emportera sur ses effets néfastes. De multiples mesures sont nécessaires pour relever les défis de l'IA générique. Bien qu'elle ne soit pas spécifique aux élections, la Loi de la Colombie-Britannique sur la protection des images intimes offre par exemple une possibilité de protéger les candidates politiques contre les cas d'hypertrucage. Nous devrions envisager l'adoption d'un projet de loi similaire pour relever les autres défis posés par l'IA générique.

En résumé, le passé nous enseigne que la désinformation ne va nulle part, mais que nous avons le pouvoir de l'atténuer. Le présent nous dit qu'il faut aussi s'attaquer aux incitations économiques. L'avenir nous met en garde contre les problèmes liés à l'intelligence artificielle, tels que les cas d'hypertrucage, avant qu'ils ne deviennent incontrôlables.

Je vous remercie.

• (1700)

Le président: Merci, madame la professeure. Vous n'avez pas dépassé votre temps de parole. Nous vous en sommes reconnaissants.

Monsieur Boyd, vous avez la parole pour cinq minutes. Allez-y, s'il vous plaît.

M. Kenneth Boyd (directeur de l'éducation, CIVIX): Bonjour, mesdames et messieurs les membres du Comité.

Mon nom est Kenneth Boyd. Je suis directeur de l'éducation à CIVIX, une organisation caritative nationale non partisane qui se consacre au développement des compétences et des habitudes d'une citoyenneté active et informée. Nous travaillons principalement avec des enseignants de la maternelle à la douzième année de chaque province et territoire en offrant des programmes gratuits en anglais et en français sur les thèmes de l'engagement démocratique, du discours civique et de la maîtrise des médias numériques.

Les membres du Comité connaissent peut-être mieux notre programme de vote des étudiants, qui est notre programme d'élections parallèles pour les étudiants n'ayant pas atteint l'âge de voter, ainsi que notre programme de journée des représentants, qui invite les députés et d'autres représentants élus dans les salles de classe pour dialoguer directement avec les étudiants.

Nous considérons la sensibilisation aux médias numériques comme une composante nécessaire d'une citoyenneté éclairée. S'engager dans le processus démocratique exige que les citoyens soient capables d'identifier des sources d'information fiables et dignes de confiance et qu'ils aient les compétences nécessaires pour faire la différence entre les faits et la fiction.

Nous savons que les effets de la désinformation en ligne peuvent nuire à la citoyenneté engagée d'une manière qui va au-delà du simple fait d'être induit en erreur. Par exemple, dans une enquête récente que nous avons menée auprès de 800 enseignants dans l'ensemble du Canada, nous avons constaté que 81 % des répondants ont déclaré qu'ils pensaient que la désinformation sur les médias sociaux contribuait « dans une large mesure » à la propagation de la rhétorique haineuse dans leurs écoles.

Le manque de capacité à s'engager de manière critique dans le contenu en ligne a donc des conséquences en aval sur la capacité des gens à avoir des conversations constructives et significatives sur des questions importantes.

Pour résoudre ces problèmes, nous avons créé CTRL-F, notre programme d'éducation aux médias numériques qui enseigne des techniques de vérification empiriques qui ont prouvé qu'elles augmentaient la capacité des gens à déterminer la véracité des affirmations et à identifier les motivations des sources non familières en ligne.

Depuis 2019, CTRL-F a été utilisé par plus de 5 200 enseignants qui ont enseigné le programme à plus de 300 000 élèves dans l'ensemble du Canada. Nous mettons constamment à jour notre programme pour répondre aux nouveaux types de fausses informations et de désinformation en ligne, y compris celles produites par l'intelligence artificielle, et nous adaptons actuellement nos ressources pour qu'elles puissent être utilisées par des apprenants adultes.

Si la maîtrise des médias numériques est nécessaire pour tous, il est particulièrement important que les élèves acquièrent ces compétences dès leur plus jeune âge. Toutefois, l'enseignement d'une bonne maîtrise des médias numériques aux Canadiens se heurte à un certain nombre de difficultés. Même si nous reconnaissons que l'éducation est une question provinciale, il convient de souligner les problèmes que nous avons constatés dans notre travail dans les écoles et avec les enseignants, car ils sont révélateurs des problèmes auxquels tous les Canadiens sont confrontés.

Tout d'abord, nos recherches ont montré que les ressources mises à la disposition des éducateurs canadiens varient considérablement en matière de qualité. Les provinces peuvent mentionner les res-

sources éducatives, mais pas en imposer l'utilisation, et de nombreuses ressources obsolètes sont encore utilisées dans les salles de classe et par les Canadiens dans tout le pays. Dans certains cas, ces ressources ont été développées avant l'adoption généralisée d'Internet, et il a même été démontré que certaines d'entre elles ont un effet inverse à celui escompté, en rendant les gens moins confiants dans les sources crédibles.

La sensibilisation aux médias numériques n'est pas non plus une chose unique. Il s'agit d'un terme générique qui englobe de nombreux concepts et compétences différents. Cependant, les éducateurs et les Canadiens en général ne disposent que de peu d'indications sur les ressources disponibles, sur celles qui sont de grande qualité et sur celles qui sont fondées sur des données probantes.

Deuxièmement, il y a une pénurie générale de formation à l'éducation aux médias numériques. Par exemple, il est fréquent de trouver des éducateurs chargés de l'enseignement de l'éducation aux médias numériques qui n'ont pas de formation spécifique dans ce domaine ou qui ont reçu leur dernière formation lorsqu'ils étudiaient pour devenir enseignants. Même pour ceux qui choisissent de s'informer sur les derniers développements en matière d'éducation aux médias numériques, le monde en ligne bouge et change si rapidement qu'il est difficile de suivre.

En réponse à ces questions, nous pensons qu'il est nécessaire de mettre en place une stratégie nationale pour faciliter la formation à l'éducation aux médias numériques. Notre travail nous a permis de constater qu'en matière d'évolutivité, il est plus efficace de former les éducateurs, ainsi que les organisations de la société civile et les leaders communautaires, afin d'atteindre le plus grand nombre de Canadiens possible.

Nous encourageons également le Comité à envisager d'aborder les problèmes de désinformation comme un problème de compétences généralisé plutôt que comme un simple problème de sensibilisation. Se contenter de sensibiliser les gens à la nécessité d'avoir un regard critique sur les contenus qu'ils trouvent en ligne ne nous aidera pas à progresser. Les Canadiens doivent avoir accès à des compétences en matière d'éducation aux médias numériques et être formés à ces compétences, ce qui nécessite un investissement soutenu de la part du gouvernement fédéral pour garantir la disponibilité de ressources de haute qualité et la poursuite de l'efficacité des programmes.

Enfin, une citoyenneté informée exige l'accès à des informations de qualité. Dans nos ressources, nous disons que l'environnement de l'information en ligne est pollué. Il est certainement possible de trouver des informations fiables, mais la désinformation et les fausses informations y sont mélangées. La désinformation a également tendance à être gratuite et facilement accessible. En effet, il est dans l'intérêt des fournisseurs de ces informations qu'elles soient aussi facilement accessibles que possible, de sorte qu'il est réellement nécessaire de prendre des mesures pour limiter le degré de pollution de l'information en ligne. L'un des moyens de résoudre ce problème est de soutenir les journalistes, en particulier les journalistes locaux, qui sont en mesure de fournir des informations fiables et d'offrir aux Canadiens de meilleures options pour trouver des informations importantes en ligne.

Je me ferai un plaisir de répondre à vos questions, et je vous remercie pour votre temps.

• (1705)

Le président: Nous vous remercions, monsieur Boyd.

Nous passons maintenant aux représentants de l'Alliance démocratique des Canadiens russes.

Vous avez jusqu'à cinq minutes pour vous adresser au Comité. Vous pouvez y aller, je vous prie.

Mme Maria Kartasheva (directrice, Alliance démocratique des Canadiens russes): Chers membres du Comité. Je suis Maria Kartasheva, directrice de l'Alliance démocratique des Canadiens russes. Je suis accompagnée de notre avocat, Guillaume Sirois.

Je vous remercie de votre invitation et d'avoir abordé la question de la menace que la propagande russe et la guerre cognitive font peser sur la sécurité nationale.

L'Alliance démocratique des Canadiens russes est un organisme à but non lucratif dirigé par des bénévoles, créé à la suite de l'invasion criminelle à grande échelle de l'Ukraine par la Russie. Notre mission est de soutenir le développement de la communauté russo-canadienne autour des idéaux de la démocratie, des droits de l'homme et de l'État de droit. L'opposition à l'invasion de l'Ukraine et au régime de Poutine est au cœur de notre travail.

Je tiens tout d'abord à vous remercier d'avoir reconnu la menace sérieuse que les opérations d'information et d'influence russes font peser sur notre démocratie et notre société. La guerre cognitive vise à manipuler l'information et les perceptions pour influencer la pensée, déstabiliser les sociétés et atteindre des objectifs stratégiques sans confrontation militaire directe. La Russie emploie ces tactiques dans le cadre d'une stratégie plus large, se considérant en guerre contre l'Occident, y compris le Canada. Il est essentiel de comprendre ce contexte pour élaborer des réponses efficaces afin de préserver notre démocratie.

J'ai moi-même été une victime directe de cette guerre cognitive. La Russie m'a condamné à sept ans de prison pour avoir diffusé des informations véridiques sur le massacre de Bucha alors que j'étais à Ottawa. J'ai même été menacé d'expulsion du Canada en raison de mon activisme politique.

L'Alliance démocratique des Canadiens russes, une organisation que j'ai cofondée, a été qualifiée d'organisation « indésirable » par le régime de Poutine. Cette désignation met en danger tous nos partenaires et nos collaborateurs, y compris moi-même. L'un de nos directeurs s'est vu contraint de démissionner par crainte de persécution. Cette situation souligne la nécessité urgente de prendre des mesures décisives pour protéger non seulement nos institutions démocratiques, mais aussi les personnes qui travaillent activement à leur maintien.

Entretemps, malgré les campagnes de désinformation menées de longue date par la Russie au Canada, je n'ai pas encore vu d'individus tenus pour responsables ou confrontés aux conséquences de leurs actes. En dehors de déclarations publiques et de sanctions inefficaces, il semble que le Canada ne fasse pas grand-chose pour empêcher la Russie de prendre le dessus dans sa guerre cognitive contre les Canadiens.

Comme nous l'avons appris, notamment au cours des travaux du comité sur l'ingérence étrangère, la propagande russe a un impact sur le travail des parlementaires de quatre manières principales.

Premièrement, la désinformation russe influence la manière dont les Canadiens, et leurs représentants parlementaires, pensent et votent sur des questions essentielles, y compris le soutien à l'U-

kraine, l'OTAN et même des questions intérieures comme l'inflation.

Deuxièmement, la désinformation alimente la peur et l'hostilité, contribuant aux menaces et à la violence à l'encontre des députés, ce qui compromet leur capacité à exercer leurs fonctions en toute sécurité.

Troisièmement, la saturation de la désinformation contribue à l'apathie politique croissante de la population en général, ce qui affaiblit la participation démocratique.

Quatrièmement, ces campagnes de désinformation visent à déstabiliser les fondements mêmes de notre démocratie en semant le doute sur l'intégrité des élections et de nos processus démocratiques.

En réponse, le gouvernement du Canada doit prendre les cinq mesures suivantes:

Premièrement, évaluer chaque année l'ampleur de la désinformation russe et d'autres désinformateurs parrainés par l'État qui ciblent le Canada, et rendre compte des résultats au Parlement dans un souci de transparence et de responsabilité.

Deuxièmement, adopter une stratégie de lutte contre la propagande russe, en se concentrant sur la protection du travail des membres du Parlement et de la diaspora russe contre ces campagnes de désinformation.

Troisièmement, créer un organisme indépendant similaire au CRTC ou à Élections Canada pour surveiller, évaluer et réagir à la propagande étrangère, en veillant à ce que l'intégrité des processus démocratiques soit préservée.

Quatrièmement, s'engager avec la diaspora russe et les organisations de la société civile pour aider à identifier et à combattre la propagande russe.

Cinquièmement, appliquer une politique étrangère résolue qui mette un frein à la désinformation de la Russie, la diplomatie et les partenariats mondiaux garantissant la responsabilité des actions de la Russie au Canada.

Pour conclure, l'ingérence de la Russie dans les processus démocratiques du Canada, illustrée par les campagnes de désinformation en cours, représente une menace importante qui ne doit pas être ignorée. Depuis des décennies, la Russie mène des opérations destructrices, telles que l'opération Tenet Media, dans une relative impunité. En reconnaissant la gravité de cette menace et en nous engageant à prendre des mesures sérieuses, nous pouvons protéger notre démocratie pour les prochaines générations.

Je vous remercie de votre attention. Je me ferai un plaisir de répondre à toutes vos questions.

● (1710)

Le président: Je vous remercie.

Merci à tous nos témoins pour leurs déclarations préliminaires très intéressantes.

Nous allons procéder à des tours de six minutes pour chaque parti, et nous allons commencer par M. Barrett.

Monsieur Barrett, à vous la parole pour les six prochaines minutes.

M. Michael Barrett: Monsieur Boyd, j'ai eu l'occasion de m'engager avec votre organisation lors des journées des représentants et je sais comment je me suis comporté lors du vote local des étudiants. Je suis aussi satisfait de ce résultat que des résultats obtenus lors des élections générales et partielles. John Bosco à Brockville et St. Edward à Westport, qui m'ont invité à participer aux journées des représentants. Je pense que c'est un excellent programme. Il y a toujours d'excellentes questions qui démontrent la compréhension qu'ont ces étudiants grâce aux efforts de votre programme. C'est tout à fait louable.

Vous avez dit que l'éducation était une responsabilité provinciale. Je me demande si vous pourriez nous parler rapidement de votre financement. Quel est le montant du financement fédéral que vous avez reçu, et quel est le montant du financement provincial que votre organisation reçoit?

• (1715)

M. Kenneth Boyd: Je ne peux pas vous donner les pourcentages exacts de mémoire. Nous sommes un organisme de bienfaisance enregistré, alors toutes nos données sur le financement sont évidemment du domaine public. Je dirais que, pour nos programmes d'éducation aux médias numériques en particulier, nous recevons des fonds de diverses sources: gouvernement fédéral, Initiative de citoyenneté numérique, organismes et donateurs privés, centres de recherche et gouvernements provinciaux.

Pour ce qui est de ce programme, je dirais que nous avons surtout reçu du financement de Patrimoine canadien et de l'Initiative de citoyenneté numérique.

M. Michael Barrett: Je crois que vous avez élargi votre champ d'action à l'étranger en offrant des services en Colombie et au Chili. Comment ces initiatives sont-elles financées?

M. Kenneth Boyd: Elles sont financées par des subventions indépendantes qui ont été demandées par nos équipes en Colombie et au Chili. Ces dernières ont récemment reçu une subvention de l'Union européenne pour continuer à financer leurs projets. Elles se sont inspirées du travail que nous avons accompli au Canada, surtout en ce qui concerne les programmes d'éducation aux médias numériques, et l'ont adapté au public en Colombie et au Chili.

M. Michael Barrett: Vous montrez aux enfants comment s'y retrouver face à ce que vous avez appelé, je crois, la pollution numérique. Décidément, il y a beaucoup de pollution en ligne. Il est de plus en plus difficile de réfléchir de façon critique et de discerner ce qui est réel et ce qui ne l'est pas.

Quelle recommandation concrète pourriez-vous nous faire afin que nous en tenions compte dans ce rapport? Selon vous, qu'est-ce qui pourrait améliorer l'éducation aux médias numériques pour les enfants partout au Canada?

M. Kenneth Boyd: Je pense qu'il faut mener une enquête sur les types de ressources qui sont efficaces, fondées sur des données probantes, et qui peuvent être... Comme je l'ai déjà mentionné, nous sommes conscients que l'éducation relève davantage des provinces. Cependant, en ce qui concerne la possibilité de faire une recommandation, certains outils se sont révélés efficaces. Il faut comprendre de quoi il s'agit et les faire connaître, non seulement aux élèves, mais aussi aux Canadiens en général.

Il est possible d'apprendre des stratégies efficaces d'éducation aux médias numériques. À mon avis, ce serait quelque chose de concret que le Comité pourrait envisager.

M. Michael Barrett: Donnez-moi une idée de l'uniformité du matériel distribué partout au Canada dans le domaine des connaissances civiques et de l'éducation aux médias numériques. Existe-t-il une norme dans les provinces et les territoires? Si oui, quelle est-elle? Sinon, y a-t-il même une uniformité au sein de chaque province en ce qui concerne le matériel distribué dans les conseils scolaires?

M. Kenneth Boyd: En ce qui a trait aux différentes provinces, il est courant de trouver, dans les programmes d'études, des exigences quant à la façon d'enseigner l'éducation aux médias numériques ou l'évaluation des sources. Les provinces peuvent faire des recommandations ou dresser la liste des ressources possibles, mais elles ne rendent pas obligatoire l'utilisation d'une ressource en particulier. Autrement dit, il se peut que l'éducation aux médias numériques varie d'une province et d'un territoire à l'autre.

Il n'y a pas de mandat unifié et cohérent quant aux ressources à utiliser ou à ne pas utiliser.

M. Michael Barrett: Selon vous, quel est le moyen le plus important par lequel votre organisation protégera sa crédibilité à l'avenir? Quelles mesures sont en place, que ce soit pour la sélection des membres du conseil d'administration ou pour la sélection des sources de financement, pour veiller à ce que votre organisation, en tant qu'entité chargée de ces importantes initiatives pédagogiques, demeure crédible et irréfutable dans le milieu très nébuleux des fournisseurs d'information?

M. Kenneth Boyd: Je suis désolé; pourriez-vous reformuler la question au sujet de la crédibilité? J'ai manqué la première partie de cette question.

Le président: Il vous reste 10 secondes.

M. Michael Barrett: En fait, je me demandais simplement ce que vous faites pour protéger votre crédibilité, que ce soit en sélectionnant des personnes au sein de votre conseil d'administration ou en choisissant des sources de financement, en raison de la nature nébuleuse du milieu de l'information. Comment protégez-vous votre crédibilité en tant que source pédagogique?

• (1720)

Le président: J'aurai besoin d'une réponse très brève, monsieur Boyd.

M. Kenneth Boyd: Très rapidement, comme je l'ai mentionné, nous sommes un organisme de bienfaisance, alors nous sommes très transparents au sujet de toutes nos sources de financement. Je pense que c'est l'une des façons de maintenir notre crédibilité.

Le président: Je vous remercie.

[Français]

Madame Shanahan, vous avez la parole pour six minutes.

[Traduction]

Mme Brenda Shanahan: Merci beaucoup, monsieur le président.

Je tiens à remercier tous les témoins de leur présence, mais je veux surtout porter mon attention sur une nouvelle qui est sortie le mois dernier et que les témoins connaissent sûrement. Cela concerne l'affaire Tenet Media. Il y a un lien avec ma province, le Québec, car deux habitants de l'ouest de l'île de Montréal, soit Lauren Chen et une autre personne, ont été nommés dans une mise en accusation aux États-Unis. On allègue qu'ils ont diffusé de la désinformation. Il se peut qu'ils aient été, comme on le dit couramment, des « idiots utiles », mais il se peut aussi qu'ils aient agi en toute connaissance de cause. Je l'ignore, mais parlons de ce qui s'est passé là-bas.

Selon l'acte d'accusation américain:

Après l'invasion de l'Ukraine par la Russie en février 2022, RT a été sanctionnée, abandonnée par les distributeurs et finalement forcée de cesser ses activités officielles aux États-Unis, au Canada, au Royaume-Uni et dans l'Union européenne.

C'est là un très gros marché.

On peut lire ensuite:

En réaction, RT a créé, pour reprendre les mots de sa rédactrice en chef, un « véridable empire de projets secrets » conçu pour façonner l'opinion publique des « auditoires occidentaux ».

L'acte d'accusation poursuit en alléguant que Tenet Media est l'un des projets secrets de RT.

En quoi l'empire de projets secrets de RT nuit-il aux Canadiens d'origine ukrainienne? Je pose la question à Mme Kartasheva.

Mme Maria Kartasheva: Je crois qu'il serait préférable de poser cette question aux Canadiens d'origine ukrainienne, car je suis une représentante de la société russe au Canada, mais à mon avis, la propagande russe en général nuit à tout le monde. En ce qui concerne plus précisément les Ukrainiens au Canada, je me suis entretenue avec l'un des directeurs du Congrès des Ukrainiens Canadiens, qui m'a dit qu'après la guerre et à cause de la propagande russe, il y a eu une augmentation épouvantable des crimes haineux contre les Ukrainiens, qu'il s'agisse d'insultes ou simplement de quelques symboles à l'extérieur des universités ou dans la rue.

Nous savons qu'il y a maintenant beaucoup plus d'Ukrainiens au Canada, car lorsque la guerre a commencé, le Canada leur a ouvert ses portes. J'imagine que, pour eux, cela doit être très traumatisant de sortir de la guerre et de voir ces symboles haineux autour d'eux. Selon ce que je comprends, le Canada n'en fait pas assez pour les protéger ou même pour réagir à ces crimes.

Mme Brenda Shanahan: Je vous remercie beaucoup de cette réponse et, en fait, merci d'avoir élargi la question.

Je tiens à souligner que ma circonscription, Châteauguay—Lacolle, qui s'appellera bientôt Châteauguay—Les Jardins-de-Napierville, compte une magnifique région agricole. Elle s'étend jusqu'à la frontière américaine.

Nous avons un grand nombre de russophones d'origine mixte russo-ukrainienne. Même dans la petite ville de Châteauguay, qui compte 50 000 habitants, nous étions très fiers de pouvoir accueillir plus de 100 familles ukrainiennes qui ont été déplacées après l'invasion de l'Ukraine par la Russie. Tout le monde a mis l'épaulé à la roue, et c'était un merveilleux projet communautaire. En fait, le groupe a depuis été démantelé puisque les Ukrainiens se sont complètement intégrés; ils travaillent et subviennent à leurs besoins et à ceux de leur famille, mais les liens d'amitié perdureront. Cette expérience a beaucoup sensibilisé notre collectivité à cette désinfor-

mation, à cette mésinformation et au tort que cela peut causer. Quelle est la meilleure façon de riposter?

Mme Maria Kartasheva: Eh bien, c'est une question très importante, et je suppose que c'est la raison pour laquelle nous sommes tous réunis ici. Il doit y avoir une sorte d'organisme indépendant qui enquêtera sur ce genre de désinformation et qui formulera des recommandations sur la façon d'y réagir ou peut-être même, parfois, sur l'application de certaines solutions. Évidemment, c'est une question très complexe, et le problème ne concerne pas seulement, par exemple, des médias comme Russia Today. La stratégie de propagande russe est très complexe; elle comprend les médias sociaux, différents « experts » qui donnent des entrevues sur différents médias, y compris des médias conventionnels et respectés, ainsi que divers professeurs. C'est une question très complexe qui doit être traitée à tous ces niveaux, et c'est pourquoi j'ai proposé la création d'un organisme indépendant chargé de coordonner cette activité, parce que personne ne réglerait les problèmes si tout le monde s'y affairait. Il doit y avoir un organisme qui surveille tout cela.

• (1725)

Mme Brenda Shanahan: Je vous remercie de cette réponse.

Je tiens à vous remercier du travail que vous faites pour sensibiliser les Canadiens au fait qu'il y a effectivement des Russes ici au Canada qui se battent activement pour la démocratie, parfois même à leurs risques et périls. Je vous suis reconnaissante du travail que vous accomplissez. Connaissez-vous d'autres projets de la chaîne RT qui visent à influencer les auditoires occidentaux?

Mme Maria Kartasheva: Je ne connais pas RT à ce point-là parce que, personnellement, je trouve pénible de regarder son contenu et tout le reste. Je sais toutefois que ses stratégies sont très complexes et, comme je l'ai dit, cela se fait à plusieurs niveaux. Je suis au courant parce que, honnêtement, RT agit également de la sorte en Russie dans le but de répandre de la désinformation et de semer le doute chez les gens afin qu'ils se méfient non seulement les uns des autres, mais aussi du gouvernement ou de qui que ce soit d'autre, et donc...

Le président: Je vous remercie. Ce n'est pas grave, madame Kartasheva. Ça ira.

Je suis désolé, mais nous avons dépassé le temps imparti de près de 45 secondes.

[Français]

Monsieur Trudel, vous avez la parole pour six minutes.

M. Denis Trudel: Merci, monsieur le président.

Madame Tworek, la désinformation, l'intelligence artificielle, les médias sociaux et la façon de contrer la désinformation et la mésinformation sont des sujets qui soulèvent vraiment de grandes questions.

Un groupe de réflexion d'Emploi et Développement social Canada a publié, cette année, un rapport dans lequel on dresse la liste des 35 plus grandes perturbations mondiales qui nous guettent actuellement. Selon ce rapport, la désinformation est la plus grande menace que le monde doit affronter aujourd'hui.

Êtes-vous d'accord sur cela, madame Tworek?

[Traduction]

Mme Heidi Tworek: Je dirais que c'est à la base de nombreuses autres menaces. Qu'il s'agisse de questions liées à la guerre, aux changements climatiques, etc., nous constatons que la désinformation fait partie de tous ces problèmes, et c'est ainsi que j'ai tendance à voir les choses. Nous constatons également que les dérapages et le harcèlement sont un élément clé de la désinformation. Nous ne savons jamais exactement qui sera touché, en fonction de l'enjeu. Je vois cela comme un fondement sous-jacent, et c'est pourquoi je pense qu'il s'agit d'une menace existentielle.

[Français]

M. Denis Trudel: Quand on y pense, l'intelligence artificielle est un peu terrifiante. On peut maintenant reproduire mon visage et ma voix, et on peut me faire dire à peu près n'importe quoi sur les réseaux sociaux. C'est quand même terrible.

Comment peut-on s'attaquer à ce phénomène? Que pourrait-on mettre en place, sur le plan législatif, pour empêcher que, lors de la prochaine campagne électorale, une vidéo de moi en train de vanter le programme du Parti conservateur du Canada circule sur les médias sociaux, par exemple?

[Traduction]

Mme Heidi Tworek: Ce que nous disons dans notre rapport, c'est qu'il s'agit évidemment d'une question qui doit être abordée sous plusieurs angles. Il y a des entreprises qui réfléchissent elles-mêmes à des choses comme le tatouage numérique pour voir si quelque chose est généré par l'intelligence artificielle ou non. Il faut donc s'assurer de mettre en œuvre quelque chose de ce genre... Nous avons besoin de programmes comme l'éducation civique, non seulement pour les écoles, mais aussi pour les gens qui ne sont plus en âge d'aller à l'école, et nous devons également réfléchir à différents types de règlements. Ce rapport contient toute une série de recommandations, et je me ferai un plaisir de le transmettre au Comité afin que vous puissiez en prendre connaissance. Je pense toutefois qu'au bout du compte, il n'y a pas qu'une seule partie responsable. Nous avons besoin d'une série de mesures différentes pour contrer ce phénomène.

• (1730)

[Français]

M. Denis Trudel: Dans vos remarques préliminaires, justement, vous avez parlé du fait que l'intelligence artificielle avait été utilisée lors de campagnes électorales déclenchées dans d'autres pays.

Que s'est-il passé exactement, et comment a-t-on fait pour savoir qu'il s'agissait de contenu généré par l'intelligence artificielle, et non de vrais contenus politiques?

[Traduction]

Mme Heidi Tworek: Dans certains cas, par exemple, en Slovaquie, un hypertrucage audio avait été diffusé. La personne elle-même a évidemment affirmé qu'il s'agissait d'un hypertrucage. Nous avons également observé des cas similaires en Inde.

Il est toujours très difficile de déterminer si cela fait changer l'avis d'une personne ou non, mais nous soulignons dans le rapport ce genre d'exemples singuliers survenus dans divers pays pour montrer que ce type d'intelligence artificielle générative est à tout le moins utilisé.

Pour l'instant, nous ne trouvons pas beaucoup de preuves de son effet persuasif. C'est pourquoi je dis que nous devons anticiper le

problème avant qu'il ne devienne quelque chose que nous ne pouvons pas vraiment maîtriser.

[Français]

M. Denis Trudel: Dans les pays qui ont fait l'objet de vos études, l'attaque, ou la menace, venait-elle d'un pays étranger, ou venait-elle d'autres partis politiques du même pays?

[Traduction]

Mme Heidi Tworek: Malheureusement, c'est quelque chose que nous n'avons pas pu déterminer. Nous n'avons pas mené ce genre d'enquêtes.

Parfois, cela peut effectivement être très difficile. L'exemple de Tenet Media nous montre que, dans ce cas, il ne s'agissait pas de savoir qui créait le contenu, mais plutôt qui le finançait. C'est pourquoi j'ai recommandé de réfléchir au financement et d'examiner le contenu lui-même, car il peut y avoir, d'une certaine façon, des choses qui se produisent en dehors des plateformes et qui influent réellement sur le type de contenu créé.

Nous devons non seulement penser au contenu, mais aussi aux acteurs et à leurs comportements.

[Français]

M. Denis Trudel: Pensez-vous que certains partis politiques au Canada pratiquent la désinformation à des fins partisanes, en ce moment?

[Traduction]

Mme Heidi Tworek: C'est une question à laquelle il est très difficile de répondre.

À notre connaissance, les partis politiques vont évidemment militer en faveur de leur victoire, mais nous n'avons pas examiné précisément ce qu'ils font à l'interne. Il est évidemment très difficile pour nous de répondre à cette question.

[Français]

M. Denis Trudel: Merci.

Monsieur Boyd, j'aimerais vous poser la même question.

Pensez-vous que, au Canada, il y a des partis politiques qui ont pratiqué la désinformation à des fins partisanes dans le passé, qui le font en ce moment ou qui comptent le faire dans l'avenir?

[Traduction]

M. Kenneth Boyd: Je vais donner la même réponse que Mme Tworek, à savoir qu'il est très difficile de déterminer si les partis politiques eux-mêmes créent ce genre d'information à l'interne. Je n'ai certainement aucune idée des intentions pour l'avenir, alors je n'ai pas de bonne réponse à vous donner. Je suis désolé.

[Français]

M. Denis Trudel: D'accord, merci.

Le président: Merci, monsieur Trudel.

[Traduction]

Monsieur Green, vous avez six minutes.

M. Matthew Green: Pour ce tour, mes questions s'adresseront à Mme Tworek.

En 2023, une note d'information intitulée « Media/Digital Literacy in an Era of Disinformation », qui résume une présentation que vous avez faite en 2022, a été publiée dans le *Journal of Intelligence, Conflict, and Warfare*.

Au cours de cette présentation, vous avez évoqué le fait que la mésinformation et la désinformation se recourent souvent avec les dérapages en ligne — et vous y avez fait allusion tout à l'heure —, dérapages qui visent des groupes professionnels et des groupes marginalisés, notamment les femmes, comme vous l'avez mentionné, je crois. Vous avez dit que c'était le fondement.

Pourquoi en est-il ainsi, d'après vous?

Mme Heidi Tworek: Dans le cadre des études que nous avons menées depuis 2019, nous avons constaté que, souvent, ce genre d'attaques basées sur l'identité et ce type de harcèlement peuvent avoir des effets disproportionnés sur les personnes issues des communautés racisées, les personnes 2SLGBTQ+ ou les femmes. Cela peut souvent coïncider avec une sorte de désinformation au sujet de ces personnes.

La distinction ici, bien entendu, c'est qu'on peut avoir des discussions vigoureuses et rigoureuses sur des questions, mais force est de constater que ces groupes font souvent face à des attaques contre leur identité.

Cela a une influence sur les candidats politiques eux-mêmes et, j'ajouterais, sur leurs équipes de campagne. C'est vraiment important, parce que ce sont souvent des gens qui pensent à se lancer en politique et peut-être à devenir candidats. Ils voient le genre de dérapages et de harcèlement en ligne qui visent un candidat et ils se disent que la politique n'est peut-être pas pour eux.

Si nous voulons avoir une assemblée législative diversifiée qui représente la diversité des Canadiens, nous devons nous attaquer à ce problème.

• (1735)

M. Matthew Green: Il est intéressant que vous souleviez cette question. Je sais, par exemple, que ce point a été soulevé par l'une des anciennes membres du Comité, Mme Pam Damoff, qui a longuement parlé de la façon dont la violence politique s'exprime.

Selon vous, à quel moment ces campagnes vont-elles cesser d'être simplement de la mésinformation et de la désinformation et se transformer en violence politique ou, si j'ose dire, en une approche profasciste en vue du démantèlement de la démocratie dans le pays?

Mme Heidi Tworek: C'est évidemment une grande question dont les politicologues peuvent débattre. Je pense que j'irais dans une direction légèrement différente, en disant qu'il s'agit souvent de menaces réelles à l'endroit de la sécurité physique ou psychologique des gens. Il y a toutes sortes de façons d'aborder cela.

Un rapport que j'ai coécrit avec Chris Tenove en 2020 contient toute une série de recommandations sur la manière dont nous pouvons traiter ce genre de choses afin de continuer à avoir une démocratie et, espérons-le, à évoluer dans une démocratie qui dispose de candidats et de représentants politiques de divers horizons. Je serais heureux de soumettre ce rapport à votre comité.

M. Matthew Green: C'est bien, car ma question suivante porte sur les façons de réduire au minimum ce type de dérapage en ligne.

Les deux problèmes que vous avez cernés lors de cette présentation de 2022 étaient la faible présence du journalisme de type expli-

catif et le manque de connaissance au sujet des médias sociaux chez certains communicateurs professionnels qui essaient de publier de l'information de haute qualité en ligne. Pouvez-vous nous expliquer ces deux problèmes et nous dire s'il existe au Canada des initiatives pour renverser la vapeur?

Mme Heidi Tworek: En ce qui concerne la faible présence de journalisme de type explicatif, une autre façon de voir les choses serait la suivante: nous devons réfléchir à ce en quoi consiste le journalisme au XXI^e siècle, qui peut fournir cette information, etc. Il existe évidemment une foule d'initiatives.

Je n'en citerai qu'une, The Conversation Canada, qui a été cofondée par deux de mes collègues de l'Université de la Colombie-Britannique. L'idée est de jumeler des universitaires qui sont très mauvais pour rédiger des articles d'opinion avec des journalistes qui sont capables de corriger leurs textes. Nous développons ainsi un savoir-faire universitaire, sauf que les articles sont rédigés de manière à ce que la plupart des gens puissent les comprendre. Les articles résultants peuvent être republiés sans frais. Ce n'est qu'un exemple de la manière dont nous pouvons donner de l'importance au journalisme et faire en sorte qu'il émane d'experts.

En ce qui concerne l'expertise en matière de médias sociaux, il s'agit d'un domaine assez problématique à l'heure actuelle, car nous constatons que les plateformes de médias sociaux ont, même depuis 2022, de plus en plus réduit la capacité pour les chercheurs d'accéder aux données des plateformes, qu'il s'agisse de CrowdTangle de Meta ou de X, dont les coûts sont désormais prohibitifs. Il est donc de plus en plus difficile pour nous, chercheurs, d'accéder au type de données dont nous avons besoin pour répondre aux questions fondamentales que pose ce comité. C'est pourquoi des projets de loi comme le projet de loi C-63 intègrent certaines notions, comme celle d'une transparence pour les chercheurs.

M. Matthew Green: Vous parlez de la transparence à l'égard des algorithmes, de ce qu'il nous faudrait pour comprendre comment on sert l'information aux gens. Est-ce à cela que vous faites allusion?

Mme Heidi Tworek: Il s'agit en partie de cela, oui. Il s'agit aussi de questions concernant l'accès aux messages, car, sur de nombreuses plateformes de médias sociaux, le nombre de messages auxquels nous pouvons accéder est très limité. Par exemple, sur X — Twitter à l'époque —, en 2019, il y avait beaucoup de questions que nous pouvions poser dans le cadre de notre étude sur les candidats politiques. Or, ces questions, nous ne pouvons désormais plus les poser pour la bonne et simple raison que nous n'avons pas accès à ce niveau de données.

M. Matthew Green: Ce que je vois ici, c'est la marchandisation de l'information. Je sais que l'apprentissage automatique et l'intelligence artificielle sont capables de vérifier avec force précision l'humeur des gens sur une plateforme. Bien sûr, cela a été évoqué lors de l'élection de 2016, sous Trump, lorsqu'on a exposé comment Cambridge Analytica et d'autres avaient ciblé les gens.

Selon vous, comment pouvons-nous « démarchandiser » ce type de capitalisme de l'information afin de le rendre plus démocratique et transparent, comme vous l'avez évoqué?

Mme Heidi Tworek: C'est une excellente question. Je ne pense pas qu'il y ait de solution miracle, mais les chercheurs proposent divers moyens.

Certains considèrent le recours à une approche antitrust. D'autres proposent des mesures ciblant la confidentialité des données comme moyen d'empêcher les entreprises d'avoir accès à une telle quantité d'information. D'autres encore se demandent s'il y aurait lieu d'avoir une intelligence artificielle publique. C'est ce que Mozilla soutient, par exemple.

Je ne pense pas qu'il y ait de solution miracle, mais il y a toute une série de possibilités que nous pourrions explorer.

M. Matthew Green: D'accord. Merci beaucoup.

Le président: Merci, monsieur Green.

Voilà qui conclut notre premier tour de questions.

Nous avons suffisamment de temps pour une série de questions de cinq minutes pour les conservateurs, et la même chose pour les libéraux.

[Français]

Le temps de parole accordé à M. Trudel sera de deux minutes et demie.

[Traduction]

Nous aurons deux minutes et demie pour vous, monsieur Green, ce qui nous permettra de remplir le temps qu'il nous reste.

Je donne maintenant la parole à M. Caputo, pour cinq minutes.

Allez-y, monsieur.

M. Frank Caputo: Merci, monsieur le président.

J'aimerais remercier les témoins qui sont ici en personne, ainsi que ceux qui sont avec nous par vidéoconférence, c'est-à-dire M. Boyd et la professeure Tworek.

Je note, professeure, que vous venez de l'Université de la Colombie-Britannique. En tant que diplômé de l'Université Simon-Fraser, je m'en voudrais de ne pas faire une boutade amicale en soulignant la supériorité de mon alma mater.

• (1740)

Le président: Vous avez des comptes à régler, monsieur Caputo?

Un député: Oh, oh!

M. Frank Caputo: Plus sérieusement, l'une des choses qui m'ont vraiment dérangé au sujet de l'ingérence étrangère, en particulier lors des élections, c'est le temps qu'il faut au gouvernement pour agir. Autrement dit, les gens sur le terrain savent exactement ce qui se passe, mais il y a un délai important entre le moment où cette information parvient aux forces de sécurité du Canada et celui où des mesures sont prises.

L'un d'entre vous, monsieur Boyd ou madame Tworek, aurait-il quelque chose à dire à ce sujet?

Mme Heidi Tworek: Je dirai brièvement que l'une des choses que j'ai préconisées, c'est de réfléchir à la transparence et à la façon dont elle peut être assurée de manière appropriée.

Le président: Monsieur Boyd, avez-vous une réponse à nous donner?

M. Kenneth Boyd: Comme vous l'avez mentionné, il y a possiblement ou inévitablement, un certain temps de latence dans ce genre d'affaires, mais je pense que cela souligne la nécessité d'aborder ces problèmes sous de multiples angles. Quant à la possibilité pour les citoyens canadiens de contribuer au repérage des informa-

tions fausses ou trompeuses, j'estime que c'est une chose qui pourrait aider à combler le passage à vide qui existe dans l'attente d'une intervention par un quelconque organisme fédéral.

M. Frank Caputo: Poursuivons sur cette lancée.

Je suis désolé. M. Sirois a quelque chose à ajouter.

Merci.

M. Guillaume Sirois (avocat, Alliance démocratique des Canadiens russes): La propagande russe, en particulier, est un problème qui existe depuis très longtemps, depuis au moins une décennie, voire plus. La Commission sur l'ingérence étrangère nous a appris aujourd'hui que la stratégie visant à lutter contre cette ingérence étrangère n'en est qu'à ses balbutiements. Il s'agit d'un délai très long pour traiter un tel enjeu de sécurité nationale. Nous en avons vu les conséquences avec ce que Tenet Media a fait. Si nous avions eu une stratégie plus tôt — par exemple, après l'ingérence constatée en 2016 lors de l'élection présidentielle —, nous ne serions peut-être pas ici aujourd'hui à parler encore une fois d'ingérence étrangère.

M. Frank Caputo: Je suis tout à fait d'accord avec vous, monsieur Sirois. Si je dois être franc — et je crois que je dois l'être dans ces comités et au Parlement en général —, je dirais que j'ai constaté un manque de volonté politique à s'attaquer à ce problème de front. Franchement, c'est le gouvernement qui en est responsable. Je l'ai dit à presque toutes les réunions de comité que nous avons eues. Nous avons 11 personnes qui, selon nos forces de sécurité, ont travaillé volontairement ou semi volontairement avec des États étrangers hostiles.

Vous parlez de faire face à ce problème et de le faire rapidement. Je crois que le terme que vous avez utilisé est « balbutiements ». Il s'agit de choses que nous savons, que nos forces de sécurité savent, mais que nous, en tant que Canadiens, ignorons. Nous avons posé d'innombrables questions à nos services de sécurité, mais nous avons l'impression qu'on ne nous dit rien de nouveau.

N'est-ce pas tout à fait le contraire de l'approche que nous devrions adopter, à savoir qu'il faut faire la lumière, la faire briller intensément et tôt dans le processus?

M. Guillaume Sirois: Je pense que nous sommes tous les deux d'accord pour dire que la transparence est la clé pour répondre à la propagande étrangère, comme l'ingérence russe dont nous discutons aujourd'hui. La transparence permet d'amorcer une discussion sur la manière dont nous pouvons aborder ce problème. À moins de savoir ce que le gouvernement fait derrière des portes closes, nous ne saurions avoir une discussion appropriée sur ce qu'il devrait faire ou sur ce qu'il fait de travers.

M. Frank Caputo: Madame Kartasheva, vous avez mentionné au début quelque chose qui m'a interpellé, à savoir que la Russie vous a condamnée par contumace à sept ans de prison.

Voulez-vous en parler? Votre temps est venu de le faire. Vous pourriez nous dire quelles sont les conséquences de cette condamnation et nous parler de ce que vivent d'autres personnes qui se retrouvent dans la même situation. N'hésitez pas. Vous avez la parole.

Mme Maria Kartasheva: Le pire pour moi, c'est que je n'ai pas reçu d'aide du Canada à temps. Je l'ai reçue plus tard, après avoir réussi à attirer l'attention des médias. Pendant des mois, je me suis battue pour qu'on s'intéresse à mon cas, y compris auprès de ma députée. Elle s'est excusée plus tard parce qu'il y avait apparemment eu une erreur de la part de son assistante. Pendant des mois, je me suis sentie complètement abandonnée par le Canada, et je suis très inquiète du fait que cela puisse arriver à quelqu'un d'autre.

En bref, ce qui s'est passé, c'est que ma demande de citoyenneté était en cours de traitement au moment où j'ai été condamnée en Russie. J'ai d'abord été arrêtée, puis condamnée. J'en ai informé le ministère de l'Immigration, mais ce dernier n'a pas tenu compte de mes représentations, et ma première cérémonie de citoyenneté a été annulée. Six mois plus tard, j'ai reçu une lettre m'informant que je ne pourrais peut-être pas obtenir ma citoyenneté parce que j'étais fichée comme criminelle en Russie.

• (1745)

M. Frank Caputo: Juste pour que ce soit clair pour moi: vous avez reçu quelque chose du ministère de l'Immigration vous disant...

Mme Maria Kartasheva: C'était six mois après. Je leur ai écrit plusieurs fois pour leur demander s'il y avait des progrès. Ils m'ont dit qu'ils examinaient mon dossier et que tout se passait bien. Puis ils m'ont envoyé une lettre disant que j'avais un mois pour leur envoyer tous les documents que je voulais éventuellement fournir. Pour que vous compreniez bien, ils m'ont envoyé cette lettre au début du mois de décembre. Cela faisait des mois, et nous étions maintenant rendus à la période des Fêtes. Personne ne répondait à mes demandes d'envoi de documents. Ce n'était pas une période très agréable. Pas du tout.

Le président: D'accord. La pire partie de mon travail est de devoir couper la parole à quelqu'un qui raconte son histoire.

M. Frank Caputo: Je suis désolé.

Peut-être que l'un de mes collègues libéraux vous permettra de continuer, parce que je pense que cela vaut la peine d'être entendu.

Le président: Voyons si M. Bains acceptera de se plier à votre demande.

Monsieur Bains, vous avez cinq minutes. Allez-y, je vous prie.

M. Parm Bains: Oui, j'accepte de le faire, si tel est votre souhait.

Mme Maria Kartasheva: Fondamentalement, ma plus grande appréhension et la crainte de mes collègues de l'organisme et de beaucoup de citoyens russes au Canada, c'est qu'ils aient des problèmes au Canada lorsque leur demande de citoyenneté ou d'autres documents d'immigration seront traités, et que s'ils ont été persécutés en Russie, cela aura une incidence sur leur présence au Canada. Ma plus grande crainte était d'être expulsée. J'ai vécu avec cette peur tous les jours pendant un mois, car je ne savais pas comment cela allait se terminer.

Encore une fois, personne ne m'a présenté des excuses. Je ne sais pas pourquoi cela s'est produit. Peut-être qu'il y a quelqu'un au ministère qui voulait m'empêcher de devenir citoyenne canadienne. Peut-être que quelqu'un voulait me renvoyer en Russie pour que je finisse en prison. Je n'en sais rien. À ma connaissance, il n'y a pas eu d'enquête et je ne sais pas s'il y en aura une.

J'ai lancé une pétition pour empêcher de tels cas de se produire. J'ai dressé une liste de lois étrangères qui n'empêcheraient pas les

gens de devenir citoyens ou d'obtenir des visas, et le ministère de l'Immigration a répondu que son système était tout à fait correct et qu'il fonctionnait dans l'intérêt de personnes comme moi. Je vous laisse juger de cela, mais ce n'est pas mon avis. J'ai l'impression d'avoir été manipulée par le ministère et, je présume, par le ministre de l'Immigration, et cela me contrarie.

M. Parm Bains: Je vous remercie de nous avoir fait part de cela. Je vous présente mes excuses au nom du gouvernement. J'aimerais que nous puissions trouver une solution. Certaines des recommandations que vous avez formulées sont consignées, et elles seront assurément examinées et étudiées, et nous pourrions peut-être examiner votre cas plus en détail.

Je vais poursuivre avec vous et M. Sirois.

Pourriez-vous nous dire quels sont, selon vous, les plateformes ou les canaux les plus couramment utilisés à l'heure actuelle pour assurer la diffusion de la désinformation russe au Canada? Je sais que c'est quelque chose qui ne date pas d'hier. Très franchement, plusieurs experts en la matière nous ont dit que la Russie était à l'origine de ce genre de guerre des temps modernes, la guerre de l'information.

Pourriez-vous nous dire ce que vous savez ou ce que vous observez présentement en ce qui concerne les plateformes ou canaux utilisés à l'heure actuelle?

Mme Maria Kartasheva: Cela dépend du type de public visé.

Pour les jeunes, ce serait Telegram. Pour les personnes plus âgées, peut-être, ou les personnes qui ne sont pas très à l'aise avec Telegram, il y a Facebook. Vous pouvez voir de nombreux robots sur Facebook qui diffusent de la propagande russe, et vous pouvez savoir que ce ne sont pas de vraies personnes parce que ces avatars ne publient rien d'autre.

Il s'agit aussi de Canadiens, ou de gens qui ont émigré au Canada. Il y a aussi divers médias, des experts et des professeurs d'université au Canada qui relaient la propagande russe. Ils se rendent en Russie dans le cadre de voyages manifestement parrainés par le Kremlin, puis racontent à quel point tout est formidable en Russie et dans les territoires occupés. Ils parcourent ensuite le Canada et diffusent cette information à la population canadienne.

Les Russes utilisent assurément plusieurs stratégies pour atteindre différents groupes, et je peux dire que cela fonctionne.

M. Parm Bains: On utilise surtout des robots.

Mme Maria Kartasheva: Je pense que c'est l'un des...

M. Parm Bains: Est-ce le principal outil qui est utilisé?

• (1750)

Mme Maria Kartasheva: C'est l'un des outils qu'ils utilisent, mais ce n'est assurément pas le seul.

M. Parm Bains: D'accord.

J'aimerais passer rapidement à M. Boyd, s'il me reste un peu de temps.

Aujourd'hui même, il a été rapporté que TikTok était poursuivi aux États-Unis par plus d'une douzaine de procureurs généraux qui allèguent ceci:

[...] la plateforme de médias sociaux trompe le public quant à son caractère inoffensif. Selon les procureurs, l'application nuit à la santé mentale des enfants. Certains d'entre eux se blessent ou trouvent même la mort à cause des « défis » viraux que publie TikTok.

Êtes-vous en mesure de suivre les tendances sur TikTok ou sur d'autres plateformes? Je sais que d'autres plateformes utilisées par les jeunes peuvent avoir un impact sur eux.

M. Kenneth Boyd: Nous suivons en général les types de plateformes qui sont les plus utilisées par les jeunes, et nous menons des enquêtes auprès des enseignants et des élèves de l'ensemble du pays afin de connaître leurs habitudes en matière de médias numériques.

Il est certain que TikTok reste l'une des principales plateformes utilisées par les jeunes, et nous en sommes conscients. Souvent, lorsque nous utilisons des exemples de désinformation et de désinformation que les jeunes peuvent rencontrer, nous utilisons des exemples provenant de TikTok et nous donnons aux élèves la possibilité d'essayer de vérifier ce qui est vrai et ce qui ne l'est pas sur la plateforme.

Le président: Je vous remercie, monsieur Boyd.

Monsieur Bains, je vous remercie d'avoir permis à Mme Kartasheva d'utiliser votre temps de parole pour conclure son histoire.

[Français]

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

M. Denis Trudel: Merci, monsieur le président.

Madame Kartasheva, votre histoire est très touchante. Elle est très troublante, en fait. J'espère que le gouvernement va faire un suivi pour qu'on puisse aller au fond de cette histoire, parce que cela n'a pas de bon sens.

Dans vos remarques, vous avez dit que des analystes travaillant pour la Russie étaient invités à s'exprimer dans des médias traditionnels.

Pouvez-vous nous donner des noms?

[Traduction]

Mme Maria Kartasheva: Je suis désolée. Pouvez-vous répéter la question?

[Français]

M. Denis Trudel: Dans vos remarques, vous avez dit que des analystes travaillant pour la Russie étaient invités à s'exprimer dans des médias traditionnels, pas seulement sur des réseaux sociaux, et que cela faisait partie des méthodes utilisées par la Russie pour faire de l'ingérence étrangère, notamment au Canada. Ce sont des experts qui viennent parler de certaines situations, comme la guerre en Ukraine, et qui sont payés pour répandre la propagande du gouvernement russe.

Pouvez-vous nous donner des noms?

M. Guillaume Sirois: Il est difficile de donner des noms précis sans risquer de tomber dans la diffamation. On peut juste parler d'allégations et de choses qu'on entend dire, sans donner de réponse claire comme on pourrait le faire devant un tribunal, par exemple.

Cela dit, il y a certainement des gens qui propagent des messages du Kremlin. Certains ont collaboré à des articles sur le site Russia Today par le passé. C'est le cas d'un professeur qui a été invité à témoigner dans le cadre de l'Enquête publique sur l'ingérence étrangère et qui a dit qu'on devrait se calmer en ce qui concerne l'aide à l'Ukraine et les messages que le Kremlin essaie de propager, par exemple. Si vous voulez un nom, c'est Paul Robinson. C'est de l'information publique.

Ce genre de discours peut être très dangereux pour la diaspora, dont la diaspora russe.

M. Denis Trudel: On peut comprendre que la Russie s'intéresse à des pays comme les États-Unis, la Chine, l'Allemagne ou la France, mais le Canada, on va se le dire, n'est pas une grande puissance mondiale.

Qu'est-ce que la Russie cherche ici? Quelle est sa stratégie, globalement?

M. Guillaume Sirois: Je peux répondre aussi à cette question.

[Traduction]

Mme Kartasheva peut ajouter quelque chose, si elle en ressent le besoin.

[Français]

Le Canada est un allié important dans plusieurs alliances internationales. On peut penser à l'OTAN ou au Groupe des cinq, qui est une alliance des services de renseignements de cinq pays. Il est un partenaire très proche des États-Unis, évidemment.

On peut facilement imaginer que des acteurs étrangers hostiles, comme la Russie, mais aussi la Chine et l'Iran, souhaitent entrer par la porte arrière pour essayer de miner ces organisations importantes pour la sécurité internationale.

Le président: Merci, monsieur Trudel et monsieur Sirois.

[Traduction]

Monsieur Green, vous avez la parole pendant deux minutes et demie.

M. Matthew Green: Merci beaucoup.

Je vais m'adresser ma question à Mme Tworek.

Dans le livre que vous avez publié en 2019, intitulé *News from Germany: The Competition to Control World Communications*, vous avez découvert comment les Allemands se sont battus pour réglementer l'information chez eux et ont utilisé les nouvelles technologies pour amplifier leurs pouvoirs à l'étranger, en montrant ainsi que la guerre de l'information existe depuis longtemps. Vous avez fait allusion à cela dans votre déclaration préliminaire. Je me souviens aussi du documentaire sur Edward Bernays intitulé « Le siècle du moi », et de ses propos concernant la propagande. Il s'agit d'un outil politique très ancien.

Quelles leçons pouvons-nous tirer de l'histoire et nous en inspirer pour trouver des solutions aux problèmes actuels de désinformation et de désinformation que nous affrontons aujourd'hui?

• (1755)

Mme Heidi Tworek: Je vous remercie beaucoup de votre question.

Je pense qu'il y a toute une série de solutions.

Comme je l'ai indiqué, la première consiste à examiner les relations internationales dans leur ensemble pour essayer de prédire quels pays vont s'engager dans cette voie. C'est probablement beaucoup moins coûteux que d'autres modes d'ingérence étrangère. Nous devons être à l'affût de ce genre d'ingérence étrangère, en ayant recours à nos experts en matière de relations internationales.

Deuxièmement, il faut être attentif à la manière dont les nouvelles technologies sont utilisées. On raconte que les Allemands se sont emparés des nouvelles technologies, alors que d'autres, comme les Britanniques, s'appuyaient sur des technologies plus anciennes et n'ont pas vu venir le problème dans une certaine mesure. Nous devons être prévoyants à cet égard.

La troisième leçon est qu'il y a beaucoup de mesures que nous pouvons prendre. Nous ne sommes pas impuissants à cet égard. Nous avons déjà fait face à des situations semblables liées à de nouvelles technologies. Nous ne devrions donc pas nous contenter de lever les bras et de dire ce qui suit: « Internet et l'intelligence artificielle générative sont sans précédent, alors nous ne pouvons rien faire pour gérer les menaces qu'ils présentent ». Il y a en fait de nombreux précédents. Nous pouvons examiner des exemples de façons dont nous avons tenté de gérer ces problèmes auparavant, afin de déterminer ce qui a fonctionné et ce qui a échoué.

M. Matthew Green: Vous avez mentionné le fait que nous devons prévoir quelles entreprises utiliseront... Je suis désolé. J'ai commis un lapsus. Je voulais dire « pays », mais j'ai prononcé le mot « entreprises » parce qu'il y a aussi une foule d'acteurs non étatiques.

Pouvez-vous nous parler de la façon dont les acteurs non étatiques utilisent également ces outils en ligne? J'ai parlé de la marchandisation de l'information, et vous avez discuté brièvement de la souveraineté des données. Pourriez-vous nous en dire davantage à ce sujet? Pourriez-vous également nous parler de l'omniprésence de ces outils?

En fait, je pense que l'on peut dire, sans crainte de se tromper, que tous les pays se servent, d'une manière ou d'une autre, de ce type d'outils de désinformation.

Le président: Nous disposons de très peu de temps pour entendre la réponse à votre question.

Veuillez prendre la parole, s'il vous plaît.

Mme Heidi Tworek: Le nombre d'entreprises concernées est évidemment très faible, alors nous devons donc faire attention à la façon dont elles gagnent de leur argent, c'est-à-dire surtout grâce aux publicités, et réfléchir à la façon dont nous pourrions réglementer ces activités et à ce que les options publiques pourraient être, comme nous l'avons fait dans le passé dans le cas de la radio et de la télévision.

M. Matthew Green: Je vous remercie de votre réponse.

Le président: Je vous remercie, monsieur Green.

Voilà qui met fin à l'audience de notre groupe de témoins d'aujourd'hui. Je tiens à remercier tout le monde d'être venu.

Professeure, j'ai cru comprendre que vous alliez fournir au Comité une copie d'une étude que vous avez réalisée. Pourriez-vous le faire? Je veillerai à ce que la greffière communique avec vous.

Je tiens à remercier les représentants de l'Alliance démocratique des Canadiens russes d'avoir participé à notre réunion. Je crois comprendre que vous avez été très occupés à comparaître devant des comités parlementaires ces derniers temps. Je vous remercie encore une fois d'avoir pris le temps de comparaître devant le nôtre.

Monsieur Boyd, je vous remercie également de votre participation.

Avant de partir, je mentionne que je suis sur le point de publier l'ordre du jour de jeudi.

Monsieur Bains, votre témoin sera présent jeudi. Je vous prie de m'excuser à cet égard parce qu'en raison de la façon dont son nom figurait dans la feuille de calcul Excel, nous ne l'avons pas vu initialement, mais nous avons constaté qu'il était là lorsque nous avons consulté de nouveau le document. Je sais que vous avez soulevé la question au cours de la dernière réunion, et je vous informe qu'il sera présent jeudi.

L'autre chose que je dois mentionner au Comité, c'est que les entreprises de médias sociaux ont accepté de comparaître après la relâche de l'Action de grâce, ce qui signifie qu'il serait nécessaire que nous ajoutions deux autres réunions à cette étude. Compte tenu du niveau d'intérêt et, pour être franc, des informations importantes que nos témoins ont fournies au Comité, je vais proposer que nous prolongions cette étude en programmant deux réunions supplémentaires, afin que nous puissions entendre les entreprises de médias sociaux. Il s'agit de TikTok, Google et Meta. Elles se présenteront toutes pendant la semaine qui suivra l'Action de grâce.

Les membres du Comité sont-ils d'accord?

[Français]

Monsieur Trudel, êtes-vous d'accord sur cela?

M. Denis Trudel: Oui.

Le président: D'accord.

[Traduction]

C'est ce que nous allons faire. Nous verrons tout le monde jeudi. Je vous remercie pour toutes vos contributions.

Au nom des Canadiens, je remercie nos témoins de s'être joints à nous aujourd'hui et de nous avoir fourni de précieux renseignements.

La séance est levée.

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

PERMISSION DU PRÉSIDENT

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

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

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

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

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

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

SPEAKER'S PERMISSION

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

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

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

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

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