CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 163 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mercredi 15 mai 2019

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le mercredi 15 mai 2019

● (1530)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Chers collègues, je constate que nous avons le quorum. Bienvenue à la 163e réunion de notre vénérable comité, le meilleur comité sur la Colline.

Je suis heureux d'accueillir nos invités aujourd'hui, qui en sont tous à leur première comparution devant un comité parlementaire. J'ai demandé à mes collègues de vous ménager.

Comme vous le savez sans doute, vous aurez chacun 10 minutes. J'inviterai M. Jarry à prendre la parole en premier. Lorsqu'il aura terminé, je demanderai à M. Gull de présenter les membres de son groupe, qui seront ensuite invités à intervenir pour une période de 10 minutes.

Monsieur Jarry, vous pouvez y aller.

[*Français*]

M. Luc Jarry (conseiller sénior en cybersécurité, à titre personnel): Merci, monsieur le président.

Bonjour, mesdames et messieurs les membres du Comité.

Je m'appelle Luc Jarry et je suis conseiller sénior en cybersécurité auprès de l'entreprise Cascades. Je suis également chargé de cours. J'enseigne la cybersécurité industrielle à Polytechnique Montréal, qui est affiliée à l'Université de Montréal.

Il s'agit de ma première expérience comme témoin. J'ai consacré un peu de temps à la lecture des autres témoignages et je constate que plusieurs sujets ont été abordés. Aujourd'hui, je vais vous parler d'un sujet qui touche pratiquement tous les domaines, que ce soit sur le plan financier, industriel, des affaires ou personnel. Je parle de l'Internet des objets, mieux connu sous l'acronyme IDO, qui est naturellement associé à l'intelligence artificielle.

En quoi consiste l'Internet des objets? Je crois que la meilleure définition est la plus courte: c'est une intégration entre le monde physique et le monde virtuel et informatique. Depuis quelques années, partout dans le monde, on vit une révolution extraordinaire quant au branchement des objets sur les réseaux TCP-IP. Je parle ici d'Internet. On estime que, d'ici 2020, entre 40 et 50 milliards d'objets seront connectés à Internet. Il faut d'ailleurs se demander s'il ne faudrait pas remplacer le terme « Internet des objets » par « Internet de tout ».

Associé à l'intelligence artificielle, l'Internet des objets rend possible ce qui était inimaginable il y a quelques années. Je vais vous donner comme exemple les automobiles qui vont se conduire elles-mêmes. Elles font encore l'objet de tests. Nous en avons tous entendu parler. Aujourd'hui, si votre automobile est le moindrement récente, elle est probablement munie d'un témoin qui mesure la pression de ses pneus. Si un des pneus est mou, le témoin va envoyer un message à l'ordinateur de bord pour que le conducteur sache qu'un des pneus est mou. Le conducteur va alors devoir remédier à la situation.

Avec l'Internet des objets, la même chose va se produire, mais en plus d'informer le conducteur, la voiture va elle-même prendre un rendez-vous chez le concessionnaire ou au garage qui assure son entretien. La voiture va se rendre elle-même chez le concessionnaire pour qu'on y règle le problème et va ensuite revenir à son point d'origine. Vous voyez un peu le potentiel que cela représente. Cela va ouvrir des possibilités extraordinaires dans tous les domaines.

Hélas, avec toutes les nouvelles technologies, on fait face à de nouvelles menaces et à de nouvelles conditions de vulnérabilité. Or, ce sont presque uniquement les ordinateurs — munis de microprocesseurs et exploités par des systèmes d'exploitation — qui sont branchés sur nos réseaux Internet. Cela nous permet d'établir des défenses de base en cybersécurité. Par exemple, je constate qu'il y a dans la salle des ordinateurs portatifs qui sont ouverts. Je suis certain que ces ordinateurs font l'objet d'une protection de base en matière de cybersécurité. Il s'agit ici d'un pare-feu personnel activé et, probablement, d'un logiciel antivirus — qui, je l'espère, inclut les dernières signatures virales —, ainsi que d'un détecteur de maliciels. Un fait est important à noter. Ces ordinateurs sont munis d'un processeur et sont en mesure de chiffrer et déchiffrer les informations. Je parle ici de cryptage, une stratégie largement utilisée en cybersécurité.

Le problème, dans le cas de l'Internet des objets, est que les objets sont dépourvus de systèmes d'exploitation et de processeurs. Il n'est donc pas possible de les munir d'une protection de base, comme on peut le faire pour les ordinateurs. Cela les rend extrêmement vulnérables.

Au cours des 15 ou 20 dernières années dans le monde industriel, beaucoup d'investissements ont été faits dans des projets de mécanisation et d'automatisation. Aujourd'hui, les usines modernes utilisent des contrôles industriels tels que des automates programmables, des SCADA, qui communiquent entre eux par l'entremise de leurs protocoles de télécommunication. Ce sont des réseaux fermés et invisibles sur Internet. On en parle souvent comme de l'Intranet. Pour que les entreprises puissent bénéficier des avantages de l'intelligence artificielle, elles doivent brancher ces automates ou ces contrôles industriels à Internet pour communiquer avec des fournisseurs de services en intelligence artificielle, ce qui les rend très vulnérables.

D'un autre côté, selon mes propres observations, les contrôles industriels actuels dans les usines sont maintenus et contrôlés par des électromécaniciens, dont la plupart n'ont pas reçu de formation en cybersécurité.

Présentement, plusieurs entreprises font des branchements à l'Internet et créent des failles dans leurs propres réseaux, ce qui peut mener à des intrusions. On parle ici de vol d'information et d'espionnage industriel, bref, d'accès non autorisés.

Il y a pire que cela maintenant. Avec l'Internet des objets, imaginez qu'un pirate informatique ou même un groupe terroriste prenne le contrôle à distance d'infrastructures essentielles telles que des barrages hydroélectriques, des usines de filtration d'eau et des hôpitaux. Imaginez tous les dégâts et les menaces à la sécurité publique et financière que cela entraînerait.

On ne peut pas ignorer l'aspect de la vie privée. Comme vous le savez, les gens connectent de plus en plus des objets à leur réseau privé à la maison ou à leur téléphone cellulaire. À titre d'exemple, vous pouvez acheter un réfrigérateur qui se branche à l'Internet et qui est muni d'un écran semblable à celui d'une tablette. Le réfrigérateur peut faire l'inventaire de tous les aliments qu'il contient, gérer leurs dates de péremption et même vous proposer, au moyen de l'intelligence artificielle, des recettes basées sur ces aliments. C'est merveilleux. Par contre, du point de vue de la vie privée, on peut se demander si les compagnies d'assurance-vie souhaiteraient connaître le contenu du réfrigérateur de leurs clients. La réponse est oui.

Au Canada, les Canadiens et les Canadiennes sont protégés par des lois sur les renseignements personnels, mais il y a un problème. De nombreuses études démontrent que près de 95 % des gens acceptent des conditions de confidentialité sans les avoir lues. Les gens acceptent souvent des choses, mais ils ne savent pas quoi exactement.

Toujours au sujet de la vie privée, il y a des assistants qui se branchent à l'Internet et qui s'activent après que vous avez prononcé une phrase ou un mot clé. Vous pouvez alors échanger avec eux au sujet de diverses informations qui se trouvent sur l'Internet, telles que la météo et les nouvelles. Si des appareils de ce genre sont branchés sur un réseau résidentiel non sécurisé, auquel il est très facile d'avoir accès, un pirate informatique, au moyen d'un ver informatique, pourrait vous enregistrer. Si l'appareil est muni d'un appareil photo, un pirate informatique pourrait prendre des photos de vous. Il y aurait manifestement une violation de la vie privée.

Je pourrais vous donner plusieurs exemples. Le document que je vous ai présenté contient une série de recommandations, mais, hélas, je n'aurai pas le temps de toutes les passer en revue.

Avec votre permission, monsieur le président, je vais répondre aux questions maintenant.

Je vous remercie.

● (1535)

Le président: Merci, monsieur Jarry.

[*Traduction*]

Je vais probablement devoir me procurer un de ces réfrigérateurs, comme ça je n'aurai plus à préparer mes propres repas. Ce sera véritablement miraculeux.

M. Michel Picard (Montarville, Lib.): Ils ne préparent pas les repas pour vous.

Le président: Un sandwich au baloney reste un sandwich au baloney, peu importe qui le prépare.

Monsieur Gull, vous avez 10 minutes; je vous demanderais de bien vouloir présenter vos collègues.

M. Tony Gull (président, Tawich Development Corporation): Merci.

[*Le témoin s'exprime en cri.*]

[*Traduction*]

Je vous remercie de nous avoir donné l'occasion de nous exprimer et de vous décrire rapidement les occasions que nous envisageons saisir pour le bien de notre nation — la nation crie — et de notre collectivité, plus précisément, Wemindji.

À ma gauche sont les conseillers qui travaillent avec nous, la société, dans ce dossier. Je vous présente Sam Gull, conseiller; Jean Schiettekatte, également conseiller; et Robert Milo. Ces trois conseillers sont en quelque sorte des experts en matière de ce que nous cherchons à accomplir.

Comme vous l'avez sans doute compris, nous cherchons à établir un lien de télécommunication par fibre optique reliant le Canada, l'Asie et l'Europe, lien essentiel pour assurer la cybersécurité dans le secteur financier au Canada.

La société elle-même appartient à part entière à la collectivité de Wemindji, qui compte quelque 1 400 habitants. Pour vous donner une idée, à l'heure actuelle, la société s'appelle Tawich. Tawich signifie « éloigné ». C'est littéralement une société de développement éloignée.

Pour votre information, je précise que la société compte actuellement plus de 1 000 employés au Québec — en Abitibi et ailleurs — et regroupe diverses compagnies. Tout simplement, nous avons ici une nouvelle occasion formidable de nous rapprocher de notre objectif, qui est de convaincre certaines personnes de contribuer au projet ensemble.

Comme vous le savez déjà, c'est *keskun*, qui signifie « nuages ». Dans le monde de l'informatique et d'Internet, « nuages » se dit *keskun* dans notre dialecte. Concrètement, il s'agit du projet de centre de données qui sera construit sur le territoire cri de notre collectivité. *Keskun* est essentiellement un parc de grands centres de données nordiques; c'est le projet qui nous occupe.

Le projet nécessitera initialement une alimentation en électricité de 200 mégawatts. Tout le monde sait que la centrale Robert Bourassa, située à quelques heures de route de chez nous, est la source d'énergie verte la plus fiable en Amérique du Nord. Le 29 avril 2019, la Régie de l'énergie du Québec a autorisé l'attribution d'un certain nombre de mégawatts aux centres de calcul.

Nous sommes d'avis que le Canada est essentiellement limité aux États-Unis pour sa connectivité Internet internationale. Environ 11 % du trafic Internet international canadien ne passe pas par les États-Unis.

Le témoin précédent a invoqué une image que nous utilisons souvent. Il se bâtit une grande autoroute, et nous voulons y construire un point d'accès pour pouvoir l'emprunter. La cybersécurité canadienne, y compris les transactions financières, dépend des États-Unis. C'est ce que nous considérons comme un maillon faible.

Je cède maintenant la parole à mes conseillers et collègues, qui vous en diront un peu plus sur le projet.

● (1540)

M. Sam Gull (conseiller, Tawich Development Corporation): *Meegwetch*.

[*Le témoin s'exprime en cri.*]

[*Traduction*]

Je vous remercie de m'avoir invité à faire ma présentation.

Comme vous pouvez le voir à l'écran, notre plus gros problème ici, au Canada, est que tous nos liens sont aux États-Unis. Seuls 11 % de ces liens se situent au Canada — plus précisément, entre Terre-Neuve et le Groenland. C'est notre seule issue. Tous les autres liens se trouvent aux États-Unis. C'est selon nous un grave problème.

Comme vous pouvez le voir à l'écran, nous envisageons participer à un projet : le lien de fibre optique Quintillion. L'Alaska est déjà desservie; c'était la première phase. La deuxième consistera à étendre le réseau de l'Alaska jusqu'au Japon, et la troisième, à rejoindre l'Alaska et l'Europe en passant par le détroit d'Hudson. C'est dans le cadre de la troisième phase que nous souhaitons connecter Wemindji au réseau. En effet, quand la canalisation sera posée, nous aurons une seule occasion de nous connecter, et nous ne voulons certainement pas la manquer.

Le lien nordique consiste en une fibre... Six grandes liaisons à fibres optiques y sont connectées, dont deux se situent exclusivement en eaux internationales. C'est à ces deux liaisons-là que nous souhaitons nous connecter, car notre Première Nation considère essentielles la sécurité, la sûreté et la souveraineté de l'Arctique. Le lien qui longera la baie James ira également rejoindre Montréal, Toronto et le réseau du sud.

Un projet de fibre optique nordique est nécessaire pour assurer la connectivité internationale du Canada et assurer la cybersécurité de son réseau.

Comme vous pouvez le voir sur la carte qui s'affiche à l'écran, la liaison optique traverserait le passage du Nord-Ouest, de l'Alaska en passant par le détroit d'Hudson. C'est là que nous voulons rejoindre le réseau, par la baie James jusqu'à la collectivité de Wemindji, où se situe la Société de développement Tawich, et à partir de là, on irait rejoindre Montréal et Toronto.

Comme vous pouvez le voir sur la carte, 89 % des données canadiennes transitent par les États-Unis. Ainsi, elles sont régies par la Patriot Act américaine, créant une vulnérabilité sur le plan de la sécurité. Une nouvelle fibre optique nordique du Canada serait en mesure de changer ce paradigme. Il est important d'avoir des centres de données avec accès par fibre optique à la connectivité internationale et à très haute connectivité à très faible latence — de l'ordre des millisecondes — sur de longues distances. La position géographique — soit la proximité des centres financiers à Londres, New York, Tokyo, Shanghai, Montréal et Toronto — est elle aussi critique. Nous avons aussi l'avantage d'être alimentés par de l'énergie renouvelable provenant d'un réseau nordique inépuisable, ultra fiable et très peu coûteux, soit de l'ordre de 4 ¢US par kilowatt. De plus, les coûts d'exploitation de nos centres de traitement des données sont très faibles, surtout compte tenu de leur capacité de refroidissement. Comme on le sait, ces ordinateurs ont tendance à surchauffer.

Un lien nordique assurerait la sécurité de la connectivité internationale indépendamment des États-Unis. En guise d'exemple, on serait en mesure d'accélérer les délais de transmission de 18 millisecondes entre Montréal et Tokyo. Aux États-Unis, on ne constaterait aucune réelle différence. C'est entre Montréal et Toronto et l'Angleterre et l'Asie que l'on verrait la plus grande amélioration.

Dans son plan stratégique, Hydro Québec a annoncé un taux d'environ 4 ¢ par kilowatt, ce qui représente un avantage considéraBle pour nous en matière de consommation électrique. Nous avons aussi l'avantage d'être sur le bouclier canadien, qui n'éprouve aucun tremblement de terre. Vous avez sûrement entendu parler de ce qui s'est passé au Japon et en Alaska. Comme les tremblements de terre sont un grave problème, il y aurait intérêt à situer les centres de données du Nord sur le bouclier.

J'aimerais maintenant céder la parole à Jean Schiettekatte, qui terminera notre présentation.

● (1545)

M. Jean Fernand Schiettekatte (conseiller, Tawich Development Corporation): Merci, Sam.

Merci à tous de votre accueil aujourd'hui.

[*Français*]

Comme vous l'avez vu dans la présentation, en raison des temps de latence très faibles, toutes les transactions financières canadiennes passeront par ce lien. C'est une occasion pour nous d'offrir aux Canadiens une solution de sécurité qui n'est pas que logicielle; elle est aussi matérielle. L'idée est de construire une fibre nordique indépendante et internationale, dont le principal avantage serait de permettre aux Canadiens d'assurer leur souveraineté sur ce territoire, avec les Premières Nations. C'est un aspect très important que nous voulons voir dans ce projet.

Je pense que c'est aujourd'hui votre dernière réunion sur ce sujet. Nous aimerions que le Comité se penche sur cette option. Il y a le lien Quintillion qui est en développement dont un premier segment est déjà en service, mais il pourrait y avoir un autre projet canadien qui se relierait au réseau. Comme l'a dit M. Gull, des parties de ce câble resteraient en eaux internationales. Cela pourrait fournir une connexion internationale cybersécuritaire et assurerait aux Canadiens un accès à d'autres marchés avec un temps de latence très faible. Cela nous donnerait un avantage dans nos transactions financières internationales et, plus important encore, cela nous permettrait d'assurer la souveraineté du Canada sur ce passage.

Il serait intéressant de combiner cela avec l'interconnexion des communautés nordiques, mais cela ne devrait pas être le premier objectif. Le premier objectif est d'assurer notre sécurité. Évidemment, il y a toutes sortes d'autres avantages, comme la formation de travailleurs et la création d'emplois dans le Nord, qui sont bénéfiques sur le plan économique.

Merci, monsieur le président.

Le président: Merci à tous.

[*Traduction*]

Monsieur Graham, je précise que vous avez sept minutes.

M. David de Burgh Graham (Laurentides—Labelle, Lib.): Merci à tous d'être venus. Nous avons deux témoins très différents aujourd'hui.

Je dois dire que je trouve le projet *keskun* fort intéressant. Comme vous le savez, nous en avons déjà parlé.

Monsieur Gull, si on manque la chance de se raccorder au réseau de fibre optique Quintillion à l'étape de sa construction, dans quelle mesure sera-t-il difficile de s'y raccorder par la suite?

M. Sam Gull: En tant que Canadien et que Cri, j'estime que le Canada doit agir, qu'il doit construire sa propre fibre optique. Tout le monde sait que la quantité d'information ou de données que nous utilisons par année augmente, et elle continuera d'augmenter. Ça ne ralentira pas de sitôt.

Si nous ne pouvons pas nous connecter au réseau Quintillion, j'estime que le Canada devrait agir et construire son propre réseau de fibre.

M. David de Burgh Graham: Vous disiez dans votre introduction que c'est une question de souveraineté des réseaux. Le Canada n'a aucune telle souveraineté. Quintillion, qui relie Tokyo à Londres, si j'ai bien compris, nous permettrait d'avoir une certaine souveraineté par rapport aux États-Unis, ce qui semble être l'objectif premier.

À propos de l'exploitation de centres de traitement des données, vous avez parlé d'un avantage de 18 millisecondes et de son impact sur le secteur des finances. Relativement aux investissements, qu'est-ce que cela signifie pour le secteur financier? Faudra-t-il que les centres de données du secteur déménagent plus au nord?

M. Tony Gull: J'aurais une observation à faire avant que Jean vous donne une réponse un peu plus pointue.

En ce qui me concerne, c'est une question de développement économique; c'est pour ça que je suis ici. J'ai pour mandat le développement économique, et j'estime également que le gouvernement fédéral a une responsabilité à cet égard — tout comme vous, dans une certaine mesure. Je pense que le projet présente d'importants débouchés économiques, mais surtout... Quand on parle de cybersécurité ou de souveraineté des réseaux, tout revient aux données elles-mêmes. Il est essentiel qu'on les ait et qu'on les garde.

Pour moi, quand on parle d'impact, tout revient au développement économique, car c'est mon mandat. C'est mon domaine d'activité, et c'est pourquoi j'ai voulu comparaître devant vous aujourd'hui.

Allez-y, Jean.

M. Jean Fernand Schiettekatte: La réponse simple est assez intéressante. On peut la trouver dans le tableau des latences. À ce point-ci, aucune banque au monde ne peut se permettre de ne pas avoir un centre. Quiconque effectue des opérations en devises étrangères doit avoir accès en tout temps aux données provenant des marchés de Londres, de Tokyo et de New York. Nous serons le point d'accès. Les principales transactions commerciales — celles dont vous avez parlé, où quelqu'un s'est fait pirater — passeront par cette ligne, et c'est nous qui la contrôlerons. Ce n'est pas le cas pour le moment et toutes nos transactions passent par New York. Chaque fois que vous transférez de l'argent, la transaction transite par New York, par son système.

Voilà pourquoi nous estimons que c'est si important au chapitre de la cybersécurité. Pour combler cette lacune, il faut absolument envisager des solutions matérielles.

● (1550)

M. David de Burgh Graham: Qui contrôle la ligne?

M. Jean Fernand Schiettekatte: Aux États-Unis, c'est la NSA qui surveille toutes vos transactions.

M. David de Burgh Graham: Je suppose qu'ils travaillent de ce côté-ci de la frontière, aussi, ce qui m'amène à une autre question. La ligne Quintillion et la ligne *keskun* touchent toutes deux à la sécurité nationale. Que peut-on faire pour protéger les lignes contre d'éventuelles attaques par des sous-marins en mission scientifique dans le Nord?

M. Jean Fernand Schiettekatte: Je pense qu'il faudrait avant tout affirmer notre souveraineté. Quiconque arrive le premier occupera le territoire. C'est compromettre sa souveraineté que d'attendre qu'une autre compagnie ou qu'un autre pays prenne l'initiative. L'idée, c'est justement de surveiller [*Inaudible*]. Je pense qu'il est très difficile d'affirmer la sécurité d'une liaison par satellite, c'est pourquoi on construit le réseau sous terre. Ainsi, on peut assurer une surveillance et déterminer si les propriétés de la fibre optique sont intactes et s'il y a eu tentative d'interception. C'est la façon de procéder. Je ne vois aucune autre option.

M. Sam Gull: J'ajouterais également que, selon les discussions que nous avons eues, la ligne sera posée au moins trois pieds sous le plancher océanique à cause des icebergs. C'était un problème. Si nous la mettons sous terre, les sous-marins ne pourront ni la trouver, ni la voir.

M. Robert Milot (conseiller, Tawich Development Corporation): Une chose est sûre, à partir du moment où Quintillion ou autre aura terminé la construction de la canalisation de fibre optique, on ne pourra plus se connecter au réseau. Il faut que ce soit fait avant. Nous avons déjà fait des démarches auprès du gouvernement du Québec, du premier ministre et de divers ministères; l'idée semble susciter un vif intérêt.

M. David de Burgh Graham: Voilà qui répond à bien des problèmes qui ont été soulevés dans le cadre de l'étude. Nous avons toujours des problèmes dans [*Inaudible*], mais c'est la première fois qu'on vient nous présenter une solution. Je vous en suis très reconnaissant.

J'ai quelques courtes questions à poser à M. Jarry, s'il me reste du temps.

[*Français*]

Monsieur Jarry, dans votre présentation, vous avez parlé de l'Internet des affaires.

M. Luc Jarry: C'est l'Internet des objets.

M. David de Burgh Graham: D'accord. On parlait d'une automobile qui parle à un mécanicien pour prendre rendez-vous. Cela n'ouvre-t-il pas grand la porte pour que l'automobile aille directement à la maison du voleur?

M. Luc Jarry: À la maison du voleur, vous dites?

M. David de Burgh Graham: Oui. Je crève le pneu d'une automobile, puis je lui dis que je suis son mécanicien. Elle s'en vient me voir et j'ai l'automobile.

M. Luc Jarry: Cela peut être une des vulnérabilités.

Il va de soi que ces nouvelles technologies vont mener à des situations semblables, mais il y a pire que cela. Présentement, avec votre téléphone cellulaire, vous pouvez même contrôler la porte de votre maison lorsque vous êtes absent. Vous pouvez répondre et ouvrir la porte à distance. Si quelqu'un s'infiltre dans votre système, il peut facilement savoir que vous êtes absent et déverrouiller votre porte.

M. David de Burgh Graham: Hier ou avant-hier, il y a eu une faille de sécurité dans WhatsApp. Êtes-vous au courant de cela?

M. Luc Jarry: Oui.

M. David de Burgh Graham: Pouvez-vous nous en parler davantage?

M. Luc Jarry: Un logiciel malveillant a été installé et a espionné les communications de téléphones cellulaires. Si on a appelé une personne, l'appareil a été infecté, et ce, même si elle n'a pas répondu,. C'est encore une question de mises à jour. Vous avez raison. C'est sorti dans les médias hier.

M. David de Burgh Graham: Vous avez dit que 95 % des gens ne lisent pas le contrat de licence d'utilisation, mais je dirais que c'est plutôt 99,99 %.

M. Luc Jarry: Le chiffre que j'ai donné vient d'entrevues qu'a faites Deloitte dans le cadre d'une étude. Je suis d'accord avec vous que ce chiffre est très conservateur.

M. David de Burgh Graham: Vous êtes sans doute au courant de ce qu'a fait PC Pitstop en 2005. Elle offrait 1 000 $ à qui lirait son contrat de licence d'utilisation. Cela a pris cinq mois et 3 000 ventes pour que quelqu'un réclame les 1 000 $.

M. Luc Jarry: Tout à fait.

Le président: Merci, monsieur Graham.

[*Traduction*]

Monsieur Motz, vous avez sept minutes.

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): Merci, monsieur le président.

Je remercie les deux groupes de témoins d'avoir accepté de comparaître.

Votre projet de connexion m'intrigue. Vous avez indiqué qu'il va falloir agir rapidement pour se connecter au réseau de fibre optique en cours de construction. Quand est-ce que vous vous attendez à connaître la décision afin de pouvoir prendre votre place en ligne et vous assurer d'être connecté avant l'installation de la ligne?

● (1555)

M. Jean Fernand Schiettekatte: Présentement, le délai est de deux ans.

M. Glen Motz: C'est l'échéancier prévu pour la construction de la ligne.

M. Jean Fernand Schiettekatte: Ils doivent d'abord dresser des plans pour voir s'il est possible d'établir un lien dans le détroit d'Hudson qui irait rejoindre le reste. L'idée, c'est qu'il faut d'abord dresser des plans et déterminer le processus. On s'occupe présentement de la connexion entre Alaska et le Japon. Au terme d'un exercice de repérage l'été dernier, le feu vert a été donné à cette phase-là du projet. Par la suite, ils commenceront à dresser les plans pour les deux années suivantes.

M. Glen Motz: Dans votre conclusion, vous parlez, entre autres, de solutions matérielles. Vous allez certainement avoir besoin de matériel pour rejoindre ce réseau. Comment assurer, d'une part, la sécurité matérielle, et de l'autre, la fiabilité du fournisseur? C'est une question de cybersécurité. L'étude du comité s'intéresse avant tout aux dimensions financières, mais elle touche également à maints égards à la cybersécurité. Comment comptez-vous contrôler la sécurité du matériel que vous recevrez?

M. Jean Fernand Schiettekatte: Je pense que c'est une question de conformité de l'ensemble du processus d'approvisionnement. Notre argument principal, c'est qu'on va dépendre des États-Unis tant qu'on n'aura pas sa propre ligne. Il est impossible de sous-estimer la gravité du problème. Évidemment, il faut s'assurer que le fournisseur des composantes de ce qu'on appelle les stations de raccordement aux lignes terrestres respecte toutes les normes canadiennes en matière de sécurité. Il y a certaines normes qui s'appliquent. Nos forces armées en ont. Je pense qu'il faudrait appliquer ces normes-là si on veut véritablement garantir la sécurité matérielle.

M. Glen Motz: À mesure que votre organisation dresse ses plans et franchit des étapes — je pense d'ailleurs que c'est un excellent projet auquel participer — il y aura des attentes, c'est sûr. En tant que promoteur du projet, on attendra de vous que vous assuriez la sécurité du matériel que vous utilisez. C'est par curiosité que je pose ces questions.

M. Jean Fernand Schiettekatte: Nous faisons affaire avec un certain nombre d'entreprises-conseil, dont notamment IBM, qui a la réputation d'avoir réalisé des projets semblables; effectivement, elle suit certaines normes.

M. Glen Motz: Dans votre présentation, monsieur Tony Gull, je pense que vous avez mentionné qu'une de vos entreprises s'appelle Creenet. Je pense que c'est une excellente initiative commerciale, mais j'imagine que vous vous êtes retrouvés face à d'importants obstacles lorsque vous avez entamé le processus pour établir un fournisseur de services, surtout dans la région que vous vouliez desservir. Comment avez-vous réussi à créer ce réseau, compte tenu des difficultés que vous avez eues?

M. Tony Gull: Creenet a commencé aux alentours de 1998. L'idée était d'établir un fournisseur de services qui serait en mesure de desservir la région en question; à l'époque, il n'y en avait pas.

Dans le même ordre d'idées, la taille du marché complique les choses à maints égards. Les entreprises du milieu fonctionnent dans un marché très concurrentiel de très grande envergure; il faut donc avoir un marché suffisant. Nous poursuivions le marché de la nation crie, mais en bref, on a plutôt appuyé l'idée d'une entité régionale; je pense qu'il en a été question aujourd'hui. C'est le Réseau de communications Eeyou, une entité régionale dirigée par le gouvernement de la nation crie.

M. Glen Motz: À votre avis, monsieur, les infrastructures essentielles du Nord — celles dont nous parlions et les autres — sont-elles suffisamment protégées par le gouvernement? Le gouvernement prend-il la protection des infrastructures essentielles dans votre région du Canada aussi au sérieux qu'il le devrait?

M. Tony Gull: Avant d'occuper mes fonctions actuelles, j'ai géré directement l'entreprise pendant de nombreuses années. Selon mon expérience, nous sommes très vulnérables, comme tout le monde. En ce qui concerne la sécurité et la protection de l'information, nous n'avons ménagé aucun effort pour prendre les mesures appropriées.

Toutes les nations ou toutes les entreprises, comme monsieur en a parlé plus tôt, sont vulnérables aux problèmes de cybersécurité. Il faut toujours rester à jour, que l'on pense au logiciel ou au matériel utilisés.

● (1600)

M. Sam Gull: Je voudrais ajouter quelque chose. Je crois que nous savons qui entre dans la communauté et qui en sort. Il n'y a qu'une voie d'accès vers Wemindji et une route vers le nord, la route de la baie James. Toutes les entrées et les sorties sont surveillées. L'accès routier est très facilement contrôlable. Wemindji a évidemment un aéroport. La communauté est donc accessible par avion. Il y a aussi la baie James, qui est très peu profonde. Je ne crois pas que les sous-marins peuvent s'y déplacer. Quelques rochers se dresseraient sur leur chemin. La baie est très peu profonde, et l'emplacement des sédiments change constamment.

M. Glen Motz: Monsieur Jarry, ma dernière question s'adresse à vous. Compte tenu de votre expérience et de votre emploi actuel, avez-vous l'impression que les gouvernements font du bon travail pour garantir que les infrastructures essentielles canadiennes résistent aux attaques? À votre avis, y a-t-il des aspects à améliorer?

M. Luc Jarry: Selon mon expérience, compte tenu du développement de l'Internet des objets, la question ne touche pas seulement le Canada, mais tous les pays du monde. En ce qui concerne les cyberattaques, il s'agit essentiellement de protéger l'information. On cherche à empêcher les vols d'identité, les fraudes, les attaques par déni de service et ce genre de choses. En passant à la connexion des objets, l'aspect physique prend de l'ampleur. C'est ce qui est préoccupant.

En avons-nous fait assez en matière de cybersécurité? Par exemple, dans le cas d'une transaction très délicate ou d'une commande pour fermer une valve donnée, a-t-on recours à une méthode d'authentification, qu'elle soit biométrique ou autre, suffisamment forte? Je ne crois pas que la réponse soit oui. C'est probablement non. Les mesures prises sont insuffisantes. Cela dit, ce n'est pas propre au Canada. La situation est la même partout dans le monde.

Le président: Merci, monsieur Motz.

Monsieur Dubé, vous avez sept minutes.

[*Français*]

M. Matthew Dubé (Beloeil—Chambly, NPD): Merci, monsieur le président.

Je remercie tous les témoins d'être parmi nous aujourd'hui.

Monsieur Jarry, j'ai une question pour vous.

J'imagine que vous connaissez l'histoire selon laquelle le CRTC a participé à une perquisition, faite par la GRC, chez un individu qui utilisait des logiciels, des « bots », comme on dit en bon français, pour la cryptomonnaie. Tout le monde l'a appris parce que c'était la première fois que l'on avait recours à ces pouvoirs. Ce sont des pouvoirs qui ont été accordés en vertu de la Loi canadienne anti-pourriel.

Cela m'a mené à une réflexion et à une question, et je suis curieux de vous entendre à ce sujet. Si on apporte un changement tant sur le plan législatif que sur le plan réglementaire pour toutes les questions soulevées pendant cette étude, entre autres, comme l'Internet des objets, se tournerait-on vers le CRTC en cas de problème? Serait-on mieux de créer un nouvel organe pour assurer la mise en œuvre de normes pour les appareils, par exemple? Serait-ce quelque chose qui serait examiné autant du point de vue législatif que réglementaire?

M. Luc Jarry: C'est sûr que, dans le domaine de la télécommunication, le CRTC a un rôle important à jouer, particulièrement dans tout ce qui concerne la sécurité des transmissions électroniques. N'oublions pas le sans-fil. La cybersécurité ne porte pas seulement sur les télécommunications, mais aussi sur la programmation, le développement. On parle aussi de plus en plus de la dimension physique, qui doit être prise en considération.

Selon moi, il devrait y avoir un organisme qui chapeaute toutes ces organisations et qui touchera tous les domaines. Alors, ce n'est pas seulement le CRTC.

M. Matthew Dubé: Je comprends et je suis du même avis.

Cependant, prenons l'individu chez qui on a fait la perquisition et qui poserait peut-être aussi une menace à la cybersécurité. C'était en lien avec la cryptomonnaie, mais on sait bien que c'est peut-être un individu qui s'était engagé dans d'autres activités connexes. Si on regarde la Loi actuelle, croyez-vous que la GRC ou le CRTC aurait été en mesure de faire quoi que ce soit? A-t-on vraiment besoin d'une mise à jour de la Loi? Comme vous dites, faut-il mieux encadrer qui s'occupe de quoi pour éviter de la confusion?

M. Luc Jarry: En ce qui a trait au gouvernement, je ne peux vraiment pas répondre à cette question. Par contre, je peux vous dire ce que je vois dans l'industrie. Pendant ma présentation, je mentionnais que, aujourd'hui, ce sont des électromécaniciens qui s'occupent de bon nombre d'équipements. Ces gens n'ont pas reçu de formation en cybersécurité. Pourtant, ils effectuent des branchements directement à Internet.

Pour répondre à votre question, oui, plusieurs choses peuvent être faites. Doit-on créer un corps de police spécialisé ou une équipe d'intervention spécialisée? Peut-être, mais cela touche plusieurs domaines. Encore une fois, la cybersécurité ne s'applique pas seulement aux télécommunications.

● (1605)

M. Matthew Dubé: Messieurs, vous avez beaucoup parlé de la collaboration souhaitée avec Hydro-Québec. Je veux aborder un autre aspect de cette question qui n'a pas été soulevé. Je suis curieux de vous entendre, étant donné le travail que vous faites.

Il y a quelques années, le gouvernement du Québec, l'Union des municipalités du Québec et Hydro-Québec ont indiqué que le réseau de fibres optiques en expansion d'Hydro-Québec, avec les compteurs intelligents, serait peut-être une solution pour offrir la connectivité dans les régions plus éloignées. Que pensez-vous de cela, surtout en ce qui concerne les propositions que vous mettez en avant?

M. Jean Fernand Schiettekatte: En fait, il y a actuellement des discussions avec Hydro-Québec pour pouvoir utiliser son réseau de fibre noire, mais c'est encore un réseau qui dessert le Sud. Effectivement, cela permettrait d'optimiser le Réseau de communications Eeyou, ou RCE, et d'augmenter la sécurité du côté du Sud, mais cela n'apporte pas de solution dans le Nord.

Nous pensons que cela doit être traité par le Comité, parce que c'est un enjeu très important, actuellement.

M. Matthew Dubé: Tout à fait; vous l'avez bien expliqué. Cela mène à une autre question.

L'une des préoccupations soulevées relativement à la cybersécurité est l'impact sur notre vie quotidienne, car nous nous servons de plus en plus d'objets qui peuvent être menacés par des atteintes à la cybersécurité.

Quelle est votre réalité, étant donné que vous êtes éloignés physiquement des grands centres? Dans le cas où une attaque de cybersécurité survenait contre notre réseau dans un grand centre, elle causerait une panne et nous aurions énormément de difficultés, mais, au moins, il y a la proximité géographique d'autres communautés et d'autres personnes. Quel impact cela peut-il avoir chez vous?

M. Jean Fernand Schiettekatte: Je peux répondre de façon indirecte. L'idéal serait le cas de la Suède, où le réseau de fibre noire est installé par le gouvernement. Tous les fournisseurs s'en servent et illuminent la même fibre. En cas de panne, un des fournisseurs sera touché et pas les autres.

Actuellement, notre problème est qu'il y a seulement un fournisseur qui utilise une fibre. L'idée serait d'avoir une stratégie de diversification et c'est ce dont nous discutons avec les gens du gouvernement. Il est question de voir s'il y a moyen que plus d'un fournisseur desserve la région.

M. Matthew Dubé: C'est parfait.

J'ai fait le tour de mes questions, mais j'aimerais faire écho à ce qu'a dit M. Graham, c'est-à-dire que c'est intéressant d'avoir une solution concrète et tournée vers l'avenir plutôt que de continuellement s'attarder aux menaces dans le présent. C'est important, mais le point de vue que vous présentez est intéressant aussi.

Merci.

[*Traduction*]

Le président: Monsieur Picard, vous avez sept minutes.

[*Français*]

M. Michel Picard: Merci, monsieur le président.

Monsieur Jarry, vous dites que vous travaillez aussi pour Cascades.

M. Luc Jarry: Oui.

M. Michel Picard: Depuis que les ordinateurs existent et que les compagnies ont des systèmes électroniques, nous avons des départements des technologies de l'information pour s'occuper des logiciels, des mises à jour et des pare-feu, entre autres.

Le fait d'appeler maintenant le département de cybersécurité comme tel vient-il d'un simple changement de nom de ce département ou y a-t-il une dimension différente qui justifie pourquoi on parle maintenant de cybersécurité dans une entreprise privée comme Cascades?

M. Luc Jarry: Le département des TI est toujours le même. Par contre, il y a maintenant un groupe de cybersécurité associé à la gouvernance qui ne fait pas partie de l'équipe des TI.

M. Michel Picard: Quel a été le processus par lequel la compagnie a mis sur pied cet élément de cybersécurité? Était-elle préoccupée par son équipement et la crainte qu'il y ait interruption de service ou d'opération de ses machines, ou bien craignait-elle d'être victime d'attaques extérieures mettant en danger ses données administratives?

M. Luc Jarry: Monsieur, la cybersécurité est basée sur trois piliers, soit la confidentialité, l'intégrité et la disponibilité des informations. Il y a un aspect de conformité, également. D'ailleurs, toutes les entreprises doivent maintenant demeurer conformes. Non pas que je sois âgé, mais je suis expérimenté et j'ai connu le temps où les mesures de cybersécurité étaient reconnues comme des pratiques exemplaires. Toutefois, il s'agissait plutôt de suggestions; elles n'étaient pas obligatoires.

Nous avons maintenant des lois et des règles obligatoires en place. Cascades a été l'une des entreprises, comme bien d'autres, à établir des normes et une politique de sécurité basée sur les normes ISO 27001 et 27003. L'entreprise a établi un groupe de gouvernance et a déployé une politique de sécurité selon ses propres standards, toujours basés sur la confidentialité, l'intégrité et la disponibilité des systèmes.

● (1610)

M. Michel Picard: Justement pour éviter que vous soyez victimes à l'intérieur de votre réseau, comment faites-vous pour garantir que vos fournisseurs répondent aux mêmes standards dans votre écosystème?

M. Luc Jarry: C'est par demande contractuelle. Nous pouvons demander au fournisseur d'avoir des certifications précises. Par exemple, lorsque nous traitons des renseignements personnels de nos employés, nous exigeons une certification ISO 27018 relative à la protection des renseignements personnels à tous nos fournisseurs. C'est une façon de le faire. Sinon, cela se fait carrément par des obligations ou des normes précises que nous incluons dans nos contrats.

M. Michel Picard: Ce qui suit peut sembler être une question piège, mais je dois la poser quand même.

Voyons les choses dans l'ordre inverse. Si Cascades était victime d'une attaque extérieure contre ses données, est-ce qu'elle aurait l'obligation de le rapporter à quelqu'un, quelque part, d'une façon ou d'une autre?

M. Luc Jarry: Cela dépendrait du type d'attaque. Si l'attaque touchait les renseignements personnels, absolument, nous devrions rapporter l'incident.

M. Michel Picard: D'accord.

Cela se fait à Polytechnique Montréal et à l'Université Ryerson, dont ma collègue a invité un représentant, mais il existe peu d'établissements au Canada, ou de ressources, qui offrent l'expertise pour répondre aux besoins de gestion de nos problèmes de cybersécurité. Les ressources sont limitées et rares. On craint que la qualité de l'expertise, aussi bonne soit-elle, ne soit pas suffisante.

Si l'on compare l'expertise qui se fait ailleurs, et surtout la qualité et la profondeur des attaques qui viennent de l'extérieur, comment estimez-vous le niveau d'expertise et le niveau de la formation offerts au Canada relativement aux menaces externes?

Je ne veux pas faire de publicité ou de marketing, mais, franchement, si on veut améliorer la situation, il faut savoir à quel niveau on se trouve.

M. Luc Jarry: Vous avez raison. C'est d'ailleurs une inquiétude non seulement sur le plan de l'enseignement, mais partout dans l'industrie. Les ressources expérimentées sont de plus en plus rares.

Je dois dire qu'il y a maintenant de plus en plus de jeunes qui s'intéressent à la cybersécurité. Cependant, c'est un domaine encore en évolution. Les bonnes ressources expérimentées sont excessivement difficiles à trouver.

J'ai mentionné que j'étais chargé de cours. N'oublions pas que cela demande une expertise dans la matière enseignée, mais aussi des techniques d'enseignement. Ce sont deux choses.

M. Michel Picard: En élaborant sa stratégie de cybersécurité, Cascades craint-elle que les attaques puissent être telles qu'elles pourraient compromettre la survie de l'entreprise? Peut-être qu'on en est pas là non plus?

M. Luc Jarry: Au cours des dernières années, Cascades a modernisé toutes ses plateformes. Elle a migré sur des plateformes modernes, entre autres, des plateformes SAP, pour ne nommer que celles-là. En ce qui a trait à la disponibilité, lorsque ces systèmes échouent, la période d'intolérance est d'environ deux heures. Cela veut dire que, après deux heures, les usines commencent à fermer et à cesser de fonctionner. Cela est extrêmement coûteux.

Vous avez raison: cela crée une énorme dépendance. Nous traitons cela par des plans de mesures d'urgence et des essais de réconciliation avec des relayages ou des centres de données, mais ce sont aussi des exigences que nous posons à nos fournisseurs de service.

M. Michel Picard: Compte tenu de la participation de Cascades — qui est aussi fournisseur — à cet écosystème réseautique, est-ce que la connectivité est à ce point sensible qu'un impact chez vous pourrait créer des préjudices comparables pour certains de vos fournisseurs?

Par exemple, quelqu'un pourrait-il compromettre un de vos fournisseurs en utilisant votre système?

● (1615)

M. Luc Jarry: Sur le plan de la connectivité, je dirais que non, pas avec le modèle que nous avons.

Nous avons, en effet, des liens dédiés avec certains de nos fournisseurs, justement parce que nous demandons une fiabilité et une disponibilité élevées. Ce sont des choses dont discutent mes collègues concernant des fibres optiques.

Nous utilisons des protocoles avec différents fournisseurs de services au Canada et aux États-Unis avec des liens MPLS dédiés. Pour d'autres, ce n'est pas nécessaire. Il ne faut pas oublier qu'il y a des niveaux de criticité qui sont associés à nos systèmes: il y a les niveaux « critique », « régulier » et « moyen ». Nous mettons en place les mesures nécessaires pour assurer la disponibilité.

M. Michel Picard: Je vous remercie.

Le président: Monsieur Paul-Hus, vous avez cinq minutes.

M. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, PCC): Merci, monsieur le président.

Ma première question s'adresse aux représentants de Tawich Development Corporation.

Nous avons fait un peu de recherche à votre sujet. Nous avons constaté que vous êtes allés en Chine, récemment, et que vous avez des photos de votre rencontre avec les gens d'Alibaba.

Pouvez-vous nous dire si des ententes ont été conclues avec eux? Si oui, de quel type sont-elles?

M. Jean Fernand Schiettekatte: Les gens d'Alibaba cherchent à ouvrir des centres de données au Canada. Ils désirent avoir des centres de données qui correspondent aux standards canadiens. En fait, ce sont toutes les transactions entre l'Asie et le Canada qui pourraient passer par une fibre nordique. Cela rend la chose intéressante, parce que cela réduit le temps de latence. Actuellement, Alibaba a ouvert plusieurs centres de données aux États-Unis.

M. Pierre Paul-Hus: Sur la photo, on voit la nation crie signer une entente avec les Chinois, je crois. Avez-vous signé un protocole d'entente déjà?

M. Jean Fernand Schiettekatte: Nous avons conclu des ententes, mais elles ne portent pas sur des centres de données. Nous importons du matériel de sécurité pour les mines, des chandails et des choses comme cela.

M. Pierre Paul-Hus: Il n'y a rien de technologique.

M. Jean Fernand Schiettekatte: Non.

M. Pierre Paul-Hus: D'accord.

L'entreprise serait établie au Québec. Avez-vous évalué les retombées économiques pour le Canada ou pour le Québec du projet que vous voulez réaliser?

M. Jean Fernand Schiettekatte: Nous avons commencé le processus de discussion en vue d'une étude de préfaisabilité, où les retombées économiques seront mieux chiffrées. Nous pensons que les centres de traitement de données bancaires qui viendraient s'installer dans le Nord du Québec généreraient de grandes retombées économiques pour le Québec.

M. Pierre Paul-Hus: Dans le Nord, il y a déjà le Système d'alerte du Nord, dont la portion canadienne est prise en charge par la Défense nationale, dans le cadre du NORAD. Le lien de télécommunication par fibre optique proposé serait-il relié aux 47 stations radars déjà établies?

M. Jean Fernand Schiettekatte: C'est un point très intéressant. Je ne l'ai pas mentionné dans notre présentation, qui traite davantage des Premières Nations, mais, effectivement, il serait important de relier les bases militaires canadiennes à ce lien. C'est un aspect qui pourrait être considéré.

M. Scheer veut assurer la sécurité et la représentation du Canada dans le Grand Nord, et nous pensons que cette fibre optique est l'un des outils qui permettraient de le faire.

M. Pierre Paul-Hus: Parfait, je vous remercie.

Monsieur Jarry, lorsqu'on parle de l'Internet des objets, on parle aussi de la chaîne d'approvisionnement. Mon collègue a posé une question sur la vérification des appareils qui sont achetés. Que pensez-vous de l'entreprise chinoise Huawei?

M. Luc Jarry: Ce qui est un peu surprenant, au sujet de Huawei, c'est qu'elle fait affaire avec Bell Canada depuis longtemps. On se pose maintenant des questions, surtout parce qu'on a des préoccupations liées à la sécurité et à l'espionnage. Je trouve surprenant qu'une entreprise comme Bell Canada fasse affaire depuis plusieurs années déjà avec Huawei alors que d'autres entreprises ont simplement reculé.

M. Pierre Paul-Hus: Est-ce le déploiement du réseau 5G qui est problématique? Les anciens appareils étaient différents. Les nouveaux appareils et la technologie 5G peuvent-ils avoir un impact différent?

M. Luc Jarry: Je suis un retraité de Bell Canada et j'y ai travaillé plusieurs années, mais je n'ai pas participé directement à ce projet. Je peux dire cependant que nous avions des inquiétudes relativement à la sécurité; je parle ici d'espionnage. J'ai été surpris d'apprendre cela.

● (1620)

M. Pierre Paul-Hus: D'accord.

Concernant l'Internet des objets, vous avez parlé de différents contrôles à distance sur des objets. Il s'en trouve sûrement parmi nous qui ont des serrures électroniques contrôlées à distance. Ces objets sont contrôlés par un système domotique résidentiel. L'équipement peut-il être programmé au moment de son installation et être contrôlé plus tard, ou faut-il obligatoirement contrôler le système domotique pour contrôler l'objet?

M. Luc Jarry: L'un des principaux problèmes que pose l'Internet des objets a trait à la cybersécurité. Lors de la conception et de la fabrication de la plupart des objets qu'on veut connecter à Internet, l'aspect de la cybersécurité n'est pas pris en compte. D'ailleurs, l'une de mes recommandations que j'ai formulées au Comité est justement de voir à cet aspect une fois pour toutes. Maintenant, on doit tenir compte de la cybersécurité lorsqu'on connecte un appareil.

N'oublions pas que les systèmes domotiques ne sont pas nouveaux. Comme je l'ai mentionné, on investit dans ce domaine depuis 15 ou 20 ans. Par contre, ces systèmes étaient sur des réseaux fermés. Maintenant, avec l'intelligence artificielle, on sera capable de prévenir des bris de machinerie dans des usines.

On a parlé tantôt de disponibilité des systèmes chez Cascades. On va pouvoir faire fonctionner les systèmes 24 heures sur 24, 7 jours sur 7, 365 jours par année. On peut prévenir les bris de machinerie à l'aide de l'intelligence artificielle. Maintenant, pour bénéficier de cela, il faut connecter tous les équipements.

N'oublions pas que la majorité des cyberattaques que nous avons subies au Canada et qu'il y a eu partout dans le monde concernaient l'information et les dénis de service. À mesure que l'on connecte des objets, cela devient physique. Maintenant, la question qu'on doit se poser sur le plan de la sécurité est si cela fera partie de l'arsenal militaire des pays.

[*Traduction*]

Le président: Merci.

Madame Sahota, vous avez cinq minutes.

Mme Ruby Sahota (Brampton-Nord, Lib.): Je cède mon temps de parole à M. Graham.

[*Français*]

M. David de Burgh Graham: Je vais revenir sur ce qui s'est dit plus tôt au sujet de l'attaque subie par WhatsApp qui a été annoncée hier. Selon les analyses dont nous avons pris connaissance jusqu'à maintenant, il semblerait que des acteurs en lien avec des États soient à l'origine de cette attaque et que le secteur des droits de la personne ait été ciblé.

Selon vous, les plus grandes menaces en matière de cybersécurité viennent-elles du secteur privé ou d'acteurs liés à des gouvernements, à l'échelle mondiale?

M. Luc Jarry: Vous parlez des vulnérabilités?

M. David de Burgh Graham: Je parle de l'exploitation des vulnérabilités.

M. Luc Jarry: À mon avis, un des problèmes concernant la gestion des incidents de sécurité est que les entreprises commencent à communiquer davantage ce genre d'information. Je crois que c'est encore un peu tôt.

Pour répondre à votre question, je pense que c'est un peu de tout présentement.

M. David de Burgh Graham: Les attaques liées à des États existent et sont assez graves, même si ce ne sont pas les seules. Que pensez-vous du projet KesKuun, dont les autres témoins ont parlé?

M. Luc Jarry: Je trouve que le projet est intéressant. Il y a un point sur lequel ils ont tout à fait raison, et c'est qu'en matière de cybersécurité, la disponibilité est très importante. À mon avis, il est important que nous conservions une souveraineté au Canada, que nous ayons nos propres fibres pour les télécommunications.

Je viens d'entendre parler de ce projet. Dans une optique de cybersécurité, je suis tout à fait favorable à ce genre de projet et d'approche.

M. David de Burgh Graham: C'est bon.

Je vais m'adresser aux autres témoins.

[*Traduction*]

Merci.

Je me tourne vers M. Gull pour parler des étapes du projet. Vous avez dit que le projet Quintillion est déjà en service en Alaska. Il est déjà construit là-bas. Quel est le processus de mise en oeuvre?

C'est en Alaska et nous tentons d'établir un réseau qui ne serait pas américain. Pouvez-vous expliquer la situation un peu plus en détail?

M. Sam Gull: Le réseau de fibre optique qui est connecté est maintenant en service. Lorsque le lien sera construit vers le Japon et vers l'Angleterre, il se trouvera dans les eaux internationales. Deux canalisations seront à l'extérieur des États-Unis. Ce sont ces deux canalisations, dans les eaux internationales, qui nous intéressent. Les États-Unis n'y seront pas connectés.

M. David de Burgh Graham: Savez-vous quand Quintillion prévoit terminer la construction de la troisième phase?

M. Sam Gull: Tout dépendra des hivers canadiens. Le passage du Nord-Ouest connaît toujours des périodes de gel. Les responsables du projet s'inquiètent aussi du moment où installer la ligne dans ce passage. C'est pourquoi ce sera la dernière phase. Les eaux sont très peu profondes à certains endroits, sans oublier la présence d'icebergs. Il faut vraiment prendre le temps de faire des études sur cette partie du projet.

● (1625)

M. David de Burgh Graham: Vous avez parlé de connecter le Canada à la ligne Quintillion en passant par la baie James afin d'avoir un réseau pleinement souverain. Y a-t-il une façon de connecter les côtes Ouest et Est également? Pouvons-nous en faire un réseau national plutôt qu'exclusivement international? Avez-vous quelque chose à dire sur le sujet?

M. Jean Fernand Schiettekatte: Oui, ce serait possible.

Il y a un projet de ligne jusqu'à Yellowknife. Elle pourrait desservir ces régions aussi. C'est pourquoi nous recommandons d'établir une équipe canadienne pour développer ce projet dans le Nord. À mon avis, ce devrait être une recommandation du Comité.

M. David de Burgh Graham: Il est prioritaire de connecter le Canada à cette ligne.

M. Jean Fernand Schiettekatte: Oui. La priorité de Tawich est sans conteste le développement du Nord du Québec.

M. David de Burgh Graham: Je dois vous dire que la priorité du Comité est la cybersécurité. Dans ce contexte, il est fascinant d'avoir cette solution. De plus, elle est présentée par la Première Nation crie. C'est extrêmement intéressant pour nous tous.

Je crois qu'il ne me reste que quelques secondes.

Le président: Pour laisser du temps à M. Eglinski, il vous faudra être très bref.

M. David de Burgh Graham: Je vais poser une dernière question à M. Jarry, puis je céderai la parole à M. Eglinski. Je veux parler de la sécurité intégrée à la conception.

M. Luc Jarry: Quelle est mon opinion de la sécurité intégrée à la conception?

M. David de Burgh Graham: Oui.

M. Luc Jarry: Combien de minutes ai-je pour répondre?

Le président: En fait, le temps est écoulé.

C'est une excellente question. Nous devrons chercher la réponse plus tard.

Passons maintenant à M. Eglinski qui dispose des cinq dernières minutes.

M. Jim Eglinski (Yellowhead, PCC): Merci.

Je tiens à remercier les témoins d'être ici aujourd'hui.

Je vais d'abord parler de la ligne que vous proposez. Elle traverse l'Extrême-Arctique et rejoint la Chine. Elle passe au Japon? D'accord.

Pourquoi passer par l'Arctique? Pourquoi ne pas avoir traversé le bas de la baie d'Hudson et le Canada? On a beaucoup parlé d'un corridor de transport le long des provinces du Nord et au sud des Territoires du Nord-Ouest. La ligne pourrait passer à cet endroit. Le choix d'aller vers l'Arctique me semble beaucoup plus complexe que de partir du bas de l'Alaska et de suivre les îles Aléoutiennes. C'est la même chose pour le lien vers l'Europe.

Y avait-il une raison qui justifiait le choix d'un tracé beaucoup plus au nord?

M. Jean Fernand Schiettekatte: Il y avait une raison. Elle devient évidente à bord d'un avion. Tous les vols en provenance de Toronto ou de Montréal vers l'Asie passent par le Nord. La distance est plus courte en passant par le Nord que par le Sud du Canada. C'est ce qui permet de réduire les temps de latence. Il y a une raison d'ordre technique qui est associée à l'analyse de rentabilisation. C'est ainsi qu'on attire des investissements des institutions financières.

C'était la première raison. La deuxième repose évidemment sur le fait que nous nous trouvons dans le Nord. Nous défendons donc le développement de cette région. C'est le mandat de Tawich. C'est dans notre intérêt, mais également dans celui des Canadiens en général, d'autant plus que nos voisins américains souhaitent exercer une souveraineté sur le Nord, comme il a été rapporté dans les médias.

Il est crucial de comprendre que l'établissement de cette ligne entraînerait des développements importants dans le Nord canadien. Si on n'occupe pas le territoire, on risque de perdre la souveraineté sur celui-ci.

M. Jim Eglinski: Je suis heureux d'entendre de tels propos de la part du milieu des affaires. C'est effectivement un sujet de préoccupations. Notre caucus tient à ce que la souveraineté sur le Nord soit protégée. Merci d'en tenir compte dans votre stratégie.

Vous avez parlé de l'électricité dont vous avez besoin. Je lis que 300 ou 200 mégawatts seront nécessaires. Est-ce pour alimenter l'ensemble de la ligne ou faudra-t-il plus d'électricité au fil du temps? Nous parlons d'une grande distance, de votre région du pays jusqu'à l'extrémité nord.

M. Sam Gull: L'électricité provenant des barrages de la Grande Rivière servirait surtout à l'alimentation des centres de données. Ce sont les centres de données qui, en raison de leur taille, consomment beaucoup d'énergie. On atteint rapidement les 200 mégawatts dans ce secteur. C'est aussi notre cas même si, dans le Nord, nous disposons de nombreux systèmes de refroidissement naturel, ce qui réduit les coûts d'exploitation. J'ai visité des centres de données dans la Silicon Valley. Leur principal problème est le coût associé au refroidissement des ordinateurs.

● (1630)

M. Jim Eglinski: À la lumière de vos propos, je comprends que les centres de données seront situés sur vos terres territoriales traditionnelles et qu'ils transmettront les données au Canada et ailleurs.

M. Sam Gull: Oui.

M. Jean Fernand Schiettekatte: La réponse à votre question est oui. C'est pourquoi il y aura une possibilité de connecter des communautés éloignées qui fourniront de l'électricité pour alimenter les répéteurs. On a établi un plan selon lequel quelques communautés alimentent la ligne dans le Nord canadien. C'est une façon de prévoir l'alimentation. Une base militaire pourrait aussi être responsable de la distribution. C'est un projet très intéressant.

M. Jim Eglinski: Merci.

Monsieur Jarry, selon votre expérience professionnelle, pensez-vous que les simples utilisateurs des services Internet peuvent se protéger adéquatement? Existe-t-il des logiciels sur le marché qui permettent de protéger son domicile ou ne sont-ils que des produits illusoires qui ne seront probablement pas à la hauteur?

M. Luc Jarry: La sécurité repose sur deux principaux aspects: la formation et la sensibilisation. J'ai parlé plus tôt du fait que beaucoup de gens acceptent des ententes de confidentialité sans en lire les modalités.

En ce qui concerne votre question précisément, il est tout à fait possible d'améliorer la sécurité à son domicile. Est-ce à dire que ces outils sont infaillibles à 100 %? C'est un peu comme lorsqu'on conduit une voiture. Le fait de porter sa ceinture de sécurité, d'avoir des freins ABS et d'activer les nombreux systèmes de sécurité préviendra probablement les blessures en cas d'accident. Risque-t-on toujours d'avoir un accident? La réponse est oui.

M. Jim Eglinski: La sécurité dépend de la qualité du service offert aux Canadiens. Nous savons que, dans certaines régions, le service est terrible ou pratiquement pourri. Ailleurs au pays, il est excellent.

Le président: Merci, monsieur Eglinski.

Avant de vous laisser partir, j'aimerais vous poser une question: d'où provient l'argent qui finance le projet Quintillion?

M. Jean Fernand Schiettekatte: Selon l'information dont nous disposons — nous ne connaissons pas les responsables —, c'est une entreprise américaine qui appuie le projet.

Le président: Nous parlons donc d'argent américain et d'une entreprise américaine...

M. Jean Fernand Schiettekatte: Oui.

Le président: ... et ce sera un projet qui nous permettra de ne pas passer par les États-Unis.

M. Jean Fernand Schiettekatte: Oui. C'est pourquoi nous aimerions qu'une équipe canadienne soit formée. La communauté crie a une partie des fonds nécessaires, mais elle ne peut pas y arriver seule.

Le président: Une entité canadienne, que ce soit vous, un autre organisme ou un partenariat, serait-elle propriétaire de la ligne dans la baie James et la baie d'Hudson jusqu'au point de connexion ou jusqu'en Alaska?

M. Jean Fernand Schiettekatte: Nous aimerions être propriétaires de la ligne jusqu'en Alaska et jusqu'en Europe. En gros, nous voudrions détenir la troisième phase.

Le président: Quelle est l'importance de se trouver dans les eaux internationales plutôt que nationales? Vous savez que le passage du Nord-Ouest fait l'objet d'un différend. Le Canada considère que le passage est une voie interne. M. Pompeo est d'avis qu'il fait partie des eaux internationales. Quelles seraient les répercussions d'un statut national ou international du passage sur votre projet?

M. Jean Fernand Schiettekatte: Il s'agit principalement de ne pas être soumis à la Patriot Act et à toutes les lois qui en découlent. Il est préférable d'être hors de la portée de la NSA. À mon avis, les Canadiens devraient être au courant de cette préoccupation. Je pense à l'une des questions posées à M. Jarry. On lui a demandé qui se livre à des activités d'espionnage. C'est une excellente question.

Le président: Enfin, votre projet est-il soumis à un examen de la sécurité canadien?

M. Jean Fernand Schiettekatte: Il le serait, oui.

Le président: Un tel examen a-t-il été lancé?

M. Jean Fernand Schiettekatte: Non. Nous en sommes encore à l'étape de l'étude. En cherchant dans Internet, on trouvera très peu d'information sur ce que nous faisons. C'est la première fois que nous en parlons publiquement. Nous avons eu quelques conversations avec des intervenants, mais il reste beaucoup de travail à faire.

Le président: Merci de votre réponse.

Je suis désolé de devoir maintenant interrompre cette discussion très intéressante et très éclairante. Nous allons suspendre nos travaux. Je tiens encore une fois à vous remercier de votre témoignage devant le Comité.

Nous allons suspendre la séance quelques instants avant de poursuivre à huis clos. Merci.

[*La séance se poursuit à huis clos.*]