CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 149 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le mercredi 20 février 2019

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le mercredi 20 février 2019

● (1535)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Chers collègues, il semble que nous ayons le quorum. Nous aurons des contraintes de temps. Nous serons probablement interrompus par des votes.

Je tiens à présenter mes excuses à l'avance à nos témoins. Nous nous efforcerons de procéder dans l'ordre et de gagner du temps dans la mesure du possible.

Normalement, nous accordons jusqu'à 10 minutes aux témoins pour lire leur déclaration, puis nous passons aux questions des membres du Comité.

Je n'ai pas eu la chance d'en parler à tous mes collègues, mais je propose que les déclarations, telles que préparées et soumises, soient considérées comme lues et consignées au compte rendu. Les témoins se contenteraient de les résumer au lieu de les lire en entier, après quoi nous passerions aux questions, tout cela pour gagner du temps.

Cela vous convient-il, chers collègues?

Monsieur Picard.

M. Michel Picard (Montarville, Lib.): Je pense que c'est une très bonne suggestion.

Je propose que nous leur demandions de s'en tenir à un sujet principal de leur choix.

Le président: C'est cela.

Je ne crois pas avoir donné mon coup de maillet, comme j'aurais dû. Je m'excuse.

M. Michel Picard: Considérez-le comme donné.

Le président: Disons que le coup de maillet a été donné et que les déclarations ont été lues.

[*Voir l'Annexe —Remarques de la professeure Jill Slay*]

[*Voir l'Annexe— Remarques du professeur Yuval Shavitt*]

Le président: Madame Slay, puisque vous êtes le témoin le plus vulnérable à la technologie, je pourrais peut-être vous demander d'abord, si vous le voulez bien, de résumer votre déclaration.

Je demanderai ensuite à M. Shavitt de résumer la sienne, après quoi nous passerons directement aux questions.

Si vous n'y voyez pas d'inconvénient, nous avons hâte d'entendre ce que vous avez à dire.

Mme Jill Slay (professeure, présidente de la cybersécurité La Trobe Optus, La Trobe University, Melbourne, à titre personnel): Merci beaucoup.

Je viens de rédiger un document qui examine les principaux défis en matière de cybersécurité. J'ai étendu ma réflexion au-delà des aspects techniques pour relever ceux qui, à mon avis, sont importants pour nos deux gouvernements.

Comme je vous l'ai expliqué, il faut se faire une idée claire des cybermenaces. Le diagramme en forme de fleur que je vous ai fourni décrit les divers vecteurs d'attaque. Il en ressort que la cybersécurité et les cybermenaces ne s'inscrivent pas dans la compréhension traditionnelle de la technologie, de la sécurité des réseaux informatiques, mais couvrent aussi des questions comme le droit, les politiques et l'administration. Par conséquent, lorsque nous examinons la cybersécurité comme un tout, nous devons harmoniser tous ces éléments.

Une question qui m'occupe en Australie depuis des années, c'est le fait de considérer que la cybersécurité fait partie de la sécurité nationale. Très souvent, ceux d'entre nous qui sont considérés comme des experts en la matière viennent de milieux techniques où on les a félicités et où on leur a accordé des fonds pour des travaux de recherche technique dans des créneaux particuliers, mais les universitaires sont réticents à considérer leurs travaux comme faisant partie de la sécurité nationale. Quelque part dans le cadre du mécanisme d'élaboration des politiques du gouvernement, des ministères relevant du premier ministre et des ministères qui s'occupent des questions plus secrètes touchant à la cybersécurité, il y a lieu d'harmoniser le travail des informaticiens et celui des organismes chargés de la sécurité nationale.

L'autre question que j'ai soulevée et sur laquelle je travaille évidemment en Australie depuis des années, c'est que plus le besoin de s'occuper de la cybersécurité dans le cadre de la sécurité nationale se fait sentir, plus il importe pour des pays et alliés comme nous de définir ce qu'est un praticien de la cybersécurité. Nous devons être en mesure de répondre à la question suivante: qui est expert dans ce domaine?

En Australie, nous avons travaillé depuis deux ou trois ans à l'élaboration d'une norme nationale, de normes professionnelles en matière de cybersécurité, afin de pouvoir répondre à la question de savoir qui est un professionnel de la cybersécurité et qui est un technicien en cybersécurité. Cela facilite beaucoup les questions relatives au milieu de travail, aux ressources humaines et à l'emploi dans la fonction publique, car notre discipline s'est pour ainsi dire développée comme un art plutôt que comme une science.

J'ai indiqué le genre de travail que nous avons fait pour élaborer des normes professionnelles nationales.

La dernière chose que je voulais dire, c'est que dans tous nos pays, nous aurons un financement limité pour la recherche, la formation, l'harmonisation de la cybersécurité avec la sécurité nationale. Nous avons chacun des cohortes de chercheurs extrêmement compétents dans des domaines comme l'intelligence artificielle, l'apprentissage automatique pour la cybersécurité et la sécurité de l'Internet des objets, mais très souvent, l'universitaire que je suis constate que les programmes de recherche et d'enseignement ne cadrent pas avec le programme de sécurité nationale.

Je peux faire une merveilleuse étude publiable, mais dans un environnement restreint. Il est parfois très difficile de savoir ce que le gouvernement pourrait faire des résultats de mes recherches. D'un point de vue stratégique, il est essentiel d'harmoniser les politiques de financement de la recherche et de l'éducation avec les politiques de sécurité nationale, l'environnement de la sécurité nationale, si nous voulons financer des travaux vraiment importants pour le pays.

Je vais m'arrêter là.

● (1540)

Le président: Je vous remercie.

Je vais donner la parole à M. Shavitt.

M. Yuval Shavitt (professeur, Tel Aviv University, à titre personnel): Merci.

Je suis professeur à l'Université de Tel-Aviv. Je suis également membre du Blavatnik Interdisciplinary Cyber Research Center. À cet égard, je suis tout à fait d'accord avec la professeure Slay pour dire que la cybersécurité n'est pas seulement une question de technologie, mais aussi un problème interdisciplinaire.

Il y a d'autres aspects, dont les aspects juridiques et sociaux, et nous faisons donc de la recherche interdisciplinaire dans notre centre. Je suis également le directeur technique d'une entreprise appelée BGProtect, et cela est lié à ce dont je vais parler.

J'étudie le routage Internet depuis plus de deux décennies. Il y a une quinzaine d'années, j'ai lancé un projet universitaire appelé DIMES, dans le cadre duquel, à l'aide de bénévoles, nous avons suivi le routage Internet partout dans le monde. Au plus fort du projet, nous avions 1 500 agents logiciels qui fonctionnaient sur des machines de volontaires dans une quarantaine de pays, ce qui nous a permis de nous faire une idée très claire de la façon dont le routage Internet se comporte.

Il y a environ quatre ans, forts de toute cette expertise, nous avons lancé BGProtect, une entreprise qui veut aider le gouvernement et les institutions internationales à renforcer leur sécurité en surveillant l'acheminement vers leurs réseaux en fonction de leurs craintes. Le routage Internet est un protocole distribué appelé BGP, qui sert à dire à tout le monde où trouver les serveurs ou les clients sur Internet. Toutefois, lorsqu'il a été conçu il y a plusieurs décennies, le réseau Internet n'avait pas du tout la même envergure et on lui faisait entièrement confiance. Personne ne songeait à la sécurité.

Il y a une dizaine d'années, un nouveau type d'attaque a fait son apparition: l'attaque par détournement du protocole Internet. Il s'agit essentiellement d'intercepter le trafic entre deux points et de le forcer à passer par votre propre réseau. Cette interception d'origine humaine ou « attaque de l'homme au milieu » se déploie à grande échelle et permet de faire beaucoup de choses. Bien sûr, si tout le trafic passe par vous, vous pouvez faire de l'espionnage, ou vous pouvez faire ce que nous appelons des attaques de déclassement ou encore introduire des chevaux de Troie dans les réseaux. Vous pouvez pénétrer les réseaux. Il y a de nombreux types d'attaques. C'est pourquoi c'est si dangereux. Nous avons vu ces attaques se multiplier au fil des ans, surtout ces derniers temps.

Nous sommes ici pour examiner ces attaques. En ma qualité de professeur d'université, je fais des recherches et j'ai publié un article à ce sujet. Je le fais aussi comme entreprise.

Or, si nous examinons ces attaques, nous constatons qu'elles ne sont pas simples et qu'elles ne sont donc pas l'ouvrage de pirates adolescents. Ce sont des organismes gouvernementaux et de grandes organisations criminelles qui en sont les auteurs, et il faut comprendre que ce n'est pas une dichotomie. Il y a des gouvernements qui font appel à des organismes non gouvernementaux, parfois, même à des organisations criminelles, pour faire le genre de travail dont ils veulent se distancer. Songez au secteur financier. Il est particulièrement ciblé par les gouvernements et, bien sûr, par les organisations criminelles.

Que peut-on faire? Une chose, bien sûr, c'est de surveiller le trafic pour s'assurer que l'information n'ira pas aboutir là où il ne faut pas. C'est évident. C'est quelque chose que nous faisons dans notre entreprise.

Autre chose — et c'est ce que nous faisons aussi en Israël — c'est d'établir des CERT. Les CERT sont ce que les Américains appellent des centres de fusion. Ce sont des organisations où, pour les besoins de gouvernance des secteurs financiers, les banques peuvent partager, à divers degrés d'anonymat, des données sur les attaques dont elles sont témoins. Ces données peuvent être redistribuées — il y a plusieurs niveaux de distribution — à d'autres organisations financières, de sorte que lorsqu'il y a une attaque, comme un nouveau virus, un nouveau détournement ou autre, les données peuvent être transmises rapidement à tous les participants du CERT afin de les préparer à l'attaque imminente. C'est très important. Nous le faisons en Israël. Nous avons un CERT national et des CERT sectoriels.

Enfin, je ne peux passer sous silence le débat au Canada, au Royaume-Uni et dans le reste du monde occidental au sujet des fabricants de matériel. Nous savons, d'après le rapport Snowden, que de nombreuses entreprises américaines collaboraient avec le gouvernement des États-Unis pour obtenir de l'information à partir des données qui étaient échangées.

● (1545)

Il n'y a aucune raison de croire que cela ne se passe qu'aux États-Unis. C'est sûrement encore plus fréquent dans les pays non démocratiques, si j'ose dire.

Le matériel peut être conçu avec des vecteurs, des mécanismes susceptibles de détourner le trafic de ce qui semble se produire selon le protocole de routage, donc vous devez surveiller ce type de matériel en particulier, c'est-à-dire toutes sortes d'équipements de télécommunications, mais surtout les routeurs. Pour ce faire, il ne suffit pas d'examiner le protocole d'acheminement, car ici, le détournement se fait non pas par le protocole d'acheminement, mais par le matériel lui-même. Il faut une surveillance active.

C'est ce que nous faisons. Nous avons constaté une augmentation de ces attaques au cours des deux dernières années. Il est important de ne pas se limiter au protocole BGP, mais aussi d'examiner le niveau des données et la destination des paquets, surtout si on ne fait pas confiance à son fabricant de matériel.

Le président: Merci, monsieur Shavitt.

Madame Damoff, vous avez sept minutes.

Mme Pam Damoff (Oakville-Nord—Burlington, Lib.): Merci, monsieur le président. Je partage mon temps avec M. Spengemann.

Je vous remercie tous les deux de vos exposés.

Mon temps est limité, monsieur Shavitt, et j'ai quelques questions au sujet d'un article que vous avez écrit au sujet de China Telecom, dans lequel vous dites que nous détournons le trafic Internet par l'entremise de ces points de présence. Comment ces choses sont-elles établies? Comment cela se passe-t-il? Qui les réglemente, ou est-il seulement possible de les réglementer? Y a-t-il quelque chose que le gouvernement peut faire pour mettre en place une réglementation ou une structure pour empêcher que cela se produise?

● (1550)

M. Yuval Shavitt: Il y a un problème de réglementation aux États-Unis et aussi au Canada, je crois. Si l'Israélien que je suis essayait d'acheter une compagnie de téléphone au Canada, je suis sûr que je ne pourrais pas le faire, mais si je voulais acheter un fournisseur de télécommunications, un FSI, je le pourrais. Pour une raison ou une autre, on ne s'est pas occupé du volet communication des données parce que, traditionnellement, c'était le terrain de jeu de farfelus. Or, il s'agit d'une infrastructure vraiment essentielle, et il faut modifier la réglementation pour déterminer qui peut être propriétaire de ce type d'infrastructure dans votre propre pays.

En général, de nombreuses entreprises Internet, de nombreux fournisseurs de services Internet, sont disséminés dans le monde entier. Il y a des entreprises russes ici et il y a des entreprises canadiennes... peut-être pas canadiennes, mais il y a des entreprises américaines en Russie. Il y a Telia, une entreprise suédoise, partout dans le monde. Ça se fait.

Il y a un pays — la Chine — qui ne permet pas aux joueurs étrangers d'établir des communications sur son propre territoire, alors je ne vois pas pourquoi le Canada et les États-Unis permettraient aux Chinois d'avoir une infrastructure de communication qui les aide à mener ce genre d'attaques sur leur territoire.

Mme Pam Damoff: Quel genre de lois avez-vous en Israël? Ou y a-t-il d'autres pays qui ont des pratiques exemplaires auxquelles Israël adhère?

M. Yuval Shavitt: Je pense qu'Israël est presque comme la Chine à cet égard. Je ne pense pas qu'une entité non israélienne puisse avoir une infrastructure de télécommunications au pays.

Mme Pam Damoff: Y a-t-il d'autres pays à part Israël et la Chine qui sont dans cette situation?

M. Yuval Shavitt: Je ne connais pas la loi dans ses menus détails...

Mme Pam Damoff: Ça va.

M. Yuval Shavitt: ... mais le vrai problème ici, c'est la symétrie. C'est pourquoi nous pointons la Chine du doigt, non pas parce que les Chinois sont les soi-disant méchants et non pas parce qu'ils le font plus que d'autres pays, mais parce qu'il y a un manque de symétrie. Si les Chinois ne permettent pas aux pays démocratiques d'avoir de l'équipement ou des points de présence dans leur pays, en quel honneur devraient-ils être autorisés à en avoir chez nous?

Mme Pam Damoff: Merci.

Sven, je vous cède la parole.

M. Sven Spengemann (Mississauga—Lakeshore, Lib.): Merci beaucoup.

Merci à tous deux de votre présence.

Madame Slay, je vous suis reconnaissant d'être parmi nous malgré le décalage horaire avec Melbourne.

Je veux poursuivre sur le thème dont j'ai parlé à certains de nos témoins précédents, à savoir l'environnement que nous voulons créer au Canada et que nous créons pour aider les petites entreprises à démarrer. De nombreuses petites entreprises sont impliquées dans des secteurs d'activité fortement axés sur les données. Certaines se consacrent directement au développement de logiciels et d'autres encore plus directement au développement de questions touchant les marchés publics liés à la défense et aux logiciels.

Dans quelle mesure les petites entreprises sont-elles particulièrement vulnérables dans le domaine cybernétique? Dans quelle mesure les questions de sécurité constituent-elles en fait un obstacle à l'entrée sur le marché? Y a-t-il des leçons de compétence ou des pratiques exemplaires dont vous pourriez nous parler en Israël, en Australie ou dans les autres régions que vous étudiez?

Mme Jill Slay: Voulez-vous que je réponde?

M. Sven Spengemann: Bien sûr. Vous pouvez le faire tous les deux, à tour de rôle.

Madame Slay, si vous voulez bien commencer, allez-y.

Mme Jill Slay: Puis-je revenir à la question précédente? L'Australie vient de présenter un projet de loi visant à contrôler la propriété étrangère de toutes les infrastructures essentielles et à réglementer même, par exemple, les universités et leurs partenariats à l'étranger. Le problème est devenu énorme, et il vaudrait la peine que vous examiniez la situation actuelle en Australie, étant donné que nous faisons tous les deux partie du Groupe des cinq.

Nous ne sommes pas tout à fait comme Israël, mais nous avons essayé de régler les problèmes que nous croyons avoir causés nous-mêmes en faisant abstraction du danger de la propriété étrangère.

Si vous regardez cela du point de vue des petites et moyennes entreprises...

M. Sven Spengemann: La cybersécurité constitue-t-elle un obstacle concret à l'entrée sur le marché?

Mme Jill Slay: Je le crois, oui. Le gouvernement a lancé une initiative de cybersécurité en 2016, mais elle visait surtout les grandes sociétés. Avec la nouvelle politique du Parti travailliste et les élections générales qui s'annoncent, on met davantage l'accent sur les besoins des petites entreprises en matière de cybersécurité. Compte tenu de la pénurie de main-d'oeuvre qualifiée sur le marché, des salaires élevés des professionnels de la cybersécurité et du fait que, je crois, l'Australie compte environ 60 à 70 % de petites et moyennes entreprises, ces entreprises pâtissent parce qu'elles obtiennent habituellement des services généraux de TI ou de TIC. Dans bien des cas, on ne comprend même pas la nécessité de se procurer la cybersécurité comme service.

Mais si vous regardez l'envers du décor, du point de vue financier, il y a eu un investissement énorme en Australie avec les centres de cybercroissance du ministère de l'Industrie, des noeuds de cybercroissance dans un réseau, ce qui a en partie permis de renforcer la position nationale en matière de cybersécurité en créant des incitatifs pour attirer les petits joueurs sur le marché. Il y aura beaucoup de très petits joueurs, disons à Canberra, où des gens qui ont pris leur retraite de la fonction publique et qui ont des compétences en cybersécurité mettent sur pied de petites entreprises et développent des produits-créneaux, du matériel et des logiciels spécialisés, ce que le gouvernement est en fait en train d'encourager avec de nombreux incitatifs.

Ces mesures ont connu beaucoup de succès, mais le gouvernement fédéral y a consacré énormément d'argent.

● (1555)

M. Sven Spengemann: C'est vraiment utile.

Mme Jill Slay: Je vais donc essayer...

M. Sven Spengemann: Je vais vous interrompre parce qu'il reste moins d'une minute et je veux entendre M. Shavitt.

On peut donc affirmer qu'un bien commun public est en train d'être créé en Australie, et qu'il aide à ouvrir l'accès aux marchés?

Mme Jill Slay: Oui.

Le président: Malheureusement, monsieur Spengemann, votre temps est écoulé.

M. Sven Spengemann: Je pensais en avoir un peu plus.

Merci, monsieur le président.

Le président: C'était sept minutes.

Monsieur Motz, vous avez la parole pour sept minutes.

Que mes collègues veuillent bien m'excuser, mais si je suis impitoyable, c'est que le temps presse à cause du vote.

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

Messieurs, je vous remercie de votre présence.

Ma collègue, Mme Damoff, a parlé du changement de routage du trafic Internet. J'aimerais vous demander si connaissez des mesures de cyberdéfense, dans vos pays respectifs, susceptibles de dissuader des pays comme la Chine de changer le routage du trafic Internet.

M. Yuval Shavitt: La dissuasion n'est pas une chose facile. L'attribution constitue un problème majeur dans l'univers de la cybersécurité. Pour celui qui commet des attaques, le risque d'être identifié est faible ou inexistant. S'il y a identification, la personne peut toujours prétendre qu'il s'agit d'une erreur de configuration ou d'un incident du genre. Il est très difficile de démontrer qu'il y a eu une intention malveillante. Une attaque par détournement peut être confondue avec une erreur de configuration. Pour y voir clair, on n'a d'autre choix que d'interroger la personne et de la forcer à dire la vérité.

En Israël, nous avons un programme de défense nationale pour surveiller les routes informatiques qui relient les infrastructures essentielles.

M. Glen Motz: Que se passe-t-il en Australie, madame Slay?

Mme Jill Slay: Je ne saurais vous le dire. Tout ce que je sais relève du domaine public.

M. Glen Motz: Nous avons parlé du changement de routage par la Chine et monsieur Shavitt a mentionné d'autres pays qui font la même chose. L'un des témoins pourrait-il nous dire quel genre d'information a été recueillie par ces pays? Que cherchent-ils à obtenir?

Le Comité a déjà reçu le témoignage d'un universitaire qui s'est penché sur les tentatives d'accès visant à voler de l'information gouvernementale, des éléments de propriété intellectuelle industrielle, voire des secrets gouvernementaux. Notre étude porte principalement sur le secteur financier. Je vous demande donc quel genre d'information ceux qui commettent ces actes de détournement cherchent à obtenir, selon vos recherches.

M. Yuval Shavitt: Comme je suis ingénieur, le simple fait de découvrir un cas de détournement me suffit. J'ignore ce dont s'emparent ceux qui commettent ces actes. En fait, ils prennent tout et ils décident ensuite ce qu'ils gardent et ce qu'ils jettent.

Il est important de garder à l'esprit qu'il ne s'agit pas seulement d'obtenir des renseignements. Le changement de routage permet aussi d'introduire des chevaux de Troie afin de pénétrer dans un réseau. Lorsqu'il s'agit d'obtenir des renseignements, les attaques visent souvent les institutions financières, les universités et bien sûr les installations gouvernementales et les organismes gouvernementaux.

M. Glen Motz: Madame Slay.

Mme Jill Slay: Je ne suis pas toujours au fait de la nature des attaques en Australie. L'une des principales attaques qui me viennent à l'esprit est celle du Bureau of Meteorology. Comme nous l'avons annoncé, les Chinois s'y sont infiltrés pendant au moins six mois. Il y a aussi l'Université nationale australienne et sans doute beaucoup d'autres universités. L'Université nationale australienne entretient des liens étroits avec la défense. Nous savons qu'il y a eu une brèche importante. Nous pensons que la plupart de nos universités publiques sont vulnérables. Une entreprise en démarrage du secteur des télécommunications et des satellites à Adélaïde me vient à l'esprit. Son adresse IP a été volée alors qu'elle venait à peine de démarrer. Les individus se sont infiltrés dans le système et y sont restés à couvert pendant des mois, en volant l'adresse IP.

Pour bon nombre d'entre nous qui avons des habilitations de sécurité et travaillons en collaboration avec le gouvernement, nous vivons dans un environnement où nous sommes presque forcés de supposer qu'il y a eu des brèches dans nos systèmes. Dans le milieu universitaire public, nous faisons beaucoup d'efforts pour cacher notre adresse IP — c'est ce que je fais moi-même, comme beaucoup de mes collègues.

● (1600)

M. Glen Motz: Voilà qui m'amène à une autre réflexion.

Israël et l'Australie sont considérés comme des chefs de file mondiaux en matière de cybersécurité et comme des intervenants de premier plan dans ce domaine, y compris en ce qui a trait aux questions de sécurité financière dont nous avons parlé. Pourquoi? Que faites-vous différemment dans vos pays? Quelles sont ces manières de faire dont le Comité pourrait recommander l'adoption afin de renforcer la cybersécurité et améliorer la sécurité financière des Canadiens?

M. Yuval Shavitt: À mon avis, notre compétence dans ce domaine tient entre autres à la taille de notre pays. La petite taille d'Israël permet une meilleure gestion. De plus, il y a une collaboration très étroite entre le milieu universitaire, le gouvernement et le secteur privé. Les gens naviguent entre ces trois domaines. Tantôt un universitaire assumera un rôle gouvernemental, tantôt une personne du secteur privé travaillera au gouvernement, puis retournera au privé. Il s'agit d'un écosystème intégré et dynamique.

Par ailleurs, le grand public possède une bonne connaissance du problème comparativement à ce qui se passe dans le reste du monde. Dans une optique de sécurité, nous avons un programme dans lequel on enseigne la cybersécurité aux jeunes du primaire. On leur dit d'éviter d'inscrire leur nom ou leur adresse sur Facebook, par exemple. Nous travaillons à tous les niveaux. Nous disposons d'une cyberdéfense qui gère tout cela et qui déjoue les attaques. Il semble que cela fonctionne.

M. Glen Motz: Madame Slay.

Mme Jill Slay: En Australie, nous imitons les Israéliens, je crois. Israël est notre modèle de pratiques exemplaires — Singapour l'est peut-être aussi. Nous entretenons de bonnes relations avec les Canadiens. À mon avis, il y a beaucoup de choses que vous faites aussi très bien. Je pense que la culture australienne se caractérise entre autres par une tendance à la camaraderie. Entre professeurs, fonctionnaires, militaires ou gens du secteur bancaire, nous nous connaissons tous les uns les autres. Ainsi, en plus des mécanismes de communication officiels, nous avons aussi des mécanismes de communication officieux.

En ce qui me concerne, par exemple, j'ai formé des milliers de personnes au PICTL et des milliers d'autres par ailleurs. La plupart de ces personnes obtiennent par la suite des postes de cadres supérieurs à mi-carrière en Australie. Ainsi se crée un vaste réseau d'échange d'idées dans les domaines de la recherche et de la commercialisation. Voilà qui représente tout à fait l'esprit australien. En fait, je ne vois pas pourquoi ce ne serait pas aussi constitutif de l'esprit canadien.

Le président: Merci, monsieur Motz.

Étant marié à une Australienne, je me suis toujours demandé ce qu'était l'esprit australien.

Des voix: Oh, oh!

Le président: Monsieur Dubé, vous avez sept minutes.

M. Matthew Dubé (Beloeil—Chambly, NPD): Merci, monsieur le président, et merci à vous deux d'être ici.

Monsieur Shavitt, j'aimerais commencer par vous.

Je voudrais examiner certains éléments ayant trait à la localisation du trafic Internet.

Le premier élément concerne la compétence qui s'applique à la protection des données qui sont acheminées de manière légale vers une autre région du monde en raison du fonctionnement d'une entreprise ou d'un accord de libre-échange. Comme je viens de la région de Montréal, un exemple me vient à l'esprit: en raison de l'abondance d'hydroélectricité et du faible coût de l'énergie, certaines entreprises — Amazon, Google et autres — installent des serveurs au Québec.

Je ne veux pas trop digresser, mais je dirai ceci: l'autre jour, je lisais un article intéressant dans lequel on expliquait que, selon l'endroit où l'on se trouve, la musique en continu a une plus grande incidence sur les émissions de gaz à effet de serre qu'on pourrait le penser. Il y a beaucoup de faits intéressants au sujet de l'emplacement des serveurs.

La question que je souhaite vous poser va dans ce sens. Craint-on que les données, dans le cadre des mécanismes juridiques existants, traversent des régions du monde que les gens ne connaissent pas forcément très bien, des endroits qui présentent des risques pour la protection de la vie privée, entre autres? Par exemple, nous utilisons tous des cartes de crédit, dont un grand nombre proviennent d'entreprises non canadiennes qui stockent les renseignements à l'étranger. Est-ce que cela vous préoccupe? En quoi cela est-il lié aux recherches que vous avez effectuées?

● (1605)

M. Yuval Shavitt: En effet, c'est la principale inquiétude qui fait l'objet de cette recherche. Nous observons des actes — malveillants ou accidentels — de détournement du routage vers des lieux qui devraient être évités.

Soit dit en passant, la vitesse du réseau en souffre également. Par exemple, nous avons observé des cas de routes reliant Tokyo et Séoul qui ont été détournées de façon non malveillante pour passer par les États-Unis et, une semaine plus tard, par Londres. Ces cas de changements de routage non malveillants rendent la connexion Internet 10 fois plus lente.

Ce genre de choses arrivent sans arrêt. Le plus difficile, c'est d'arriver à faire la distinction entre les problèmes d'ingénierie, les erreurs de configuration et les attaques.

M. Matthew Dubé: Voici la question que je veux vous poser. En tant qu'ingénieur, vous ne serez peut-être pas en mesure d'y répondre — je dis cela en tout respect, bien entendu. Je suis Canadien. Si mes données se retrouvent sur un serveur américain, est-il à craindre que je ne bénéficierai pas des mêmes protections constitutionnelles et juridiques pour l'utilisation de ces données et pour ma vie privée, et ce, même si les États-Unis sont un pays démocratique allié du Canada? Y a-t-il des inquiétudes à ce sujet?

Vous avez dit que, à tout prendre, les pays non démocratiques sont considérés comme des acteurs plus malveillants, ce qui va de soi. Cependant, au bout du compte, tout le monde se livre à la même activité et ce sont les particuliers qui risquent d'en payer le prix. Est-ce une préoccupation ou est-ce que ces questions débordent le cadre de vos recherches?

M. Yuval Shavitt: La question de l'inquiétude est très subjective. Tout le monde n'est pas préoccupé par la même chose. Lorsque l'on construit un système du genre, il faut le concevoir de façon à ce qu'il puisse être adapté aux préoccupations des particuliers.

M. Matthew Dubé: Je comprends ce que vous dites. Merci.

Madame Slay, j'aimerais parler de l'expérience australienne en particulier.

L'an dernier, si je ne m'abuse, une loi a été adoptée chez vous. Voilà qui renvoie à l'inquiétude souvent exprimée au sujet de ces prétendues portes dérobées. En simple, toute porte dérobée que les forces de l'ordre pourraient ouvrir au moyen d'un décryptage pourrait aussi être ouverte de la même façon par des personnes mal intentionnées — par des malfaiteurs, autrement dit.

Que pensez-vous de l'expérience législative australienne? Est-il trop tôt pour se prononcer? Je crois me rappeler qu'une telle inquiétude avait été soulevée à ce moment-là.

Mme Jill Slay: Cette question n'a pas été réglée; elle a été renvoyée au Parlement. À mon avis, les fournisseurs ont réagi de façon excessive du fait qu'ils croient que le gouvernement menace d'affaiblir leurs produits. En fait, ayant travaillé avec le gouvernement pendant de nombreuses années à titre de professeure de criminalistique numérique, j'ai fait partie des gens qui ont aidé le gouvernement à comprendre comment les forces de l'ordre peuvent obtenir des preuves.

Personnellement, je me suis opposée à ceux qui veulent empêcher les forces de l'ordre d'obtenir des preuves dans des cas graves, mais cette question n'est toujours pas réglée. C'est dans les journaux cette semaine. De fait, nous ignorons comment tout cela va se terminer. Le gouvernement a eu le mot de la fin, en quelque sorte, sur le plan de la sécurité nationale. Si vous voulez suivre ce qui se passe en Australie, je vous suggère d'attendre un peu.

M. Matthew Dubé: Très bien.

Je n'ai peut-être pas assez lu sur le sujet, mais je me demande ce qu'il en est de la loi. Est-ce au cas par cas? Je suppose qu'il y a un mandat ou quelque chose du genre. Pourriez-vous préciser de quoi il retourne de façon aussi brève que possible?

Mme Jill Slay: Malheureusement, je ne suis pas non plus ingénieure. Je ne connais donc pas les subtilités de la loi. Je crois en effet que, à la base, c'est au cas par cas, les forces de l'ordre pouvant obliger... C'est lié au cryptage, quelque chose qui est chiffré — c'est ce que j'en comprends. Ce n'est pas une loi aussi radicale que ce qu'en disent beaucoup de gens, à mon avis.

M. Matthew Dubé: D'accord, merci.

Monsieur Shavitt, pendant la minute qu'il me reste, j'aimerais aborder l'Internet des objets. Vous avez parlé du temps pendant lequel les données peuvent rester quelque part avant d'être transférées vers un autre endroit. Craint-on que les protocoles de sécurité des appareils soient déficients et que le problème s'accentue à mesure que ces appareils prolifèrent à l'avenir?

M. Yuval Shavitt: Tout à fait. Le problème avec l'Internet des objets, c'est qu'il s'agit d'appareils à très faible coût. Les gens ne pourront pas dépenser quelques sous de plus pour les rendre plus sûrs. Ces milliards d'appareils qui ne sont aucunement sécuritaires constituent un problème majeur que nous devons régler sur le plan du système.

● (1610)

Le président: Il vous reste 20 secondes.

M. Matthew Dubé: Ce sera tout. Merci, monsieur le président.

Le président: D'accord, merci.

Je n'avais jamais pensé qu'être ingénieur était un mauvais coup du sort.

Monsieur Picard, ce malheur vous a épargné, je crois. Vous avez sept minutes.

M. Michel Picard: En effet, je ne suis pas du tout ingénieur.

Je me tourne d'abord vers M. Shavitt.

Pouvez-vous me rappeler ce que vous avez dit au sujet du fait qu'aucune entreprise de télécommunications en Israël ne peut venir de l'extérieur d'Israël ou d'entités étrangères?

M. Yuval Shavitt: Je ne connais pas bien l'aspect juridique, mais c'est effectivement le cas. Toutes les entreprises de télécommunications en Israël appartiennent à des intérêts israéliens.

M. Michel Picard: À votre connaissance, qu'est-ce qui fait que les entreprises de télécommunications israéliennes ne sont pas achetées par des intérêts étrangers ou que leurs services ne sont pas loués par des intérêts étrangers, lesquels pourraient ainsi contourner l'interdiction?

M. Yuval Shavitt: Je pense qu'elles ne peuvent pas être achetées par des entités étrangères. Un certain comité doit donner son accord. Je ne pense pas que cela puisse se produire. Peut-il y avoir location? Peut-être.

M. Michel Picard: C'est une zone grise, si je comprends bien.

M. Yuval Shavitt: Oui.

M. Michel Picard: D'accord.

Madame Slay, il y a quelques semaines, un article indiquait qu'à Londres, on avait examiné le cas de Huawei et, n'ayant plus aussi peur ou ne ressentant plus aussi fortement le besoin de se protéger, on commençait peut-être à changer d'avis au sujet de l'enjeu de sécurité lié à l'entreprise. En revanche, en Australie, vous vous êtes débarrassés de l'entreprise, tout simplement.

Êtes-vous au courant de ce changement d'attitude au Royaume-Uni? Si oui, qu'en pensez-vous?

Mme Jill Slay: J'ai suivi l'affaire de très près.

Selon le premier rapport du GCHQ, fournir une assurance au sujet du matériel de Huawei aurait demandé un effort beaucoup trop grand de la part du laboratoire du Government Communications Headquarters. Cependant, je crois qu'hier le GCHQ a indiqué qu'il serait peut-être à même de fournir cette assurance. Il y a des répercussions politiques au Royaume-Uni en raison de la nature de leur conseil. C'était différent pour nous en Australie. Je crois que nous nous sommes déjà engagés à ne pas utiliser Huawei au gouvernement fédéral, mais nous n'avons pas examiné toutes les relations qu'entretient Huawei en Australie avec des entreprises qui ne font pas d'achats pour le gouvernement fédéral, notamment. Par exemple, le gouvernement de l'Australie-Occidentale a un contrat avec Huawei pour l'équipement de son système ferroviaire et l'Université de New South Wales, où je travaillais auparavant, a acheté du matériel pour des travaux de construction.

En Australie, le gouvernement fédéral peut contrôler les achats fédéraux. Par exemple, il a réussi à empêcher Optus, l'une de nos compagnies de téléphone, d'utiliser Huawei pour la 5G. Cependant, il n'est pas possible de tout contrôler, puisque nous sommes un pays démocratique et que, en plus du gouvernement fédéral, nous avons des États.

À mon avis, la décision britannique n'aura aucune incidence sur la décision qui a été prise à Canberra. La raison en est que nous voyons le lien qui existe entre la cybersécurité, la capacité d'infiltrer les portes dérobées de nos systèmes, le cyberespionnage et l'ingérence étrangère. Voilà de quoi il est question en ce moment. Il ne s'agit pas seulement de la sécurité des appareils.

M. Michel Picard: N'est-il pas vrai — je n'en suis pas certain — que certaines pièces de l'iPhone sont fabriquées en Chine? Dois-je commencer à me méfier de mon iPhone? Si c'est le cas, je ne ferai plus confiance à aucun téléphone ni à aucun appareil. Dans ma circonscription, nous ne fabriquons rien, nous devons faire nos achats ailleurs.

● (1615)

M. Yuval Shavitt: On comprend mieux désormais le risque que l'on encourt lorsque l'on connaît mal la chaîne d'approvisionnement. C'est un problème complexe, parce que nous vivons dans un environnement mondialisé. Parfois, on n'a d'autre choix que d'acheter certaines pièces dans des pays où l'on préférerait ne pas avoir à s'approvisionner.

S'il y a un agent d'intégration, celui-ci doit avoir la responsabilité d'examiner la chaîne d'approvisionnement, d'identifier les risques et d'arriver à les contrôler au moyen d'inspections, de tests, etc.

M. Michel Picard: Vous avez employé un mot intéressant. Je n'ai pas le choix. J'ai le choix de ce que je mets sur ma page Facebook. Je peux être très discret ou encore chercher des amis si je n'en ai pas — je n'en ai que deux.

Des voix: Oh, oh!

M. Michel Picard: Le marché se transporte sur le Web. Si on n'y va pas, il n'y a pas d'évolution ou de progrès. C'est là que nous sommes, c'est là qu'il faut aller. Il est possible que je ne veuille pas transmettre mes renseignements financiers par téléphone ou par ordinateur, mais je ne vais pas à la banque tous les jours pour faire imprimer mes relevés. C'est sur le Web qu'il faut aller. Nous savons que nous perdons pied et nous ignorons si cela aura une fin. Est-ce là l'absence de choix dont vous parlez?

M. Yuval Shavitt: Je pense que nous savons très bien comment sécuriser les sites Web. Tout n'est pas parfait, évidemment, et ce n'est pas tout le monde qui fait ce qu'il faut pour se protéger, mais il y a des moyens.

Essentiellement, nous parlons ici de gestion des risques. Il en coûtera probablement trop cher pour passer d'un niveau de sécurité de 99,5 % à un niveau de 100 %, mais il est possible d'obtenir un niveau de sécurité assez bon. Il suffit d'investir de l'argent et des efforts et de savoir ce que l'on fait.

M. Michel Picard: En tant que bon citoyen, comment évaluez-vous la possibilité de vous retrouver dans le 1 % qui échappe à la gestion des risques?

M. Yuval Shavitt: Ce sont des statistiques, non?

Le président: Nous allons devoir laisser tomber cette question existentielle.

Monsieur Eglinski, vous avez cinq minutes.

M. Jim Eglinski (Yellowhead, PCC): Je vais commencer par vous, monsieur Shavitt.

J'ai pris connaissance l'autre jour de l'article vous avez corédigé en 2018 et qui s'intitule *China's Maxim—Leave No Access Point Unxploited*. C'est un article très intéressant. En fait, je crois l'avoir assez bien compris après l'avoir lu trois fois.

Des voix: Oh, oh!

M. Jim Eglinski: Il s'agit d'un rapport très complet. Je crois que dans le cinquième ou le sixième paragraphe, vous abordez une grande préoccupation, à savoir que tous les pays doivent unir leurs efforts et s'attaquer à ces problèmes.

Avez-vous obtenu une réaction de différents pays depuis que vous avez publié cet article?

M. Yuval Shavitt: Je préfère ne pas faire de commentaires à ce sujet.

M. Jim Eglinski: Vous préférez ne pas faire de commentaires? D'accord. Je vais parler d'autre chose alors.

Vous avez parlé de contrôle des flux du trafic, ce que vous faites dans votre pays d'origine. L'une des choses les plus importantes, bien sûr, c'est d'activer des plaques de données surveillées, pour savoir à quel genre d'équipement on a affaire. Je suis un peu curieux au sujet de ce contrôle.

Vous surveillez ce qui est acheminé et où. Lorsque vous découvrez des changements de routage inusités, est-ce que des données sont déjà perdues? Y a-t-il une façon pour vous d'intervenir avant qu'on en arrive là? Vous avez parlé de la technologie et du coût des investissements dans la protection, alors je me demande si vous pourriez nous en dire un peu plus à ce sujet.

M. Yuval Shavitt: Il existe des façons de prévenir le piratage dans certains cas. Dans d'autres cas, on doit se limiter à le détecter et à atténuer les risques. Supposons que quelqu'un lance une opération d'espionnage contre vous. Préféreriez-vous que cette opération dure 25 minutes ou 25 jours? Si vous pouviez y mettre fin après quelques minutes, ou après une demi-heure, disons, ce serait beaucoup mieux que de laisser la situation perdurer pendant des semaines. Nous avons vu des attaques qui ont duré des semaines, parfois même plus longtemps.

Certaines attaques sont très courtes. Le temps de les détecter et de tenter d'en diminuer les effets, et vous avez déjà perdu des données. Bon nombre des attaques, surtout celles qui sont le fait d'organismes gouvernementaux, peuvent durer de nombreuses semaines.

● (1620)

M. Jim Eglinski: D'accord.

Vous avez mentionné quelque chose plus tôt. Toute notre étude porte sur la cybersécurité dans le secteur financier, mais nous digressons un peu parce que la cybersécurité est un sujet très vaste. Vous avez mentionné que dans votre pays, les institutions financières ont été assez durement touchées.

M. Yuval Shavitt: Non, je n'ai pas dit cela. J'ai dit que dans l'ensemble, d'après ce que nous voyons à l'échelle mondiale, les institutions financières ont été durement touchées.

M. Jim Eglinski: D'accord. Avez-vous constaté cela dans votre propre pays?

M. Yuval Shavitt: Il y a eu des attaques contre des institutions financières dans notre pays, oui.

M. Jim Eglinski: D'accord. Merci.

Madame Slay, je regardais votre compte Twitter, juste pour en apprendre un peu plus à votre sujet. Avant mars 2018, la Russie semblait être au centre de vos préoccupations pour ce qui est des mauvais agissements, mais votre attention semble s'être portée sur la Chine depuis.

Pourriez-vous nous expliquer ce qui a motivé ce changement d'intérêt?

Mme Jill Slay: Pour être honnête avec vous, j'ai vécu à Hong Kong pendant 10 ans. Je parle couramment le chinois, mais j'ai aussi une attestation de sécurité. De plus, je fais très attention à ce que je dis sur Twitter, alors tout ce que vous pouvez voir, c'est que je suis très sélective.

J'en suis arrivée au stade où je suis très frustrée par la façon dont, comme professeure, je suis constamment ciblée par les Chinois. On m'attribue des choses. J'ai été la cible de vols. On m'a parachuté des étudiants au doctorat. Par conséquent, j'ai décidé de parler davantage de la situation. C'est ce que vous voyez sur Twitter.

Pour moi, le problème, comme je suis de plus en plus connue, c'est que je suis beaucoup plus susceptible d'être ciblée. Je crains que tous les professeurs dans notre domaine, quel que soit le pays où ils se trouvent — et je ne pense pas que le Canada soit à l'abri — soient ciblés, en particulier par la Chine, parce que c'est vraiment la PI qui est visée, et ce, depuis de nombreuses années.

M. Jim Eglinski: Pouvez-vous me dire quelles sont vos préoccupations au sujet des produits 5G Huawei dans votre pays et pourquoi vous pensez que c'était une bonne idée de les interdire?

Le président: En 10 secondes ou moins.

Mme Jill Slay: Je pense qu'il y a deux façons d'envisager la question avec Huawei. Je ne peux pas commenter certaines choses parce que, comme je viens de vous le dire, j'ai une attestation de sécurité. Huawei est une entreprise qui a la réputation de constamment voler la propriété intellectuelle. Si vous regardez le cas le plus connu, celui des routeurs Cisco, à partir de 2012, je crois, il y a un aspect d'éthique des affaires.

De plus, l'autre aspect plus logique, c'est que si vous achetez leur équipement, il est possible qu'ils aient besoin d'y avoir accès pour l'entretien. S'ils choisissent de vous espionner, ils peuvent alors intégrer un logiciel malveillant dans votre équipement. Il peut s'agir de matériel ou de logiciels, mais nous sommes très vulnérables.

Le président: Merci, monsieur Eglinski.

Madame Dabrusin, vous avez la parole pour cinq minutes.

Mme Julie Dabrusin (Toronto—Danforth, Lib.): Merci.

Je crois, madame Slay, que vous avez parlé de normes professionnelles nationales en matière de cybersécurité. Une chose a été soulevée à quelques reprises dans les témoignages que nous avons entendus, c'est la nécessité d'avoir plus de personnes formées, plus de formation pour que les gens deviennent des professionnels de la cybersécurité. Est-ce que l'Australie fait quelque chose en particulier, qui donne de bons résultats, pour créer un pipeline — à défaut d'un meilleur terme — de jeunes qui font l'acquisition des compétences nécessaires pour entrer dans le domaine de la cybersécurité, afin de pouvoir nous aider à régler ce problème?

Mme Jill Slay: Oui. Nous investissons énormément d'argent et d'efforts dans ce domaine. Grâce à l'Australian CyberSecurity Growth Network et aux centres de développement, nous avons maintenant des systèmes. Nous avons imité les Américains de bien des façons, alors nous avons l'équivalent du programme CyberPatriot Capture the Flag pour les enfants. Nous essayons d'intégrer la cybersécurité dans le programme d'études pour tout le monde, de la 7e à la 9e année. Nous tentons d'intégrer la sensibilisation à la cybersécurité dans le programme des collèges TAFE, qui sont des collèges communautaires ou des collèges techniques, peu importe le domaine d'études. Cela devrait se faire très bientôt. Du financement national a été prévu à cette fin.

Pour ce qui est de l'Australian Computer Society, nous avons un programme national en TIC. Nous essayons donc d'élaborer un programme national en cybersécurité interdisciplinaire, afin de nous concentrer non seulement sur les questions de TI, mais aussi sur le droit, l'éthique, la criminologie et la psychologie, dans le cadre d'un programme de trois ans. Mon université et quelques autres en ont un. Le gouvernement a déclaré qu'il s'agit d'un enjeu interdisciplinaire qui doit être reconnu à ce titre par tout le système d'éducation.

● (1625)

Mme Julie Dabrusin: Monsieur Shavitt, Israël fait-il quelque chose pour constituer une telle capacité?

M. Yuval Shavitt: Nous faisons des choses semblables à ce qui se fait en Australie. Nous avons un programme pour les jeunes enfants. Il est possible d'obtenir une certification en cybersécurité à la fin du secondaire. Autrefois, c'était en informatique. Il y a maintenant un choix entre l'informatique et la cybersécurité. À l'université, nous avons aussi un programme spécifique pour la cybersécurité.

Il y a une chose que nous avons, mais que l'Australie et le Canada n'ont probablement pas, c'est l'armée, qui facilite considérablement les choses. Chaque année, des centaines de milliers de jeunes Israéliens sont recrutés dans des services du renseignement et dans d'autres unités où ils sont formés. Ils travaillent beaucoup à un haut niveau de la cybersécurité dans un environnement très encadré. Cela nous donne un grand avantage.

Mme Julie Dabrusin: Nous n'avons pas de système semblable.

J'essaie simplement de comprendre ce que les gens font de bien et dont nous pourrions tirer des leçons. Il est vraiment intéressant d'entendre parler des différentes initiatives qui existent.

Nous avons aussi entendu parler d'HackerOne, qui utilise des pirates — des pirates bien intentionnés, faute d'une meilleure façon de les décrire — pour tester le système. Il pourrait y avoir des primes de bogue, je crois qu'on les appelle ainsi, pour aider à déterminer où se trouvent les problèmes et les failles. Avez-vous cela dans l'un ou l'autre de vos pays? Est-il utile de légaliser ce genre de travail?

M. Yuval Shavitt: Tout d'abord, c'est légal. De nombreuses entreprises ont des primes. Si vous signalez un problème, vous pouvez obtenir un prix en argent, et il peut atteindre 100 000 $ si c'est vraiment quelque chose... C'est ce qui se passe partout dans le monde. Il n'y a pas de limites. Si Cisco ou une autre entreprise a un problème, il lui importe peu que la solution vienne de la Belgique ou du Canada.

De plus, du moins en Israël, nous avons une équipe rouge bénévole. Ce sont des experts en cybersécurité qui consacrent une journée par mois ou quelques jours par mois à des tests, avec permission. Ils font des tests d'intrusion dans des infrastructures essentielles. Il peut s'agir d'un hôpital, d'une installation d'aqueduc, etc. À la fin, ils présentent un rapport dans lequel ils disent : « Voici les problèmes que vous avez. » Je pense que c'est vraiment utile. Lorsqu'une autorisation est donnée, il n'y a pas de problème juridique. Je ne pense pas qu'il faille une nouvelle loi pour cela.

Le président: Merci, madame Dabrusin.

Comme mes collègues et les témoins peuvent le constater, les lumières clignotent. Normalement, je suis obligé de suspendre la séance, mais je suppose qu'il y aura unanimité pour continuer pendant une vingtaine de minutes. Vous aurez 10 minutes pour nous rendre à l'étage supérieur pour voter. Cela vous convient-il?

Un député: Cela me convient.

Le président: D'accord.

Monsieur Motz, vous pouvez poursuivre pendant encore cinq minutes.

M. Glen Motz: Merci.

Comme on l'a dit, Israël et l'Australie sont reconnus comme des pays très avancés en matière de cybersécurité. En disposant d'entreprises de cybersécurité plus fortes, ainsi qu'en attirant des investissements pour lutter contre la cybersécurité, vos deux pays font-ils l'objet d'attaques semblables à celles que nous avons eues au Canada? Faites-vous face au même nombre et au même type d'attaques que nous, ou s'agit-il davantage de gens qui tentent de percer les systèmes?

Mme Jill Slay: Puis-je répondre?

M. Glen Motz: Je vous en prie. Vous pouvez répondre tous les deux.

Mme Jill Slay: La semaine dernière, nous avons annoncé publiquement une attaque majeure contre le Parlement, contre tous nos courriels et l'ensemble de nos services. Le premier ministre en a parlé lundi. Chacun des trois grands partis politiques a aussi été attaqué. Ce matin, en me réveillant, j'ai appris qu'un gros hôpital de Melbourne avait été attaqué par un rançonneur et que les dossiers des patients avaient été altérés et ne pouvaient pas être déchiffrés correctement.

Je dirais que vous ne devriez d'aucune façon vous considérer comme les parents pauvres par rapport à nos pays. Nous faisons tous l'objet du même nombre d'attaques. En tant que membres du Groupe des cinq en particulier, nous nous appuyons mutuellement. Je pense toutefois que le niveau d'attaque est assez élevé en ce moment. Dans notre cas, c'est à cause des élections générales imminentes, mais il y a d'autres enjeux politiques. Je le vois à la fois d'un point de vue politique et d'un point de vue criminel. Il y a les États-nations et la cybercriminalité, et cette dernière ne cesse de croître.

● (1630)

M. Glen Motz: Monsieur Shavitt.

M. Yuval Shavitt: Je pense que c'est probablement la même chose partout dans le monde. Peut-être qu'Israël est un peu plus ciblé à cause du conflit israélo-arabe, mais en général, nous sommes tous menacés.

M. Glen Motz: Très bien. Merci.

Le Canada est l'un des deux seuls alliés du Groupe des cinq qui n'a pas encore pris position sur Huawei. Le directeur du Service canadien du renseignement de sécurité, le SCRS, a exprimé publiquement ses préoccupations au sujet de l'espionnage parrainé par des États au moyen de la prochaine génération de la technologie 5G. Nous savons que l'Australie a été à l'avant-garde en interdisant la participation de cette entreprise.

Madame Slay d'abord, puis monsieur Shavitt, que signifierait, selon vous, la volonté du Canada de faire affaire avec Huawei pour la longévité du Groupe des cinq?

Mme Jill Slay: Je dois dire que c'est une question de souveraineté. C'est vraiment au Canada de décider.

Évidemment, je ne peux pas parler au nom du gouvernement. Je parle en mon nom uniquement. Je pense que le partenariat du Groupe des cinq profiterait, d'un point de vue technique, d'une perspective commune au sujet de Huawei. Mais je pense que l'annonce faite hier par les Britanniques, une annonce en demi-teinte selon laquelle nous pourrions peut-être régler ce problème, qui disait que peut-être, avec des efforts, nous pourrions fournir le genre d'assurance... compliquerait également les choses pour le Canada.

Pour moi, tant comme personne que comme ingénieure, c'est tout noir ou tout blanc. Alors, je suis rassurée par le fait que le gouvernement fédéral ne va pas acheter de technologie Huawei. Je dirige également la chaire Optus, et Optus finance une bonne partie de la recherche à mon université. De toute évidence, Optus était la compagnie qui était en rapport avec Huawei pour la technologie 5G. Je me suis sentie en plein conflit d'intérêts en raison de mes fonctions, et j'ai été très soulagée de ne pas avoir eu à m'occuper de cette question.

D'un point de vue politique, je pense que pour maintenir la solidarité du Groupe des cinq, il faudrait en arriver aux mêmes conclusions. Mais je pense que d'autres aborderont cette question cette semaine.

M. Glen Motz: Monsieur Shavitt.

M. Yuval Shavitt: C'est une question de gestion des risques. Comme je l'ai dit dans ma déclaration préliminaire, nous savons, d'après le rapport Snowden, que les entreprises américaines collaborent avec le gouvernement américain, alors il n'y a aucune raison de supposer que cela ne fonctionne pas de la même façon dans d'autres pays, surtout en Chine. C'est de la gestion des risques. Combien seriez-vous prêt à investir pour éviter qu'Huawei s'installe au Canada? Bien sûr, l'équipement va vous coûter plus cher.

Je dirais que si vous décidez d'utiliser Huawei, vous devez mettre en place de l'équipement et des installations de surveillance pour vous assurer que des choses bizarres ne se produisent pas.

Le président: Merci, monsieur Motz.

Madame Sahota, vous avez cinq minutes.

Mme Ruby Sahota (Brampton-Nord, Lib.): D'accord.

Je vais commencer par vous, madame Slay. C'était un peu inquiétant de vous entendre dire que vous étiez ciblée et que des étudiants au doctorat assistaient à vos cours pour vous espionner. Pouvez-vous expliquer pourquoi vous avez été ciblée? Je crois que vous avez dit que tous ceux qui occupent des fonctions comme les vôtres dans le milieu universitaire pourraient être menacés. Quel est le lien entre la PI et les fonctions que vous occupez?

Mme Jill Slay: Je pense que cela fait partie de la perception à l'échelle internationale, dont il a déjà été question, selon laquelle essentiellement, de la même façon que la Chine pourrait vouloir recueillir autant de données que possible dans le système, elle a une façon beaucoup plus systématique d'envoyer des étudiants au doctorat en Australie, aux États-Unis et, je présume, au Canada. Ceux d'entre nous qui sont considérés comme des chefs de file dans notre pays finissent par avoir de nombreux étudiants chinois qui veulent étudier avec eux au doctorat.

Avec l'un de mes tout premiers étudiants au doctorat, je travaillais sur un projet avec la police. C'était dans une université publique, alors il ne s'agissait pas de données classifiées. Néanmoins, sans entrer dans les détails, la PI a été volée et ramenée en Chine. Même si j'étais là, je n'ai malheureusement pas su quand cela s'est produit. Depuis, je suis très prudente.

● (1635)

Le président: Faites-vous l'objet de piratage actuellement?

Mme Ruby Sahota: J'ai lu un peu au sujet du piratage des données des partis politiques. Savez-vous de quel genre de données il s'agit? Je sais que vous allez avoir des élections bientôt. Nous avons nous aussi des élections en octobre de cette année. Au sein d'un autre comité auquel je siège, nous avons beaucoup discuté avec la ministre des Institutions démocratiques des menaces potentielles auxquelles le Canada est confronté, tout comme de nombreux pays du monde, en ce qui concerne les élections et la protection des institutions démocratiques.

Quel genre de conseils pouvez-vous nous donner à la lumière de l'expérience australienne?

Mme Jill Slay: Je ne pense pas que nous ayons annoncé officiellement — et je ne pense pas que nous pourrons le faire à court terme — que des données ont été volées. En fait, nous ne le savons pas. Cela vient du secteur parlementaire. La plus grande préoccupation a été soulevée auprès des [*Difficultés techniques*]..., des trois principaux partis, et le fait qu'ils disposent de très peu d'argent.

Il n'en coûte que 70 000 $ par année pour sécuriser leurs systèmes. Toutefois, dans ces systèmes, on retrouve toutes les données sur les membres, les dons et ce genre de choses. Voilà ce qui suscite un débat public cette semaine. Tout comme vous, nous nous souvenons de ce qui s'est passé, véritablement ou supposément, lors des élections aux États-Unis. Le gouvernement nous assure que le problème a été pris très tôt et qu'il est maîtrisé, mais je ne pense pas qu'il y aura beaucoup plus de déclarations publiques, pour être honnête. Nous devons tous être prudents.

Mme Ruby Sahota: Pensez-vous que l'absence de déclaration publique est attribuable au fait que l'on veut protéger l'intégrité du système, ou plutôt au fait que l'on ne veut pas que les gens soient pleinement conscients de ce qui s'est ou non passé?

Mme Jill Slay: Ils ne sont pas prêts à annoncer quoi que ce soit. L'attribution est difficile et cela fait partie de la discussion. Il est facile de prétendre être un État-nation pour s'installer dans un autre État-nation. Nous ne pouvons pas savoir d'où vient l'attaque. Très souvent, nous ne savons pas d'où proviennent les attaques, parce que les gens sont très bons pour faire de l'espionnage et se cacher, en prétendant être quelqu'un d'autre.

Mme Ruby Sahota: Nous avons également eu ces conversations au sujet des entreprises privées. Elles sont nombreuses à ne pas révéler les intrusions qui se produisent par crainte de la réaction du public ou parce qu'elles ont honte.

En ce qui concerne nos institutions démocratiques, pensez-vous que nous devrions essayer, par l'entremise du Groupe des cinq à tout le moins, et d'autres démocraties, de travailler ensemble pour réduire les menaces potentielles, et de quelle façon devrions-nous le faire?

Mme Jill Slay: Nous devrions et je pense que nous le faisons. Ce n'est probablement pas beaucoup connu dans le public, mais je suis à peu près certaine qu'au sein des organisations internationales, au sein des gouvernements, il y a aussi beaucoup de partage. D'après mon expérience, il y a beaucoup de partage, que ce soit au chapitre de l'application de la loi ou de quoi que ce soit d'autre. Je ne pense pas que nous soyons nécessairement limités par ces choses.

Il peut s'agir de petites entreprises qui ne veulent pas reconnaître qu'elles ont fait l'objet d'intrusions. Toutefois, surtout en Australie, il y a maintenant une plus grande ouverture à en parler, d'autant plus qu'avant Noël, le gouvernement, Alastair MacGibbon, le sous-secrétaire, le conseiller du premier ministre, a dit très clairement que de nombreuses entreprises ont fait l'objet d'intrusions, et il y a plus d'ouverture, plus de volonté à accepter cela parce qu'il y en a tellement.

● (1640)

Le président: Merci, madame Sahota.

Monsieur Dubé, vous avez trois minutes.

M. Matthew Dubé: Merci, monsieur le président.

Très rapidement, j'aimerais vous entendre tous les deux. Nous avons beaucoup parlé des acteurs des États étrangers comme d'une menace. On a un peu parlé ici au Canada des acteurs nationaux qui opèrent, pas nécessairement dans le domaine de la cybersécurité, mais dans l'espace numérique.

Du point de vue de la cybersécurité et dans le cadre de notre étude, y a-t-il eu des préoccupations, tant en Israël qu'en Australie, au sujet d'acteurs nationaux et d'actes malveillants qui ont posé un risque pour le gouvernement ou des particuliers? M. Shavitt pourrait peut-être répondre, puis Mme Slay.

M. Yuval Shavitt: Bien sûr, on a toujours peur des activités criminelles. Les criminels considèrent Internet comme un excellent endroit où faire de l'argent très facilement. Oui, il faut aussi se protéger contre les attaques nationales.

M. Matthew Dubé: Madame Slay.

Mme Jill Slay: Oui, c'est la même chose pour nous. Nous sommes toujours conscients de la possibilité d'une attaque interne. Nous plaisantons toujours au sujet du pirate adolescent de 15 ans qui peut faire autant de tort qu'un État-nation. Nous en sommes conscients, mais à l'heure actuelle, compte tenu des problèmes entourant Huawei et la Chine, je crois que la communauté internationale met l'accent sur les attaques provenant de l'extérieur.

M. Matthew Dubé: Dans la minute qu'il me reste, j'aimerais rappeler, comme nous l'avons vu dans d'autres domaines, comme le renseignement et l'application de la loi, en termes plus traditionnels, qu'en mettant l'accent sur un côté, nous avons parfois tendance à oublier l'autre. Y a-t-il une possibilité, un risque, que l'on néglige l'aspect national en mettant l'accent sur les acteurs étrangers?

Mme Jill Slay: Si nous nous concentrons sur la défense de nos systèmes contre les attaques extérieures, nous les protégeons contre les attaques intérieures. Le problème des initiés est différent.

Le président: Monsieur Shavitt.

M. Yuval Shavitt: [*Difficultés techniques*]

Le président: Je voudrais poser quelques questions, en demandant au Comité d'être indulgent. Même si le Comité ne me le permet pas, je vais quand même poser mes questions.

Monsieur Shavitt, j'aimerais me concentrer sur votre analyse du routage qui, si j'ai bien compris, est votre spécialité. Vous avez parlé des points d'attaque, à la fois des points d'attaque logiciels et matériels, des endroits où les données peuvent être compromises et de l'acheminement de l'information là où vous ne voulez pas qu'elle soit acheminée. La question que je veux vous poser concerne la situation actuelle du réseau 4G, et lorsqu'il s'agit d'un réseau 5G, la différence importante, le cas échéant, en ce qui concerne la façon dont vous protégez ces routeurs.

M. Yuval Shavitt: Je ne pense pas qu'il y ait une différence importante. Il s'agit simplement d'un bon moment pour renouveler votre équipement et vous voulez le faire de la meilleure façon possible sur le plan de la cybersécurité.

Le président: Madame Slay, êtes-vous d'accord avec cette observation?

Mme Jill Slay: Oui. C'est le moment de bien examiner vos protections.

Le président: Pour ce qui est de logiciels malveillants dans la partie matérielle de ces routeurs, vous appliqueriez la même analyse pour un réseau 4G que pour un réseau 5G. Est-ce exact? D'accord.

Ma deuxième question porte sur la propriété de l'infrastructure, car Israël a pris une décision, et il s'agit d'un pays relativement petit, qui est donc davantage capable de contrôler la structure de la propriété. La propriété est-elle une illusion dans les faits, et peut-on pénétrer dans n'importe quel système, peu importe à qui il appartient?

M. Yuval Shavitt: Il est vrai que l'on peut pénétrer dans n'importe quel système de l'extérieur, mais il faut défendre ces systèmes. Il ne faut pas faciliter la vie des auteurs des attaques. Encore une fois, c'est une question de gestion des risques. Vous voulez rendre aussi difficiles que possible les intrusions dans votre infrastructure essentielle. On ne peut jamais être en sécurité à 100 %, mais on peut se rapprocher le plus possible de cet objectif.

● (1645)

Le président: Votre argument serait donc que, s'il s'agit d'un acteur national, la possibilité augmente au chapitre de la sécurité plutôt que de diminuer.

M. Yuval Shavitt: Oui.

Le président: Madame Slay, avez-vous quelque chose à dire à ce sujet?

Mme Jill Slay: Je pense que mon conseil serait que, particulièrement lorsqu'il est question d'infrastructures essentielles — je suis également particulièrement préoccupée par le nuage —, il y a eu une tendance à économiser de l'argent au sein des gouvernements et à utiliser les nuages externes public-privé de tiers, et je parle de mon gouvernement. Mais j'ai remarqué une tendance, encore cette semaine, à parler du stockage en nuage sur le sol australien.

Je vous recommanderais d'évaluer les coûts et les avantages que représente, du point de vue de la sécurité nationale et des finances, le fait de conserver toutes vos données dans votre propre pays.

Le président: Merci.

Monsieur Shavitt.

M. Yuval Shavitt: Il y a une chose qu'il est facile de faire et que les gouvernements semblent négliger.

Les gens ont tendance à s'aligner sur l'entité dont ils font partie. Regardez l'affaire Snowden. Snowden était un entrepreneur. Il n'était pas un employé du gouvernement. Il y a de bonnes chances que s'il avait été un employé du gouvernement, il aurait eu davantage l'impression de faire partie du système, et cela aurait diminué les risques qu'il aille contre le système.

En cybersécurité, il ne faut pas embaucher d'entrepreneurs. Vous devriez permettre de payer aux professionnels de la cybersécurité des salaires plus élevés que ce que le gouvernement payait auparavant et de les intégrer au système.

Le président: Au nom du Comité, je vous remercie tous les deux de vos conseils, de votre sagesse et de votre expérience.

Chers collègues, je peux maintenant lever ou suspendre la séance. Il nous reste 10 minutes avant le vote. Si nous suspendons la séance, nous pourrons peut-être revenir pour nous occuper de la motion. Nous pouvons aussi lever la séance et nous occuper de la motion M-167 à un autre moment.

Qu'en pensez-vous?

Un député: Levons la séance.

Le président: La séance est levée.

La cybersécurité dans le secteur financier comme enjeu de sécurité économique

Mémoire présenté au Comité de la sécurité publique et nationale de la Chambre des communes

Professeure Jill Slay, présidente de la cybersécurité La Trobe Optus

Introduction

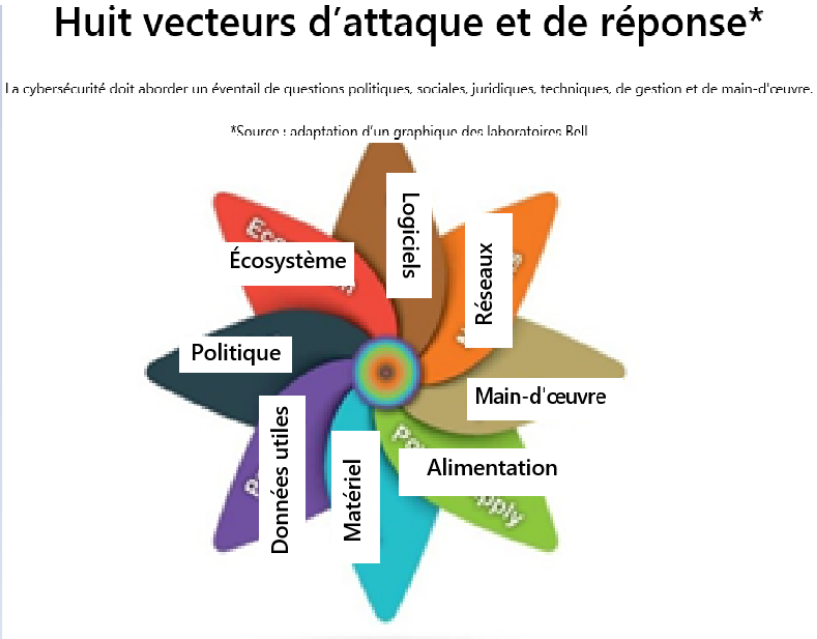
Dans ce mémoire, j'examine certains des principaux défis en matière de cybersécurité auxquels, je crois, l'Australie et le Canada (et, dans une certaine mesure, les autres partenaires du Groupe des cinq) sont confrontés et je présente des recommandations pour relever ces défis.

- Développement d'une compréhension claire de la nature des cybermenaces
- La cybersécurité dans le cadre de la sécurité nationale
- Élaborer un ensemble clair et culturellement adapté de certifications de cybersécurité nationale (résumé des travaux de l'Australian Computer Society)
- Élaborer un programme de recherche universitaire et gouvernemental approprié en cybersécurité, en particulier l'apprentissage automatique pour la cybersécurité, d'autres approches de l'intelligence artificielle et la sécurité de l'Internet des objets (IdO)

Contexte

L'un des principaux problèmes de cybersécurité auxquels l'Australie, le Canada et nos alliés font face est le grand nombre d'attaques contre le gouvernement, l'industrie et les utilisateurs à domicile. Bien que certaines soient ciblées et de grande valeur, la tendance générale est une croissance non confinée du niveau de menace et une croissance exponentielle des coûts économiques. Ces problèmes nationaux ont été mis en évidence en mai 2017 lors de la campagne du rançongiciel WannaCry. Selon un rapport d'Europol (2017), l'attaque a affecté environ 200 000 ordinateurs dans le monde en les chiffrant et en exigeant un paiement en cryptomonnaie. Au Royaume-Uni, le Service national de la santé à lui seul avait 70 000 appareils touchés, dont des appareils d'imagerie par résonance magnétique, des réfrigérateurs d'entreposage du sang et du matériel de salle d'opération. Selon une estimation, le coût économique mondial de WannaCry s'élève à quatre milliards de dollars.

La propagation de WannaCry a été interrompue en raison d'une limitation de la programmation, mais que se serait-il passé si cette limite n'avait pas existé? Et si WannaCry avait ciblé nos systèmes d'intérêt national? Mais surtout, comment l'Australie et le Canada vont-ils se défendre contre la prochaine version plus sophistiquée de WannaCry? Comment allons-nous aborder les questions du cyberrenseignement et de l'interprétation humaine de la menace que ce renseignement représente? Comment allons-nous réagir en cas d'attaque? Comment nos politiques de sécurité nationale appuient-elles la mise en œuvre d'une solution appropriée? Qui fera la recherche et la pratique dans ce domaine spécialisé?



Je pose ici un grand nombre de questions, mais en dix minutes, j'en aborderai trois.

Développement d'une compréhension claire de la nature de la cybersécurité

La cybersécurité est un terme qui est encore mal compris et qui est souvent assimilé à la « sécurité informatique et de réseau ». Or, nous devons tenir compte de la nature interdisciplinaire de la cybersécurité, y compris lorsque nous y réfléchissons sous l'angle de la sécurité économique.

La « cybersécurité » comporte au moins huit composantes fondamentales, dont certaines sont strictement techniques (mais concernent

des personnes et des organisations), tandis que d'autres sont simultanément techniques et profondément dépendantes d'intrants non techniques. Une illustration de ces ingrédients est saisie ici dans un graphique qui les décrit comme des vecteurs d'attaque et de réponse. Ce graphique est adapté d'une approche élaborée par les ingénieurs des laboratoires Bell pour régler les problèmes de défense des ordinateurs et des appareils connectés (Gupta et Buthmann, 2007). Ce concept permet de comprendre ce qui façonne la cybersécurité et la nature de la cyberdéfense. Mais il y a aussi une perspective nationale plus large, puisque la stratégie et la planification de la cybersécurité dépendent autant de l'environnement politique, juridique et social que des approches d'ingénierie et de systèmes, telles qu'elles sont conçues dans le travail original des laboratoires Bell.

La cybersécurité dans le cadre de la sécurité nationale

La cybersécurité est, pour certains du moins, encore une composante de l'informatique et une science théorique à la recherche de solutions formelles. Dans le milieu universitaire en particulier, le lien entre la cybersécurité, la cyberdéfense, l'espionnage et l'ingérence étrangère sont d'importants concepts liés qui commencent à peine à être compris.

La cybersécurité (ou la guerre cybernétique) pour la sécurité et la défense nationales est un concept relativement nouveau pour les experts techniques. La cybersécurité, en tant que problème de sécurité nationale, a été identifiée pour la première fois en Australie dans le Livre blanc sur la défense de 2000 (Défense 2000). En 2001, le gouvernement Howard a lancé une initiative de sécurité électronique, qui a permis de créer une collaboration entre les organismes du gouvernement fédéral et le Trusted Information Sharing Network (réseau de partage d'informations fiable), lequel représentait les principaux groupes sectoriels désignés comme infrastructures essentielles aux fins de la sécurité nationale (Parlement, 2013). Le gouvernement Rudd a examiné les politiques, programmes et capacités de l'Australie en matière de sécurité électronique en 2008. Le tableau ci-dessous résume les initiatives de cybersécurité depuis 2008, la source des politiques ou des conseils, ainsi que les répercussions sur la recherche et la main-d'œuvre professionnelle.

Besoin de cybersécurité	**Sources présumées de la politique ou des conseils**	**Conséquences pour la recherche sociotechnique**
• Cybersécurité • Guerre cybernétique et cyberdéfense • Cyberrenseignement et cyberespionnage	• Les 4 meilleures stratégies de l'Australian Signals Directorate (ASD, 2013) • Livre blanc sur la défense 2016 (Défense 2016) • Livre blanc sur la défense 2009 (Défense 2009) • Rapport de l'ASIO au Parlement 2011/2012 (ASIO, 2012) • Plan stratégique de l'ASIO 2013-2016 (ASIO, 2013)	Cohorte de chercheurs universitaires novateurs et de chefs de file du gouvernement/de l'industrie dans les domaines suivants : • Sécurité des réseaux et des données • Intervention en cas d'incident et informatique judiciaire • Développement de logiciels et ingénierie inverse • Effets cybernétiques • Renseignement de sources ouvertes • Lois et politiques • Relations internationales en matière de défense et de sécurité

- La politique et les conseils des 18 dernières années en Australie (et je crois que le Canada ne sera pas différent) montrent qu'il faut une main-d'œuvre hautement qualifiée pour relever les défis de la guerre cybernétique, de la cyberdéfense et de la cybersécurité et pour protéger tous les aspects de la société.
- Mes recherches, et mes connaissances du contexte australien, indiquent qu'il y a peu de recherches sur la cybersécurité pour la sécurité nationale australienne.
- Il n'y a pas de lien du secteur public entre le programme de sécurité nationale et les résultats de la recherche technique qui continuent d'être financés, mais qui ne sont pas nécessairement appliqués.
- Il n'existe pas de cadre établi sur lequel ce type de relation peut être fondée et, bien qu'il y ait de l'intérêt pour la réalisation de recherches sur de nouvelles questions difficiles comme les cyberopérations défensives, la cueillette automatisée de renseignements et de preuves cybernétiques, le leurre et certaines des questions humaines connexes, aucune recherche nationale crédible et soutenue n'est axée sur la mise en relation de la cybersécurité technique avec les visées nationales en matière de défense, de droit et de politiques.

Conseils

- Il faut créer (et mettre à l'essai et valider) un cadre pour préciser comment la cybersécurité et la cyberdéfense de l'économie canadienne et de son infrastructure essentielle pourraient être réalisées, en intégrant les perspectives techniques, sociotechniques et stratégiques.
- En l'absence de ce cadre, il faudra adopter une approche fragmentaire de la recherche universitaire sur la cybersécurité, c'est-à-dire s'appuyer sur les forces d'un chercheur ou d'un chef de recherche et sur la qualité de ses travaux antérieurs. Les études ainsi produites pourront être publiées dans un journal prestigieux, mais elles ne sauront fournir à la fois un contenu théorique à la fine pointe et des dispositifs ou techniques immédiatement utilisables et potentiellement commercialisables.

Normes professionnelles nationales en matière de cybersécurité, ensemble de connaissances commun, programmes d'études

L'Australian Computer Society est un organisme national d'accréditation informatique qui compte environ 40 000 membres. Il a élaboré un ensemble de normes professionnelles nationales en matière de cybersécurité afin que l'Australie puisse répondre aux questions « Qui est un professionnel de la cybersécurité? » et « Quel genre de compétences ces professionnels de la cybersécurité doivent-ils posséder pour répondre aux besoins de l'Australie? »

Normes professionnelles nationales

Elles ont été lancées en septembre 2017 dans le sillage des travaux effectués par le Groupe de travail sur la cybersécurité australienne (ACS) à la demande du conseiller spécial du premier ministre et chef du Australian Cyber Security Centre (ACSC), Alastair MacGibbon. Les normes ont été mises en œuvre, des évaluateurs ont été recrutés et formés et un nombre constant de nouveaux membres se prévalent maintenant de la possibilité de décrocher cette certification. Les candidats viennent de l'Australie et de l'Asie du Sud-Est et appartiennent aux divers domaines de la cybersécurité et de la TI. En résumé, les normes, tirées de la synthèse des travaux du NIST, de (ISC)^2 et d'ISACA, offrent une certification spécifique à l'Australie :

Professionnel certifié – Cybersécurité

Les exigences en matière d'évaluation de la spécialisation en cybersécurité sont équivalentes aux critères et cheminements d'évaluation des professionnels certifiés en matière de cybersécurité australienne; y est toutefois ajoutée la nécessité de démontrer une compétence approfondie dans quatre compétences du SFIA au niveau 5.

Les compétences applicables du SFIA sont les suivantes :

- Gouvernance de la TI
- Gestion de l'information
- Sécurité de l'information
- Assurance de l'information
- Gestion des risques de l'entreprise
- Test de pénétration

- Administration de la sécurité
- Programmation et développement de logiciels
- Logiciel d'exploitation
- Mise à l'essai
- Gestion des actifs

Technologue certifié – Cybersécurité

Les exigences en matière d'évaluation de la spécialisation en cybersécurité sont équivalentes aux critères et cheminements d'évaluation des technologues certifiés en matière de cybersécurité australienne; y est toutefois ajoutée la nécessité de démontrer une compétence approfondie dans trois compétences du SFIA au niveau 3.

Les compétences applicables du SFIA sont les suivantes :

- Gestion de l'information
- Sécurité de l'information
- Assurance de l'information
- Gestion des risques de l'entreprise
- Gestion du développement de systèmes
- Gestion des actifs
- Gestion du changement
- Administration de la sécurité
- Gestion des incidents
- Examen de la conformité

Enfin, nous avons deux projets d'élaboration de micro-titres de compétences et de lignes directrices pour les programmes d'études en cybersécurité. Je dirais que le Canada a besoin de la même chose pour déterminer la nature de la main-d'œuvre nécessaire et s'assurer que les programmes d'études correspondent aux besoins de cette main-d'œuvre. Je considère qu'il s'agit là des questions les plus importantes à discuter, mais je peux aussi répondre à des questions sur d'autres enjeux de recherche comme les infrastructures essentielles, l'IdO et les systèmes de déception.

Professeur Yuval Shavitt, DPT chez BGProtect – séance du 20 février 2019, SECU

Je m'appelle Yuval Shavitt, je suis professeur en génie électrique à l'Université de Tel Aviv associée au centre de cyberrecherche interdisciplinaire Blavatnik. Je suis également fondateur et dirigeant principal de la technologie chez BGProtect, une société créée pour défendre les nations et les entreprises contre les attaques de routage, donc de connectivité.

Les attaques relatives au protocole Internet (PI), également appelées attaques de déviation, sont sérieuses car elles ouvrent la porte à de nombreuses variantes d'attaques de l'intercepteur, notamment l'espionnage, la mise à niveau inférieur, le décryptage et l'usurpation d'identité. Ces attaques ciblent principalement les institutions financières compte tenu de leur potentiel lucratif tant pour les organisations criminelles que pour les gouvernements étrangers. Au cours des dernières années, nous avons documenté des attaques de déviation ciblant des organisations financières, qui comprennent de nombreuses banques moyennes et grandes, des bourses, des compagnies d'assurance et des organisations fournissant des renseignements financiers. Les attaques ne se sont pas limitées au détournement de protocole de passerelle frontière, elles ont également compris le réacheminement furtif de trafic aux points d'échange Internet et chez de grands fournisseurs de services Internet. Dans certains cas, il a fallu des semaines avant que les victimes ne se rendent compte de ces attaques.

Que peut-on faire? D'abord et avant tout, le secteur financier devrait exercer une surveillance étroite du routage vers les domaines PI cruciaux, notamment les adresses PI publiques et les serveurs PI comme le courriel, les systèmes d'adressage par domaines (DNS) et les réseaux privés virtuels (RPV). Deuxièmement, une surveillance de l'infrastructure de routage s'imposerait au niveau national pour éviter que des données provenant d'organisations financières ne soient transmises à l'étranger. Enfin, il faudrait mettre sur pied une équipe nationale d'intervention en cas d'urgence informatique (EIUI) – les États-Unis se sont dotés d'un centre de fusion – à qui les organisations financières pourront communiquer des données sur des attaques tout en étant assurées de divers niveaux d'anonymat.

La réglementation fédérale peut également aider à gérer le risque associé aux attaques relatives au protocole Internet (PI). Les lois doivent être mises à jour pour préciser qui peut être autorisé à posséder une infrastructure de communication de données sur un territoire donné. Par exemple, certains fournisseurs Internet internationaux, comme China Telecom, ont des points de présence partout dans le monde, mais la Chine ne permet pas à des fournisseurs Internet étrangers d'être présents sur son territoire. Cette asymétrie donne à China Telecom un avantage indu. Pire encore, même lorsque le coupable est identifié, celui-ci peut très facilement invoquer une erreur de configuration pour éviter les poursuites.

Comme je l'ai mentionné, je suis également dirigeant principal de la technologie chez BGProtect. Cette entreprise est chef de file en matière de détection et d'atténuation des attaques relatives au protocole Internet (PI) et à la couche de données. Notre plateforme et nos services sont actuellement utilisés dans le monde entier par des institutions financières, des gouvernements, des agences de renseignement de sécurité, des fournisseurs de service et des agences de presse internationales. Les récentes attaques ne se limitent pas au protocole de passerelle frontière, elles visent également la couche de données (p. ex. menaces aux routeurs). Notre entreprise offre le seul service capable d'identifier tous les types d'attaques de détournement de données quelle que soit la technique utilisée. Nous avons mis en place des centaines d'agents logiciels sur des serveurs situés partout dans le monde et notre base de données compte plus de 6 000 emplacements d'adresse PI de routeurs qui permettent de fournir des

résultats de mesures en temps réel et d'analyser les réseaux de routes locales et mondiales et de déceler les anomalies au moyen de notre moteur d'intelligence artificielle.

En ce qui concerne la question de Huawei, il importe de noter qu'essentiellement tout l'équipement de réseautage et de télécommunication peut être vulnérable à des attaques, notamment par des portes dissimulées, et que la meilleure façon de réduire et d'atténuer les risques consiste à investir dans de l'équipement de surveillance du trafic. En effet, « mieux vaut prévenir que guérir » comme le veut le dicton.