CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

CYBERSÉCURITÉ DANS LE SECTEUR FINANCIER COMME UN ENJEU DE SÉCURITÉ NATIONALE

Rapport du Comité permanent de la sécurité publique et nationale

L'honorable John McKay, président

JUIN 2019
42e LÉGISLATURE, 1re SESSION

CYBERSÉCURITÉ DANS LE SECTEUR FINANCIER COMME UN ENJEU DE SÉCURITÉ NATIONALE

Rapport du Comité permanent de la sécurité publique et nationale

Le président
L'hon. John McKay

JUIN 2019

42e LÉGISLATURE, 1re SESSION

AVIS AU LECTEUR

Rapports de comités présentés à la Chambre des communes

C'est en déposant un rapport à la Chambre des communes qu'un comité rend publiques ses conclusions et recommandations sur un sujet particulier. Les rapports de fond portant sur une question particulière contiennent un sommaire des témoignages entendus, les recommandations formulées par le comité et les motifs à l'appui de ces recommandations.

COMITÉ PERMANENT DE LA SÉCURITÉ PUBLIQUE ET NATIONALE

PRÉSIDENT

L'hon. John McKay

VICE-PRÉSIDENTS

Pierre Paul-Hus

Matthew Dubé

MEMBRES

Julie Dabrusin

Jim Eglinski

David de Burgh Graham

Karen McCrimmon (secrétaire parlementaire – membre sans droit de vote)

Glen Motz

Michel Picard

Ruby Sahota

Peter Schiefke (secrétaire parlementaire – membre sans droit de vote)

Sven Spengemann

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

Chandra Arya

Richard Cannings

Pam Damoff

Anju Dhillon

Earl Dreeshen

Emmanuel Dubourg

Terry Duguid

T.J. Harvey

Randy Hoback

Gudie Hutchings

Stéphane Lauzon

Dave MacKenzie
Ken McDonald
Yves Robillard
Shannon Stubbs

GREFFIER DU COMITÉ

Naaman Sugrue

BIBLIOTHÈQUE DU PARLEMENT

Service d'information et de recherche parlementaires

Holly Porteous, analyste
Dominique Valiquet, analyste

LE COMITÉ PERMANENT
DE LA SÉCURITÉ PUBLIQUE ET NATIONALE

a l'honneur de présenter son

TRENTE-HUITIÈME RAPPORT

Conformément au mandat que lui confère l'article 108(2) du Règlement, le Comité a étudié la cybersécurité dans le secteur financier comme un enjeu de sécurité économique et a convenu de faire rapport de ce qui suit :

TABLE DES MATIÈRES

LISTE DES RECOMMANDATIONS

À l'issue de leurs délibérations, les comités peuvent faire des recommandations à la Chambre des communes ou au gouvernement et les inclure dans leurs rapports. Les recommandations relatives à la présente étude se trouvent énumérées ci-après.

Recommandation 1

Recommandation 2

Recommandation 3

Recommandation 4

CYBERSÉCURITÉ DANS LE SECTEUR FINANCIER COMME UN ENJEU DE SÉCURITÉ NATIONALE

CHAPITRE 1 — CONTEXTE DE L'ÉTUDE

A. Mandat du Comité

Le 23 octobre 2018, le Comité permanent de la sécurité publique et nationale de la Chambre des communes (le Comité) a adopté la motion suivante :

> Que, conformément à l'article 108(2) du *Règlement*, le Comité entame une étude d'au moins 8 à 12 réunions sur la cybersécurité dans le secteur financier comme une question de sécurité économique nationale; que des témoins soient invités afin de mieux identifier les dangers et de proposer des mesures concrètes favorisant une meilleure protection et une meilleure prévention; que le Comité formule des recommandations et qu'il en fasse rapport à la Chambre.

Pendant les 12 réunions tenues du 28 janvier au 29 mai 2019, le Comité a entendu 45 témoins et a reçu six mémoires. Le Comité a non seulement entendu le témoignage de fonctionnaires canadiens et de représentants du secteur privé et du milieu universitaire du Canada, mais il a également entendu des témoins des États-Unis, de l'Australie et d'Israël. Le Comité se réjouit de l'expertise et de la participation de tous les témoins qui ont pris part à l'étude.

Le présent rapport constitue le premier examen de la cybersécurité effectué par le Comité. Nous espérons que le Comité SECU de la 43e législature explorera alors d'autres facettes de cette question dans de futures études et d'évaluer régulièrement les progrès réalisés par le gouvernement en ce qui concerne la mise en œuvre de ses recommandations.

Plusieurs facteurs ont poussé le Comité à commencer par le secteur financier. Le premier : la sécurité nationale et la sécurité financière sont étroitement liées[1]. Le Canada ne peut pas prétendre à une sécurité nationale robuste si les menaces qui pèsent sur les moyens de subsistance et les économies de ses citoyens et de ses

1 En fait, M. Richard Fadden, qui a occupé de nombreux postes de cadre supérieur dans le secteur canadien de la sécurité et du renseignement, a indiqué au Comité qu'il n'y a pas de distinction entre la sécurité nationale et la sécurité économique. Voir : Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Richard Fadden, à titre personnel), 42e législature, 1re session, 10 avril 2019.

entreprises ne sont pas écartées. C'est pour cette raison que le Canada, en collaboration avec ses alliés les plus proches, doit déployer tous les efforts raisonnables possibles pour prévenir les cyberagressions et les punir.

Parallèlement, le Comité reconnaît que la place du Canada sur l'échiquier international n'est pas uniquement déterminée par sa volonté d'utiliser des moyens coercitifs pour décourager les menaces, y compris les cybermenaces. Les échanges et les investissements internationaux dans ce pays sont fondés sur la confiance, qui repose quant à elle sur la fiabilité. Or, dans le contexte complexe et dynamique du cyberespace, la fiabilité n'est certainement pas une mince tâche. Pour les institutions financières canadiennes et les entreprises qui en dépendent, elle commence par de bonnes pratiques de sécurité.

Il est difficile de maintenir de bonnes pratiques de sécurité non seulement parce que les pratiques exemplaires sont en constante évolution, mais également parce que le secteur financier est confronté à des défis technologiques de taille. Bon nombre de ces défis sont imposés par le secteur lui-même. Par exemple, les banques et les autres institutions financières élargissent et numérisent les services qu'elles offrent, souvent en partenariat avec de jeunes entreprises de technologie financière (« fintech »). En tant que petites entreprises, ces jeunes entreprises « fintech » ne sont peut-être pas en mesure de se protéger pleinement contre les cybermenaces. D'autres défis sont imposés par des forces externes. Par exemple, aux différentes étapes de l'adaptation de la cybersécurité dans un monde « post-périmètre[2] », ce secteur n'a d'autre choix que de faire face aux promesses et aux dangers de l'intelligence artificielle (IA)[3] et de l'informatique quantique[4].

2 La sécurité " post-périmètre" ou " confiance zéro " fait référence à un modèle de cybersécurité qui traite tous les dispositifs connectés au réseau d'une organisation comme étant connectés à Internet, ce qui signifie qu'ils pourraient être potentiellement compromis. Contrairement aux anciens modèles orientés vers l'extérieur qui supposent que l'on peut faire confiance aux utilisateurs et aux ordinateurs fonctionnant dans le périmètre formé par un pare-feu, le modèle post-périmètre ne tient rien pour acquis et surveille en continu les signes d'activité malveillante.

3 Dans ce contexte, l'"intelligence artificielle" fait référence à l'apprentissage machine. L'apprentissage machine est un sous-ensemble de l'intelligence artificielle qui cherche à créer des machines qui peuvent apprendre à reconnaître et à tirer des conclusions sur les modèles de données sans être explicitement programmées pour le faire. Le processus est répétitif et exige généralement de diriger la machine - ou, plus précisément, l'algorithme - de façon répétée pour identifier les modèles fournis dans les ensembles de données, examiner les résultats et ajuster l'algorithme en fonction de cette rétroaction.

4 L'informatique quantique " désigne l'utilisation de phénomènes de mécanique quantique tels que le superpositionnement et l'enchevêtrement pour atteindre une capacité de calcul bien supérieure à celle de l'informatique classique actuelle. Par exemple, alors que l'informatique classique repose sur des bits électroniques qui ne peuvent exister que dans deux états (allumé (1) ou éteint (0)) l'informatique quantique exploite la capacité des particules subatomiques à exister dans plusieurs états à un moment donné. Cette superposition quantique signifie que la contrepartie quantique du bit binaire, le "qubit", peut contenir beaucoup plus d'informations.

Les témoins ont souligné que pour garder la confiance et maintenir l'avantage concurrentiel, le secteur financier doit intégrer des mesures de sécurité à toutes les nouvelles offres de services numériques. Il pourrait s'avérer désastreux de ne pas s'appuyer sur des bases solides. Le dirigeant du nouveau Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications (CST), Scott Jones, a décrit ce qui est en jeu :

> Les effets d'une perturbation substantielle sur le secteur financier pourraient avoir des répercussions qui se réverbéreraient sur l'ensemble de l'économie canadienne. Les effets d'une cyberperturbation peuvent être immédiats et entraîner des pertes financières. Ils peuvent également se faire sentir à moyen ou long terme et miner lentement la confiance des consommateurs. Le risque de cybercompromission augmente à mesure que le secteur financier continue sa transition vers des services numériques et connecte plus de dispositifs à Internet.
>
> Cette transformation a néanmoins le potentiel de créer d'immenses possibilités de croissance. En ne tirant pas parti des innovations de la technologie numérique, le Canada serait exclu de l'économie mondiale. Le retranchement n'est pas une option[5].

B. Le virage numérique des services au Canada

Le bien-être économique du Canada repose sur ses petites et moyennes entreprises (PME). M. Scott Smith, directeur principal de la propriété intellectuelle et de la politique d'innovation à la Chambre de commerce du Canada, a indiqué ce qui suit au Comité :

> [M]ême si 99,7 % des entreprises au Canada comptent moins de 500 employés, elles emploient plus de 70 % de la main-d'œuvre du secteur privé. Les PME représentent 50 % du [produit intérieur brut, PIB] du Canada, 75 % du secteur des services et 44 % du secteur de la production de biens. Elles représentent également 39 % du secteur des finances, des assurances et des biens immobiliers[6].

Les PME représentent peut-être un peu plus de la moitié de la valeur de la production canadienne, mais une autre étude récemment menée par un comité de la Chambre des communes laisse entendre que ces entrepreneurs n'ont pas encore atteint leur plein

5 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Jones, dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications), 42e législature, 1re session, 30 janvier 2019.

6 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Smith, directeur principal, Propriété intellectuelle et politique d'innovation, Chambre de commerce du Canada), 42e législature, 1re session, 18 mars 2019.

potentiel d'exportation[7]. Selon la Banque de développement du Canada, par exemple, la cybersécurité est l'un des principaux défis des entreprises en ce qui concerne le commerce électronique[8]. La perspective de se préparer à lutter contre les cybermenaces tout en essayant de maintenir une entreprise en ligne à flot est-elle trop intimidante pour certains? Peut-être. Startup Canada a indiqué que 44 % des petites entreprises faisant partie de son réseau voient les « coûts élevés » associés à la recherche, à l'intégration et à l'entretien des technologies numériques comme les « principaux obstacles à l'adoption de la technologie[9] ».

Pour pénétrer les marchés internationaux et faire de nouvelles percées auprès de la clientèle canadienne, les PME canadiennes doivent néanmoins adopter la livraison numérique. Les institutions financières et les entreprises de technologie financière sont un élément central de ce processus de numérisation parce qu'elles facilitent les transactions en ligne et les transactions mobiles. Par exemple, les petites entreprises se tournent vers des plateformes de paiement en ligne pour atteindre les marchés internationaux. PayPal, la plus grande de ces plateformes et l'une des plus vieilles entreprises de technologie financière (à 21 ans), compte 250 000 petites entreprises canadiennes parmi ses clients[10].

Avec un taux de croissance annuel prévu de 55 % en 2020, le Canada est devenu un « centre névralgique » du secteur de la technologie financière. M. Smith a attiré l'attention du Comité sur le fait que la plupart de ces nouvelles entreprises du secteur de la technologie financière sont des PME axées sur les paiements mobiles et il a souligné qu'ensemble, ces petits joueurs « constituent une très grande surface d'attaque[11] ».

---

7 Voir, par exemple : Comité permanent du commerce international de la Chambre des communes, *Commerce électronique : Regard sur certaines priorités commerciales des entreprises canadiennes*, Neuvième rapport, 42e législature, 1re session, avril 2018.

8 Comité permanent du commerce international de la Chambre des communes, *Commerce électronique : Regard sur certaines priorités commerciales des entreprises canadiennes*, Neuvième rapport, 42e législature, 1re session, avril 2018, p. 19.

9 Comité permanent du commerce international de la Chambre des communes, *Commerce électronique : Regard sur certaines priorités commerciales des entreprises canadiennes*, Neuvième rapport, 42e législature, 1re session, avril 2018, p. 19.

10 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Brian Johnson, directeur principal, Sécurité de l'information, PayPal Inc.), 42e législature, 1re session, 29 mai 2019.

11 Par "surface d'attaque" (également appelée "surface de menace"), on entend tous les points finaux accessibles sur Internet que les attaquants peuvent tenter d'exploiter pour atteindre leurs objectifs. Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Smith, directeur principal, Propriété intellectuelle et politique d'innovation, Chambre de commerce du Canada), 42e législature, 1re session, 18 mars 2019.

Les statistiques sur la vaste numérisation des transactions bancaires au Canada sont éloquentes. Quatre-vingt-dix % des Canadiens utilisent Internet[12] et, selon la Chambre de commerce du Canada, 72 % des Canadiens effectuent leurs transactions bancaires en ligne ou à l'aide d'un appareil mobile[13].

Les Canadiens magasinent de plus en plus en ligne; 86 % des adultes ayant fait un achat en ligne au cours des 12 derniers mois[14]. En janvier 2019 seulement, les ventes au détail en ligne pour le Canada ont été estimées à 1,4 milliard de dollars, ce qui représente 3,3 % de l'ensemble du commerce au détail[15]. Un récent sondage réalisé par Statistique Canada a révélé qu'entre 2010 et 2017, la contribution du commerce électronique à l'économie numérique a doublé, pour passer de 5,5 % à 12,4 %[16]. La Banque de développement du Canada prévoit que d'ici 2020, les ventes au détail en ligne au Canada s'élèveront à 56 milliards de dollars[17].

Recommandation 1

Le Comité recommande que, lors du prochain Parlement, le Comité permanent de la sécurité publique et nationale de la Chambre des communes crée un sous-comité chargé d'étudier les aspects de la cybersécurité qui ont trait à la sécurité publique et à la sécurité nationale, notamment sur les approches internationales de la protection des infrastructures essentielles, l'incidence des nouvelles technologies et la cybersécurité de la chaîne d'approvisionnement numérique.

12 Autorité canadienne pour les enregistrements Internet, *Le dossier documentaire d'Internet 2018*.

13 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Trevin Stratton, économiste en chef, Chambre de commerce du Canada), 42e législature, 1re session, 18 mars 2019.

14 Autorité canadienne pour les enregistrements Internet, *Le dossier documentaire d'Internet 2018*.

15 Statistique Canada, *Tableau 4, Vente au détail en ligne — Données non désaisonnalisées, février 2019*. Veuillez prendre note que Statistique Canada précise que ce tableau n'est pas désaisonnalisé.

16 Veuillez prendre note que dans ce sondage, Statistique Canada définit l'économie numérique comme les « activités qui favorisent la numérisation ou qui sont grandement touchées par cette dernière ». Statistique Canada ajoute que l'économie numérique « [comprend] le matériel lié aux technologies de l'information dont l'économie numérique dépend pour fonctionner, ainsi que les opérations du commerce électronique et la livraison numérique de produits aux consommateurs ». Voir : Statistique Canada, « Mesurer les activités économiques numériques au Canada, 2010 à 2017 », *Le Quotidien Daily*, 3 mai 2019.

17 Banque de développement du Canada, citée dans : Comité permanent du commerce international de la Chambre des communes, *Commerce électronique : Regard sur certaines priorités commerciales des entreprises canadiennes*, Neuvième rapport, 42e législature, 1re session, avril 2018, p. 7.

CHAPITRE 2 — DÉFIS, MENACES ET ATTÉNUATION DES RISQUES

A. Cybersécurité dans un monde post-périmètre

Dans le cadre de l'étude, le Comité a appris que les pratiques exemplaires en matière de cybersécurité ont connu de profonds changements au cours de la dernière décennie. Les programmes antivirus, les pare-feux et les systèmes de détection d'intrusions ont toujours leur place dans la cybersécurité organisationnelle, mais le contexte lié à leur utilisation a complètement changé.

Il ne suffit plus de déployer ces outils en croyant qu'ils formeront un périmètre solide séparant l'espace interne fiable de l'espace externe non fiable de réseaux publics (c'est-à-dire l'Internet). Les politiques permettant aux employés d'apporter leurs propres appareils, les clés USB et le piratage psychologique[18] ont tous permis de percer des trous dans le système de défense du périmètre. Selon les témoins, les organisations sont contraintes de présumer qu'il y aura des infractions et de continuellement en chercher des signes.

Cette chasse repose sur toute une gamme de données qui doivent être analysées et auxquelles il faut donner suite rapidement afin de freiner la menace dans sa lancée. L'IA est un partenaire naturel des responsables de la cybersécurité à cet égard parce qu'elle permet l'identification automatique de la menace et, dans certaines circonstances, une réponse automatique.

Il est devenu évident pour le Comité que les grandes organisations du secteur financier ont intégré des outils d'IA à leurs programmes de cybersécurité, mais des témoins ont indiqué que les PME (tant celles qui appartiennent au secteur financier que celles qui en dépendent) ne sont pas nécessairement en mesure d'en faire autant.

Compte tenu de l'éventail d'auteurs de menace qui ciblent les institutions financières canadiennes, du rythme accéléré auquel les changements technologiques se produisent dans ce secteur et de l'ampleur des activités économiques canadiennes qui se déroulent maintenant dans un contexte numérique, il est évident qu'il faut examiner la cybersécurité. La numérisation a non seulement ouvert de nouveaux marchés pour les

18 Comme son nom l'indique, l'attaque de piratage psychologique consiste à contourner les politiques de sécurité grâce à une manipulation psychologique. Dans un document de sensibilisation à l'intention du public, le Centre de la sécurité des télécommunications décrit toute une gamme de techniques de cyberattaque, donc le piratage psychologique. Voir : Centre canadien pour la cybersécurité, « Annexe A : Les outils de l'auteur de cybermenaces », *Introduction à l'environnement de cybermenaces*.

entreprises canadiennes, mais elle a également élargi de façon marquée la « surface d'attaque » disponible pour les auteurs de cybermenaces qui veulent cibler le Canada[19].

B. Contexte de la menace

Les témoins ont tous décrit un contexte de la menace qui évolue inexorablement. Ils ont indiqué que les banques, les caisses populaires, les sociétés de fiducie et les autres institutions financières sont confrontées à des auteurs de menace étatiques et non étatiques qui sont opportunistes et qui modifient continuellement leurs tactiques et leurs techniques.

La nature opportuniste de ces auteurs de menace est ressortie de la description faite par la Gendarmerie royale du Canada (GRC) de la manière dont les cybercriminels ciblent le secteur financier du Canada. Ils attaquent directement l'infrastructure de base des institutions financières et, si cela ne fonctionne pas, ils vont plus en aval pour cibler les utilisateurs individuellement. Voici comment le directeur général de l'unité Criminalité financière et cybercriminalité de la GRC, le surintendant principal Mark Flynn, a décrit le mode de fonctionnement des cybercriminels :

> Les cybercriminels peuvent tenter de compromettre directement l'infrastructure informatique d'une institution financière au moyen d'attaques qui accordent un accès non autorisé au système de base lui-même. Ces attaques visent à réaliser des profits en volant ou en transférant de l'argent dans ces systèmes, en volant des informations privées ou, dans certains cas, en portant atteinte à la réputation de l'entreprise. Ces crimes sont perpétrés par des personnes qui travaillent seules, des groupes du crime organisé ou des cybercriminels professionnels employés par de grandes entités, y compris des États hostiles.
>
> De plus, les criminels s'attaquent indirectement aux institutions financières en obtenant des justificatifs d'identité d'utilisateur ou d'autres renseignements personnels pour accéder sans autorisation à des comptes d'utilisateurs individuels. L'obtention de ces justificatifs d'identité peut se faire de plusieurs façons : en utilisant des outils accessibles sur Internet pour obtenir des mots de passe; en recourant à l'ingénierie sociale; ou simplement en achetant de grandes bases de données de renseignements personnels sur le Web invisible. Le coût relativement faible de ces attaques a permis à des individus

19 Le Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications (CST) utilise un terme légèrement différent, « l'exposition à la menace », qu'il définit comme « tous les points terminaux qu'un auteur de menace peut tenter d'exploiter sur des dispositifs connectés à Internet dans un contexte de cybermenace ». Le CST ajoute ce qui suit : « Les services, les dispositifs et les données peuvent tous être ciblés afin de compromettre les systèmes de production et de livraison, comme les chaînes d'approvisionnement et les systèmes de gestion des services. L'exposition aux menaces augmentera à mesure que ces processus continueront d'évoluer. » Voir : Centre canadien pour la cybersécurité, « Annexe A : Les outils de l'auteur de cybermenaces », *Introduction à l'environnement de cybermenaces*, 2018.

> malveillants et à de nouveaux cybergroupes du crime organisé de lancer des attaques à une échelle sans précédent[20].

Il convient de souligner que la GRC a rappelé que les renseignements personnels détenus par les banques et les autres institutions financières intéressent beaucoup les cybercriminels, particulièrement alors que le secteur financier commence à envisager d'adapter ses offres de services grâce à des analyses poussées des données des clients obtenues via l'Internet des objets (IdO)[21].

Nous avons constaté, dans la foulée des attaques des botnets Mirai[22], que les dispositifs de l'IdO mal sécurisés sont omniprésents. Aucun témoin n'évaluait de manière positive l'état actuel de la sécurité de l'IdO. M. Christopher Porter, chef d'intelligence stratégique chez FireEye Inc., a parfaitement résumé la situation : « Ce qui me préoccupe le plus au sujet de l'Internet des objets […] – l'ensemble des appareils physiques connectés à Internet – c'est que bon nombre de ces appareils ne peuvent pas du tout être mis à jour. Même si une faille est découverte, il est techniquement impossible de la corriger[23] ». M. Scott Jones est allé un peu plus loin en exhortant l'industrie à exiger davantage de la part des fournisseurs de produits. Voici précisément ce qu'il a déclaré :

> Je pense que le problème principal pour nous, c'est que l'équipement que nous achetons n'est pas sécurisé par défaut; vous avez raison. L'équipement est de piètre facture, et cela va de mal en pis avec l'Internet des objets. Nous devons changer cette dynamique, et nous encourageons l'industrie à réclamer l'inclusion de dispositifs de sécurité dans l'équipement. Les entreprises ne devraient pas payer de suppléments à cette fin. Certains dispositifs de sécurité devraient être inclus dans n'importe quel équipement[24].

---

20 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Surintendant principal Mark Flynn, directeur général, Criminalité financière et cybercriminalité, Opérations criminelles de la police fédérale, Gendarmerie royale du Canada), 42e législature, 1re session, 28 janvier 2019.

21 Voir, par exemple : Jim Eckenrode, directeur exécutif, Deloitte Center for Financial Services, Deloitte U.S., « Future Scenarios for IoT in Financial Services », contenu commandité, *CIO Journal, The Wall Street Journal*, 6 janvier 2016.

22 Mirai est le nom donné au maliciel utilisé pour créer de multiples réseaux d'objets connectés compromis. Les « botnets » qui en ont résulté ont quant à eux été utilisés pour perpétrer une série de cyberattaques qui ont tout d'abord attiré l'attention du public en 2016 lorsque des attaques par déni de service sur des serveurs de nom de domaine Internet exploités par l'entreprise américaine Dyn ont entraîné des interruptions des services Internet en Europe et en Amérique du Nord. Voir : Brian Krebs, « Mirai Botnet Authors Avoid Jail Time », *Krebs on Security* (blogue), 19 septembre 2018.

23 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Christopher Porter, chef d'intelligence stratégique, FireEye Inc.), 42e législature, 1re session, 6 février 2019.

24 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Jones, dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications), 42e législature, 1re session, 30 janvier 2019.

M. Mark Ryland, directeur du Bureau du dirigeant principal de l'information d'Amazon Web Services, a déclaré au Comité que les fournisseurs commencent à relever le défi de la " sécurité dès la conception " :

> [N]ous avons tous reconnu dans le passé les problèmes avec l'IdO – les appareils domestiques, etc. – qui était déployé de façon très peu sécuritaire. Par le passé, c'était la chose la moins coûteuse et la plus facile à faire. Si vous examinez la technologie récente que nous offrons, ou celle que Microsoft ou d'autres gros fournisseurs vous offrent, par défaut, leurs systèmes sont beaucoup plus sécuritaires. Vous pouvez les mettre à jour par substitution, ce qu'il n'était pas possible de faire auparavant. Ils utilisent des protocoles sécurisés par défaut; ils ne le faisaient pas auparavant. Vous pouvez aller directement au bas de la liste pour savoir comment les intérêts commerciaux de ces gros fournisseurs s'harmonisent avec la conception de systèmes qui sont sécurisés par défaut, tandis que, auparavant, cette fonction revenait à la personne qui concevait le réfrigérateur intelligent, le grille-pain intelligent ou quoi que ce soit d'autre[25].

L'IdO représente sans contredit un important vecteur de menaces pour le secteur financier et le Comité estime qu'il faut déployer tous les efforts possibles pour enrayer cette menace.

Recommandation 2

En plus d'encourager les Canadiens à adopter de saines habitudes de cyberhygiène, le Comité recommande que le gouvernement du Canada fasse des efforts pour s'assurer que les produits et services numériques sur lesquels ils comptent, y compris les produits qui font partie de l'Internet des objets, soient « sécuritaires dès leur conception ».

Pour atteindre cet objectif, les témoins ont dit au Comité que le partenariat public-privé sera essentiel. Le chef de l'exploitation de Paiements Canada, M. Justin Ferrabee, a décrit la portée de la collaboration de son organisation comme suit :

> D'un vaste point de vue industriel axé sur la collaboration, nous travaillons très étroitement avec des partenaires du secteur financier par l'entremise de groupes industriels du domaine de la cybersécurité, comme le Conseil canadien de gouvernance en matière de cybersécurité des services financiers, le groupe de spécialistes de la cybersécurité de l'Association des banquiers canadiens et du Financial Services Sharing and Analysis Center.
>
> Par ailleurs, nous participons à des exercices pour la continuité des activités et la cyberrésilience au sein de l'industrie et dirigeons de tels exercices, et nous échangeons

25 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Mark Ryland, directeur, Bureau du dirigeant principal de l'information, Amazon Web Services), 42e législature, 1re session, 15 mai 2019.

> des renseignements avec des organismes et organisations partenaires dans le milieu de la cybersécurité. Il s'agit notamment du Centre canadien pour la cybersécurité, de la Direction générale de la protection des infrastructures essentielles de Sécurité publique Canada, de l'Équipe nationale des infrastructures essentielles de la GRC et de l'Échange canadien de menaces cybernétiques. En plus de ces collaborations, nous intervenons activement au sein du milieu international du cyberrisque avec nos partenaires de la Banque du Canada[26].

Le travail de Glenn Foster, chef de la sécurité de l'information à la Banque TD, consiste à surveiller les cybermenaces dans le secteur financier. Il a souligné l'agilité avec laquelle ses adversaires arrivent à cerner et à exploiter les nouveaux vecteurs de menaces :

> Les attaques actuelles sont très sophistiquées. Elles changent d'un jour à l'autre. Entre le moment où le public est ciblé [vulnérabilité jour zéro[27]], le moment où le fournisseur commercial peut apporter des correctifs et le moment où les grandes institutions peuvent corriger les vulnérabilités constatées, le battement, même s'il est toujours plus bref, est toujours trop long vu la vitesse à laquelle les adversaires peuvent élaborer des scripts et commencer à balayer tous les comptes sur Internet. Le recours à l'automatisation et, dans certains cas, à l'intelligence artificielle pour détecter plus rapidement les vulnérabilités commence à nous poser de sérieux problèmes[28].

Pire encore, selon les spécialistes de la cybersécurité qui ont comparu devant le Comité, le temps d'arrêt (*dwell time*) moyen pour un pirate qui est arrivé à infiltrer un réseau corporatif sans être détecté est de 101 jours, alors qu'il est de six mois dans les cas où un pirate est arrivé à infiltrer un centre de données corporatif[29]. Le pirate a donc amplement le temps de se déplacer latéralement dans le réseau interne et les fonds de données de l'entreprise touchée, de s'accaparer en douce des renseignements les plus sensibles de l'entreprise et d'implanter un autre maliciel qui peut être activé ultérieurement, au besoin.

---

26 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Justin Ferrabee, chef des opérations, Paiements Canada), 42e législature, 1re session, 8 avril 2019.

27 Une « vulnérabilité jour zéro » est une faille de sécurité d'un logiciel, qui peut être exploitée et qui est inconnue des personnes responsables d'assurer la sécurité du logiciel, ou qui n'a pas été réglée par ces derniers.

28 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Glenn Foster, chef de la sécurité de l'information, Banque Toronto), 42e législature, 1re session, 3 avril 2019.

29 Le directeur de la cybersécurité pour le Groupe ADGA, Steven Drennan, a indiqué que le temps d'arrêt moyen dans le monde était de 101 jours pour le *réseau* d'une organisation, tandis que le chef de la stratégie de cybersécurité pour Illumio, Jonathan Reiber, a indiqué que le temps d'arrêt moyen était de six mois pour le *centre de données* d'une organisation. Voir : Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Steve Drennan, directeur, Cybersécurité, Groupe ADGA), 42e législature, 1re session, 10 avril 2019; et Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Mémoire : Se défendre en amont et supposer qu'il y a eu intrusion : Préparer le Canada à un avenir cyberrésilient* (Jonathan Reiber, chef, Stratégie de cybersécurité, Illumio), 42e législature, 1re session, 10 avril 2019, p. 3.

Le Comité n'a pas obtenu de données propres au secteur financier en ce qui concerne le temps d'arrêt moyen des pirates. Il ne peut donc qu'espérer que ce secteur enregistre de meilleurs résultats à cet égard.

Scott Jones, dirigeant principal du nouveau Centre canadien pour la cybersécurité du CST, a cité un récent rapport de Statistique Canada[30] qui indique que « près de la moitié des organisations canadiennes du secteur bancaire [ont] été touchées par des cyberincidents de sécurité en 2017 ». Il a affirmé que les cybercriminels constituent la principale menace pour le secteur financier[31]. Il a ajouté que les États-nations et les auteurs de menace parrainés par des États sont moins préoccupants, même s'ils cherchent à créer des perturbations. De fait, il a expliqué que parmi les dix infrastructures essentielles du Canada, le secteur financier est une cible « relativement difficile » à perturber pour un État-nation. D'après ce témoignage et celui d'autres témoins, le secteur financier semble donc, dans l'ensemble, s'en tirer mieux que la plupart des secteurs en ce qui concerne les pratiques exemplaires en matière de cybersécurité.

Toutefois, même si bon nombre d'organisations du secteur financier arrivent à bien protéger leurs actifs contre les cybermenaces, le Comité se préoccupe des petites entreprises de ce secteur. Les commentaires de la GRC à propos de l'opportunisme des criminels nous viennent en tête, tout comme les observations de la Chambre de commerce du Canada voulant que les PME dominent le secteur canadien des technologies financières. M. Smith a indiqué ce qui suit à ce sujet :

> Les PME font face à plusieurs difficultés en matière de sécurité : des ressources financières limitées, des ressources humaines limitées et une culture d'incrédulité, à savoir la fausse idée selon laquelle elles sont trop petites pour être victimes de piratage[32].

Pour que le secteur financier soit véritablement protégé contre les cybermenaces, il faut que la sécurité soit intégrée du début à la fin du processus. Comme l'a illustré Satyamoorthy Kabilan, vice-président, Politiques, Forum des politiques publiques :

> [La cybersécurité dans le secteur financier,] c'est comme si on avait des véhicules blindés avec des agents armés qui feraient passer de l'argent entre deux boîtes en

30 Voir : Howard Bilodeau, Mohammad Lari et Mark Uhrbach, *Les défis des entreprises canadiennes quant à la cybersécurité et au cybercrime, 2017*, Statistique Canada, 28 mars 2019.

31 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Jones, dirigeant principal, Centre canadien pour la cybersécurité), 42e législature, 1re session, 30 janvier 2019.

32 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Smith, directeur principal, Propriété intellectuelle et politique d'innovation, Chambre de commerce du Canada), 42e législature, 1re session, 18 mars 2019.

> carton. Ce qui nous préoccuperait là-dedans, ce serait la boîte en carton en fin de processus, parce qu'il se peut que l'utilisateur au bout de la ligne ne soit pas aussi bien protégé que la banque, l'institution financière ou le fournisseur de services, ou qu'il ne comprenne pas les choses aussi bien qu'eux[33].

C. Atténuation des risques

Il subsiste des aspects préoccupants, particulièrement en ce qui concerne les PME et la cybersécurité des consommateurs, mais le Comité estime que les grandes organisations du secteur financier sont axées sur les cybermenaces et prennent des mesures appropriées d'atténuation des risques. De fait, le recours novateur à l'IA pour la détection des fraudes dans ce secteur a fait en sorte qu'il était mieux positionné que la plupart des secteurs pour commencer à utiliser cette technologie afin de détecter les menaces à la cybersécurité et y réagir. Selon Scott Jones, le secteur financier dispose de capacités de pointe en matière d'utilisation de l'IA pour détecter la fraude et le CST cherche à tirer parti de cette expertise à des fins de cyberdéfense[34].

M. Jonathan Reiber, responsable de la stratégie de cybersécurité d'Illumio, une société américaine, a confirmé que le secteur financier dispose d'atouts importants en matière de cybersécurité. Ces forces sont celles de ceux qui ont été endurcis au combat, a-t-il dit, affirmant que :

> Le secteur financier est particulier dans la mesure où il est assiégé depuis son arrivée sur Internet. Il y a déjà eu un certain nombre d'infractions majeures qui ont retenu l'attention des responsables de la sécurité nationale et des intervenants du secteur des banques, et ce dernier en est venu à investir des sommes considérables en cybersécurité. C'est pour cette raison qu'il a tellement d'avance.
>
> Peut-être l'ai-je déjà mentionné, mais les banques sont bien plus avancées que bien d'autres secteurs économiques aux États-Unis. On pourrait raisonnablement supposer qu'il en est ainsi parce qu'elles ont les moyens d'attirer les employés les plus compétents. Elles ont les moyens de verser de bons salaires à quiconque est prêt à travailler fort[35].

---

33 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Satyamoorthy Kabilan, vice-président, Politiques, Forum des politiques publiques), 42e législature, 1re session, 30 janvier 2019.

34 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Jones, dirigeant principal, Centre canadien pour la cybersécurité), 42e législature, 1re session, 30 janvier 2019.

35 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Jonathan Reiber, chef, Stratégie de cybersécurité, Illumio), 42e législature, 1re session, 6 février 2019.

Il est également évident que les intervenants de ce milieu sont habitués à collaborer sur les questions de sécurité. Par exemple, des témoins ont indiqué à maintes reprises qu'ils étaient tout à fait ouverts à travailler avec le Centre canadien pour la cybersécurité et la nouvelle Unité nationale de lutte contre la cybercriminalité de la GRC. Des témoins ont aussi souligné la contribution utile qu'apporte déjà l'Échange canadien de menaces cybernétiques (ECMC), un organisme sans but lucratif, pour l'échange d'information.

L'ECMC est un organisme sans but lucratif basé à Ottawa qui offre une solution permettant aux entreprises, notamment les banques, de partager de l'information sur les menaces et les vulnérabilités, de même que sur les pratiques exemplaires en matière de cybersécurité. Ses neuf membres fondateurs, qui comprennent la Banque Toronto Dominion et la Banque Royale du Canada, sont toutes de grandes entreprises[36]. Toutefois, depuis que l'ECMC a amorcé ses activités en décembre 2016, l'organisme CCTX cherche activement à attirer de petites entreprises grâce à des frais d'adhésion réduits[37]. M. Bob Gordon, directeur exécutif de l'ECMC, a décrit les efforts déployés par son organisation en vue d'atteindre cet objectif :

> [L]es grandes entreprises qui ont fondé l'ECMC ont clairement indiqué que l'ECMC ne pouvait pas servir uniquement les grandes organisations. Nous devons attirer des PME. Dans tous les secteurs de l'économie, des organisations de toutes tailles subissent des cyberattaques. Nous sommes passés des neuf premiers membres fondateurs à un peu moins de 60 membres aujourd'hui, et d'autres demandes d'adhésion sont traitées toutes les semaines.
>
> En janvier dernier, nous avons changé la composition et les barèmes tarifaires de notre organisme de manière à rendre l'adhésion plus attrayante pour les PME. Ces changements ont été bien reçus. Les petites organisations représentent maintenant 28 % de notre effectif, et nous déployons des efforts pour que ce nombre augmente considérablement. À mesure que nous augmentions le nombre de petites organisations, nous avons mis au point des rapports et des services adaptés aux besoins des propriétaires de petites entreprises[38].

Chaque organisation doit assumer individuellement la responsabilité relative à l'atténuation des risques en matière de cybersécurité, mais la collaboration à l'échelle du secteur et le partage d'information sont les *seules* manières de diminuer les risques

---

36 Échange canadien de menaces cybernétiques, *About CCTX: Founding Members + Advisory Board* [DISPONIBLE EN ANGLAIS SEULEMENT].

37 Cision, « The Canadian Cyber Threat Exchange (CCTX) is operational and reaching out to Canadian businesses », nouvelles émanant de l'Échange canadien de menaces cybernétiques, 9 décembre 2016.

38 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Bob Gordon, directeur exécutif, Échange canadien de menaces cybernétiques), 42e législature, 1re session, 1er avril 2019.

systémiques dans ce domaine. À cet égard, le Comité note également le rôle clé joué par Paiements Canada, qui offre des mesures de cybersécurité à l'ensemble du secteur.

Paiements Canada exploite les deux systèmes de paiements du pays, le Système de transfert de paiements de grande valeur (STPGV) et le Système automatisé de compensation et de règlement (SACR). En raison du rôle essentiel qu'ils jouent pour ce qui est de la stabilité du système financier du Canada, le STPGV et le SACR ont été désignés comme des « infrastructures de marchés financiers » (IMF) par la Banque du Canada aux termes de la *Loi sur la compensation et le règlement des paiements*. Si l'un ou l'autre de ces systèmes subissait une défaillance majeure, cela entraînerait une profonde perte de confiance à l'égard de notre système financier. Paiements Canada doit donc répondre aux exigences de la Banque du Canada, c'est-à-dire que le STPGV et le SACR doivent être « aptes à résister aux chocs » (ce qui signifie qu'ils doivent pouvoir se relever rapidement de toute cyberattaque[39]).

CHAPITRE 3 — SÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT NUMÉRIQUE

Compte tenu du rôle central que joue Paiements Canada en matière de cybersécurité, le Comité prend bonne note que le chef des opérations de Paiements Canada, M. Justin Ferrabee, a demandé la mise en place d'un système s'apparentant aux normes d'étiquetage alimentaire, mais pour les logiciels. Voici comment il a expliqué sa proposition :

> La chaîne d'approvisionnement moderne comprend souvent des centaines, voire des milliers, de composants logiciels qui sont intégrés dans des systèmes essentiels provenant d'entreprises et de communautés de partout dans le monde.
>
> Il est important de faire le suivi et l'inventaire de tous les composants d'un système et de s'assurer qu'ils restent sécurisés. Dans le milieu de la salubrité des aliments, des normes d'étiquetage obligent les entreprises à informer les clients au sujet des ingrédients des produits et de leur valeur nutritive, mais, dans le monde informatique, aucune norme de ce genre n'aide les clients à comprendre quels composants et risques pourraient être associés au logiciel. Une politique favorisant l'atténuation du risque pour la chaîne d'approvisionnement numérique est nécessaire, et l'étiquetage

39 Voir aussi : Banque du Canada, Filipe Dinis, chef de l'exploitation, « Renforcer nos cyberdéfenses », présentation à Paiements Canada, Toronto, Ontario, 9 mai 2018.

> systémique des composants logiciels devrait être étudié du point de vue de ses avantages pour l'économie[40].

Si nous reprenons cette analogie, nous pouvons dire que Paiements Canada suggère la mise en place d'un système obligatoire de « nomenclature » pour les logiciels. Pour être autorisés à vendre leurs produits au Canada, tous les fabricants de logiciels seraient tenus de fournir des renseignements exhaustifs sur ces derniers. Comme sur l'étiquetage des aliments, ces renseignements pourraient comprendre le ou les pays d'origine, les « ingrédients » (c'est-à-dire toutes les caractéristiques et fonctionnalités du logiciel), les « allergènes » (c'est-à-dire les déclarations relatives aux vulnérabilités) et la « date de péremption » (c'est-à-dire la date à partir de laquelle le fournisseur n'offrirait plus de correctifs de sécurité pour le produit). Dans le cadre de ce système, les fabricants de logiciels dresseraient la liste de tous les composants de logiciels utilisés dans la fabrication de leur produit, déclareraient que le logiciel n'a pas de vulnérabilités connues ou contient la version publique du logiciel la moins vulnérable, et offriraient un mécanisme pour corriger les vulnérabilités qui se produiraient pendant la durée de vie déclarée du produit.

Le Comité estime qu'il serait utile d'obliger les fabricants de logiciels à faire preuve de plus de transparence à l'égard de leurs produits, mais des questions demeurent en ce qui concerne la manière dont cette approche d'étiquetage pourrait fonctionner à l'extérieur des environnements hautement sécurisés et être mises en œuvre dans le contexte du cadre normatif international existant [41].

Pour des raisons de sécurité, tous les systèmes exploités dans un environnement hautement sécurisé doivent avoir obtenu une certification précisant qu'ils fonctionnent exactement comme prévu. Essentiellement, on peut être assuré que les systèmes qui

---

40 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Justin Ferrabee, chef des opérations, Paiements Canada), 42e législature, 1re session, 8 avril 2019.

41 En raison de la demande des consommateurs, les pratiques actuelles de développement des logiciels commerciaux favorisent des cycles de commercialisation rapide. Plutôt que de perdre un temps précieux à créer des logiciels à partir de rien, les développeurs se tournent vers une multitude de cadres de développement de logiciels, de systèmes d'exploitation et de bibliothèques de codes en libre accès et répartis sur plusieurs pays. Compte tenu de cette réalité, il serait extrêmement difficile de procéder au catalogage de tous les composants qui servent à la conception d'un logiciel en fournissant assez de précisions pour contribuer au suivi de la vulnérabilité. Des milliers de sous-composants peuvent être utilisés pour la conception d'une simple application logicielle. Comme l'a souligné un intervenant de l'industrie de la cybersécurité, énumérer seulement l'ensemble des modules logiciels sous licence, plutôt que l'ensemble des sous-composants individuels de ces modules logiciels, pourrait permettre d'avoir une liste relativement courte, mais ne fournirait pas assez d'information pouvant être utilisée dans le cas où une vulnérabilité serait découverte dans un sous-composant. Voir en apprendre davantage, voir : Rob Graham, « Security Essentials: Software Bill of Materials (SBoM) — Does It Work for DevSecOps? », AT&T Cybersecurity (blogue), 14 janvier 2019.

ont été certifiés pour être utilisés dans un environnement hautement sécurisé ne comprennent pas de fonction cachée (p. ex. des portes dérobées) pouvant être exploitée à des fins malveillantes. Pour se conformer à cette exigence, les systèmes sont fabriqués en respectant des normes strictes, font l'objet de tests et d'évaluations rigoureux, et sont certifiés comme sûrs lorsqu'ils sont exploités dans une configuration particulière. Ainsi, les logiciels certifiés pour être utilisés dans un environnement hautement sécurisé offrent des fonctions restreintes et demeurent stables au fil du temps.

De nombreux témoins ont abondé dans le sens de M. Ferrabee en ce qui concerne l'importance de tenir compte des risques liés à la chaîne d'approvisionnement numérique. M. Ferrabee a mis l'accent sur les composants logiciels, tandis que d'autres témoins ont adopté une approche plus large. Satyamoorthy Kabilan, vice-président des politiques au Forum des politiques publiques, a inclus les fournisseurs de services dans sa définition, en affirmant que les chaînes d'approvisionnement numérique ne comprennent « pas seulement des pièces que nous achetons, mais aussi des organisations qui nous fournissent des services[42] ».

À cet égard, la réponse de l'Association des banquiers canadiens (ABC) aux questions du Comité au sujet des obligations des institutions financières envers leurs clients lorsqu'elles impartissent des services à des tiers fournisseurs étrangers était préoccupante. Interrogé sur ce qui se produirait dans le cas où une banque canadienne sous-traiterait à une société américaine émettrice de cartes de crédit et que cette dernière subissait une atteinte à la cybersécurité qui exposerait des renseignements sur des clients canadiens, M. Charles Docherty, avocat général adjoint de l'ABC, a expliqué que : « S'il s'agit d'un tiers indépendant, les lois du pays où l'information est détenue par ce tiers pourraient s'appliquer »[43].

A. Le rôle du CST dans l'assurance de la sécurité de la chaîne d'approvisionnement numérique pour les infrastructures essentielles

Le Centre de la sécurité des télécommunications (CST) joue un rôle central pour assurer la sécurité de la chaîne d'approvisionnement numérique en ce qui concerne les

42 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Satyamoorthy Kabilan, vice-président, Politiques, Forum des politiques publiques), 42e législature, 1re session, 30 janvier 2019.

43 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Charles Docherty, avocat général adjoint, Association des banquiers canadiens), 42e législature, 1re session, 18 mars 2019.

infrastructures essentielles. Depuis 2013, en partenariat avec Sécurité publique Canada et Innovation, Sciences et Développement économique, le CST supervise un programme de tests et d'évaluations pour certaines pièces d'équipement que les fournisseurs de services de télécommunications envisagent de déployer dans leurs réseaux (ce programme est désigné sous le nom de programme d'examen de la sécurité canadien). Des laboratoires tiers indépendants qui ont obtenu l'accréditation du CST sont utilisés pour procéder à des tests et à des évaluations sur les produits[44].

La participation du secteur privé au programme d'examen de la sécurité canadien se déroule maintenant sous l'égide du Centre canadien pour la cybersécurité du CST, qui a été créé le 1er octobre 2018.

Lors de son témoignage devant le Comité, M. Scott Jones a souligné l'attention accordée à la sécurité de la chaîne d'approvisionnement numérique dans l'*Évaluation des cybermenaces nationales 2018* réalisée par le CST et il a affirmé que son organisation « travaille […] en étroite collaboration » avec les entreprises dans ce dossier[45]. Cette évaluation de la menace définit la chaîne d'approvisionnement numérique comme « un système d'organisations, de personnes, de technologies, d'activités, d'informations et de ressources permettant d'offrir un produit ou un service dans le cadre d'une relation fournisseur-client[46] ».

Compte tenu des activités actuellement menées par le CST dans le cadre du programme d'examen de la sécurité en ce qui concerne les tests et les évaluations pour les environnements hautement sécurisés, le Comité estime qu'élargir la portée de ce programme pourrait permettre de renforcer la sécurité de la chaîne d'approvisionnement numérique pour les infrastructures essentielles, au-delà de celles qui appartiennent au secteur des télécommunications et qui sont exploitées par ce dernier.

B. Un rôle possible pour l'Association canadienne de normalisation?

M. Steve Waterhouse, un ancien officier de sécurité des systèmes d'information au ministère de la Défense nationale, considère l'Association canadienne de

44 Voir : Centre canadien pour la cybersécurité, *Programme d'examen de la sécurité du CST visant les technologies 3G, 4G et LTE*.

45 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Jones, dirigeant principal, Centre canadien pour la cybersécurité), 42e législature, 1re session, 30 janvier 2019.

46 Voir : Centre canadien pour la cybersécurité, « Note en fin d'ouvrage 14 », *Évaluation des cybermenaces nationales 2018*.

normalisation (CSA) comme un joueur pouvant potentiellement favoriser la sécurité de la chaîne d'approvisionnement[47]. Par le passé, le mandat de la CSA était principalement axé sur la certification de la sécurité des produits. En 2017, cependant, l'organisme a créé un programme de cybersécurité qui offre des tests et des évaluations de la cybersécurité fondés sur des normes reconnues internationalement[48]. Compte tenu de l'existence de ces deux programmes, le Comité estime qu'il y a lieu de créer un système de certification. Dans le cadre ce système, le CST évaluerait et accorderait une certification de sécurité à l'ensemble des produits destinés aux infrastructures essentielles, tandis que la CSA accorderait une certification à tous les autres produits pouvant être connectés à Internet et qui sont destinés au marché commercial canadien. Ce deuxième système de certification, conjugué à une plus grande sensibilisation des consommateurs à propos d'une bonne hygiène cybernétique, pourrait grandement contribuer à renforcer la cybersécurité des dispositifs finaux connectés à l'Internet, ces « boîtes en carton » dont M. Kabilan a parlé. Les deux systèmes profiteraient d'une telle approche, le Comité accorde toutefois une valeur particulière à la certification que pourrait fournir la CSA sur l'information sur la sécurité du produit, dans un langage clair que le consommateur moyen pourrait facilement comprendre.

C. Huawei, 5G et sécurité de la chaîne d'approvisionnement numérique

Comme Scott Jones l'a évoqué lors de son témoignage, le CST supervise depuis six ans les tests et les évaluations effectués sur certains types d'équipement que les fournisseurs de services de télécommunications envisagent de déployer dans leurs infrastructures[49]. Les produits de Huawei font partie de ceux qui ont été évalués[50].

Lorsqu'on l'a interrogé sur la menace pour la sécurité nationale que représente la Chine et, par extension, les produits fabriqués par les fournisseurs d'équipement de télécommunications comme Huawei, M. Jones a répondu ce qui suit :

---

47 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Steve Waterhouse, ancien officier de sécurité des systèmes d'information, ministère de la Défense nationale), 42e législature, 1re session, 4 février 2019.

48 Canadian Standards Association, « Overview: CSA Group's New Cybersecurity Program Brings Cybersecurity Testing Services to Manufacturers », *News & Press*, 19 juillet 2017.

49 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Jones, dirigeant principal, Centre canadien pour la cybersécurité), 42e législature, 1re session, 30 janvier 2019.

50 Voir : Centre canadien pour la cybersécurité, *Programme d'examen de la sécurité du CST visant les technologies 3G, 4G et LTE*.

> Pour notre part, nous indiquons dans l'évaluation de la cybermenace nationale qu'il faut se montrer vigilant à l'égard de chaque État-nation et que chaque État-nation a certainement des cybertechniques à sa disposition. Certains sont plus agressifs que d'autres.
>
> Par le passé, le Centre de la sécurité des télécommunications s'est certainement vu demander d'attribuer des cyberactivités malveillantes à certains pays, et c'est une tâche que nous continuerons d'accomplir, conformément à la politique globale du gouvernement. C'est une situation que nous surveillons continuellement, mais à mon avis, nous ne nous défendons pas contre un seul pays, mais contre tout le monde[51].

« Mon travail m'amène à ne jamais me fier à quoi que ce soit », a-t-il déclaré. Il a ajouté : « Je présume que tous les éléments constitutifs d'un produit comportent des points vulnérables[52] ».

Les commentaires qui précèdent reflètent la philosophie de « confiance zéro » qui caractérise les pratiques exemplaires actuelles en matière de cybersécurité[53]. Le Comité estime que cette approche est un principe directeur essentiel. Le Comité croit également que le programme d'examen de la sécurité du CST offre un degré élevé de protection grâce aux tests et aux évaluations. De fait, les États-Unis reconnaissent eux aussi la qualité du travail effectué par les laboratoires qui ont obtenu l'accréditation du CST pour effectuer ce travail. Les États-Unis ont d'ailleurs accordé une accréditation à ces mêmes laboratoires du secteur privé pour effectuer des tests cryptographiques et des tests de sécurité sur les produits destinés à leurs propres systèmes essentiels[54].

Toutefois, étant donné qu'il est difficile d'établir avec certitude que nous pouvons avoir confiance dans les appareils et logiciels sur lesquels nous comptons, le Comité se demande s'il est sage d'utiliser des technologies produites en Chine. En effet, le professeur Leuprecht a demandé l'interdiction totale pour Huawei de participer au développement du réseau mobile 5G du Canada. Il a dit au Comité :

---

51 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Jones, dirigeant principal, Centre canadien pour la cybersécurité), 42e législature, 1re session, 30 janvier 2019.

52 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Jones, dirigeant principal, Centre canadien pour la cybersécurité), 42e législature, 1re session, 30 janvier 2019.

53 Comme nous l'avons déjà mentionné, le modèle de sécurité post-périmètre est également appelé " confiance zéro ". En effet, le modèle suppose que le périmètre a été violé et que la fiabilité de chaque dispositif et de chaque utilisateur doit être vérifiée en permanence.

54 National Institute of Standards and Technology, « National Voluntary Laboratory Accreditation Program (NVLAP): Directory Search ». (Répertoire de recherche, sélectionner « ITST: Cryptographic and Security Testing » comme programme et « Canada » comme pays).

> Par suite d'une modification législative récente, la Chine peut demander à toute entreprise chinoise, dont Huawei, de l'aider à appuyer les intérêts nationaux, y compris en matière de renseignement.
>
> Une préoccupation connexe est que la Chine et ses industries sont soupçonnées de se livrer à de l'espionnage industriel à grande échelle à titre de moyen peu coûteux de faire des transferts de recherche et développement. De plus, Huawei et le Parti communiste au pouvoir semblent être imbriqués de bien des façons importantes, y compris par l'intermédiaire de subventions de l'État qui s'élèveraient à 10 milliards de dollars dans une seule année. Le vol systématique de propriétés intellectuelles et les énormes subventions de l'État font en sorte qu'il est impossible pour des concurrents comme Nortel Networks de faire concurrence, ce qui a fini par mener à la disparition de la principale société de haute technologie du Canada. Étant donné que les communications sont des infrastructures essentielles, le gouvernement devrait exclure systématiquement de l'ensemble des infrastructures de communications canadiennes toute entité étrangère soupçonnée d'avoir des liens avec tout pays pour lequel il existe de solides preuves de vol important de propriété intellectuelle ou de collecte de renseignements[55].

À cet égard, le Comité prend note également des préoccupations exprimées par Jill Slay, professeure et titulaire de la chaire de recherche en cybersécurité Optus-La Trobe, à l'Université La Trobe de Melbourne, qui a parlé de Huawei en tant qu'« entreprise qui a la réputation de constamment voler la propriété intellectuelle »[56].

La direction de Huawei a peut-être affiché de bonnes intentions[57], mais les actions passées et récentes de son gouvernement sont hautement problématiques[58]. Par

---

55 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Christian Leuprecht, professeur, Département de sciences politiques, Collège militaire royal du Canada, à titre personnel), 42e législature, 1re session, 30 janvier 2019;

56 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Jill Slay, professeure, présidente de la cybersécurité La Trobe Optus, La Trobe University, Melbourne), 42e législature, 1re session, 20 février 2019.

57 Par exemple, en janvier 2019, en réponse à une série de questions qui lui ont été posées par le président du comité spécial sur les sciences et la technologie de la Chambre des communes du Royaume-Uni, Huawei a écrit une lettre ouverte indiquant ceci : « Huawei n'a jamais utilisé et n'utilisera jamais du matériel ou des logiciels basés au Royaume-Uni, ou de l'information recueillie au Royaume-Uni ou ailleurs dans le monde, pour aider d'autres pays à recueillir des renseignements. Nous ne ferions cela à aucun pays. » Voir : United Kingdom House of Commons Science and Technology Select Committee, *Correspondence from Huawei*, 29 janvier 2019 [DISPONIBLE EN ANGLAIS SEULEMENT].

58 Des témoins ont exprimé des préoccupations à propos des comportements passés et du comportement actuel de la Chine à l'égard du Canada, de même qu'à propos de la possibilité que la Chine utilise Huawei pour aller à l'encontre des intérêts nationaux du Canada en matière de sécurité. Voir, par exemple : Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Christian Leuprecht, professeur, Département de sciences politiques, Collège militaire royal du Canada, à titre personnel), 42e législature, 1re session, 30 janvier 2019; Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Chris Parsons, associé de recherche, Monk School of Global Affairs, Université de Toronto), 42e législature, 1re session, 27 février 2019; et Comité permanent de

exemple, Yuval Shavitt, professeur à l'École de génie électrique de l'Université de Tel-Aviv, a déclaré au Comité que les acteurs étatiques, dont la Chine, exploitent régulièrement les faiblesses de l'architecture de l'Internet pour détourner des flux massifs de données de télécommunication vers les infrastructures sous leur contrôle. Il a expliqué ce qu'il a constaté :

> 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[59].

CHAPITRE 4 — MENACES ÉMERGENTES

A. L'intelligence artificielle comme arme

Les témoins ont prévenu le Comité de deux nouvelles menaces à la cybersécurité : l'utilisation malveillante de l'intelligence artificielle (IA) et de l'informatique quantique. La première menace est déjà à nos portes, mais la deuxième, qui ne pourrait arriver que dans plusieurs années, est susceptible d'entraîner des répercussions tellement importantes qu'elle exige également une attention immédiate.

Dans le domaine de la cybersécurité, l'IA est véritablement une arme à double tranchant. Les spécialistes de la cybersécurité qui ont comparu devant le Comité s'entendaient pour dire qu'il s'agit d'un outil essentiel dans un monde post-périmètre où il faut présumer qu'il y aura des infractions et chercher les signes de compromission des systèmes internes et du déroulement des opérations. Voici comment David Masson a expliqué la place de plus en plus centrale qu'occupe l'IA en matière de cybersécurité :

> Par le passé, les entreprises cherchaient à protéger leurs réseaux contre l'extérieur, renforçant leur périmètre au moyen de pare-feu et de solutions de sécurité des points terminaux. Aujourd'hui, la migration vers le nuage et l'adoption rapide de l'Internet des objets rendent presque impossible la protection du périmètre. Une autre approche

---

la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Richard Fadden, à titre personnel), 42e législature, 1re session, 10 avril 2019.

59 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Yuval Shavitt, professeur, Université de Tel-Aviv), 42e législature, 1re session, 20 février 2019.

> traditionnelle, connue sous le nom de « règles et signatures », reposait sur le principe de la recherche de problèmes connus. Les attaquants sont toutefois en constante évolution, et cette technique ne réussit pas à détecter les attaques nouvelles et ciblées. Mais surtout, ces approches traditionnelles ne permettent pas aux entreprises de savoir ce qu'il se passe sur leurs réseaux, ce qui rend difficile, voire impossible, la détection des menaces qui s'y trouvent déjà[60].

Steve Drennan, directeur de la cybersécurité au Groupe ADGA, préconisait une « intelligence artificielle centralisée » pouvant offrir une « orchestration de la sécurité » à l'échelle du secteur. Il s'agirait essentiellement de mesures d'intervention semi-automatiques ou entièrement automatiques pour faire face aux cybermenaces[61]. Voici ce qu'il a déclaré :

> Voyez cela comme des solutions de prochaine génération qui pourraient être déployées à l'échelle pour que tout le monde puisse les utiliser et en profiter. Le concept, c'est qu'une organisation pourrait en fait diriger cet effort et mettre cette capacité dans un lieu central pour que cela soit activé par toutes les entités [du secteur financier][62].

D'autres témoins ont recommandé de faire preuve d'une plus grande prudence et de ne pas s'en remettre uniquement à l'IA dans le domaine de la cybersécurité. Par exemple, Christian Leuprecht a présenté le bémol suivant :

> L'intelligence artificielle n'est pas une sorte de chapeau extraordinaire et magique duquel on peut sortir un lapin. Ce n'est que des mathématiques, des mathématiques avancées et sophistiquées et leurs applications. Ironiquement, bien que le gouvernement ait investi des sommes considérables pour diverses applications dans le domaine, il n'a pas fait un seul investissement dans la cybersécurité liée à ces applications[63].

Du même souffle, le professeur Leuprecht semblait également soutenir l'idée de créer une capacité centralisée et vraisemblablement automatisée[64] de détection de la menace et d'intervention afin de protéger les infrastructures essentielles du Canada, y compris le secteur financier.

---

60 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (David Masson, directeur, Sécurité d'entreprise, Darktrace), 42e législature, 1re session, 18 mars 2019.

61 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Steve Drennan, directeur, Cybersécurité, Groupe ADGA), 42e législature, 1re session, 10 avril 2019.

62 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Steve Drennan, directeur, Cybersécurité, Groupe ADGA), 42e législature, 1re session, 10 avril 2019.

63 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Christian Leuprecht, professeur, Département de sciences politiques, Collège militaire royal du Canada, à titre personnel), 42e législature, 1re session, 30 janvier 2019.

64 L'ampleur du trafic sur le réseau que les fournisseurs de services de télécommunications devraient analyser et à laquelle ils devraient donner suite éliminerait les approches manuelles.

Il a fait référence à l'« inspection approfondie des paquets[65] » à laquelle procède le CST au Canada pour protéger les réseaux gouvernementaux, ainsi qu'aux inspections auxquelles procèdent les fournisseurs de services de télécommunications australiens pour protéger leurs clients, mais il a déploré la réticence des fournisseurs canadiens de services de télécommunications à en faire autant, malgré des cadres juridiques similaires. Il a offert l'explication suivante concernant la réticence des fournisseurs canadiens de services télécommunications :

> Deux points préviennent la pleine exploitation de cette possibilité. Premièrement, comme ce niveau de détection est coûteux, les fournisseurs de services de télécommunication sont peu enclins à le fournir. Ensuite, ils jugent qu'une amélioration devient problématique sur le plan juridique une fois qu'elle est détectée[66].

Le Comité est d'avis qu'il pourrait être utile d'examiner plus à fond les raisons expliquant cette divergence entre les approches canadienne et australienne. Le Comité note que les fournisseurs de services de télécommunications ont exprimé des préoccupations concernant l'éventuelle responsabilité légale parce qu'en vertu du paragraphe 430(1.1) du *Code criminel*, il est interdit de détruire et de modifier des données informatiques et d'empêcher, d'interrompre ou de gêner l'emploi légitime de données informatiques. Cette considération et d'autres considérations d'ordre juridique sont soulevées dans un document de 2013 commandé par Recherche et développement pour la défense Canada intitulé *The Dark Space Project*. Bell Canada figure parmi les auteurs du document

L'IA peut également contribuer à éviter que des logiciels mal programmés ne soient mis sur le marché. Les développeurs de logiciels peuvent maintenant utiliser des plateformes d'IA pour déceler et éliminer les vulnérabilités dans leur code[67].

---

65 L'inspection approfondie des paquets fait référence à l'utilisation d'outils pour examiner l'en-tête, et éventuellement le contenu, des paquets de protocole Internet (IP) afin de détecter la non-conformité au protocole, les logiciels malveillants, les pourriels et autres indicateurs de cyberactivité malveillante.

66 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Christian Leuprecht, professeur, Département de sciences politiques, Collège militaire royal du Canada, à titre personnel), 42e législature, 1re session, 30 janvier 2019. Le Comité note que les fournisseurs de services de télécommunications ont exprimé des préoccupations concernant l'éventuelle responsabilité légale parce qu'en vertu du paragraphe 430(1.1) du *Code criminel*, il est interdit de détruire et de modifier des données informatiques et d'empêcher, d'interrompre ou de gêner l'emploi légitime de données informatiques. Cette considération et d'autres considérations d'ordre juridique sont soulevées dans un document de 2013 commandé par Recherche et développement pour la défense Canada intitulé *The Dark Space Project*. Bell Canada figure parmi les auteurs du document (voir Dave McMahon, Rafal Rohokinski, Bell Canada, *The Dark Space Project*, Recherche et développement pour la défense Canada, Centre des sciences pour la sécurité, juillet 2013 [DISPONIBLE EN ANGLAIS SEULEMENT]).

67 Voir, par exemple, l'outil d'analyse de code reposant sur l'IA DeepCode, basé à Zurich, www.deepcode.ai.

Il existe toutefois un pendant négatif à l'analyse de code automatisée. De fait, il y a de plus en plus de signes qui indiquent que l'IA est utilisée pour faciliter les cyberattaques, voire même pour les perpétrer. Des témoins ont indiqué au Comité que l'IA « abaissera la barre », c'est-à-dire qu'elle fera en sorte qu'il sera plus facile pour les pirates de perpétrer des attaques complexes, comme celles qui ont ciblé le réseau électrique de l'Ukraine[68]. D'aucuns croient que ce n'est qu'une question de temps avant que les humains soient écartés de l'équation et que des systèmes d'IA s'en prennent directement à d'autres systèmes d'IA. Lorsque cela se produira, les organisations qui comptent sur des systèmes traditionnels de défense du périmètre pour se protéger seront dangereusement exposées. Comme l'a indiqué David Masson de Darktrace :

> Lorsqu'on pense à la première attaque perpétrée à l'aide de l'intelligence artificielle – notre entreprise croit qu'elle pourrait se produire cette année; nous voyons des signes de cela depuis longtemps, mais elle pourrait se produire plus tard –, bon nombre des techniques et des systèmes qui sont utilisés actuellement pour protéger les réseaux des cybermenaces deviendront désuets du jour au lendemain. Cela arrivera très rapidement[69].

Tout cela est préoccupant pour le Comité et fait assurément ressortir les limites associées au fait de compter sur la sensibilisation des utilisateurs pour protéger les organisations contre des attaques perpétrées à l'aide de l'IA.

Recommandation 3

Le comité recommande au gouvernement du Canada de reconnaître à la fois les promesses et les dangers de l'intelligence artificielle pour la cybersécurité, en veillant à ce que cette dualité soit traitée dans un cadre national de cybersécurité.

B. Un ordinateur quantique pratique

Tout comme dans le domaine de l'IA, les progrès liés à la recherche quantique pourraient constituer à la fois une avancée et une menace à la cybersécurité. Par exemple, les percées qui permettront d'utiliser les effets quantiques pour communiquer de l'information sur de longues distances pourraient sonner le glas de l'interception clandestine sur les réseaux. On espère également qu'un ordinateur quantique sera bientôt disponible, qu'il sera plus puissant qu'un ordinateur classique et assez stable pour servir à toute une gamme de tâches informatiques. On désigne souvent un

68 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (David Masson, directeur, Sécurité d'entreprise, Darktrace), 42e législature, 1re session, 18 mars 2019.

69 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (David Masson, directeur, Sécurité d'entreprise, Darktrace), 42e législature, 1re session, 18 mars 2019.

ordinateur quantique qui possède ces caractéristiques comme un « ordinateur quantique pratique ». Un ordinateur quantique pratique pourrait notamment être utilisé pour « dynamiser » l'IA, ce qui pourrait permettre d'améliorer l'analyse de la sécurité des logiciels.

Toutefois, un tel ordinateur permettrait également d'effectuer facilement les calculs complexes qui sont à la base de la cryptographie à clé publique[70]. Michele Mosca, professeur de mathématiques et de cryptographie à l'Université de Waterloo et directeur de l'organisme sans but lucratif Quantum-Safe Canada, a indiqué au Comité qu'il prévoit qu'un ordinateur quantique pratique sera construit dans les 8 à 15 prochaines années. Selon lui, voici ce qui se produira si ne nous préparons pas à cet événement :

> Primo, le secteur des services financiers subira une attaque directe : vol d'argent, entraves aux activités légitimes, perte de confiance dans le secteur financier canadien. Secundo, il y aura des cyberattaques contre d'autres secteurs de notre économie, secteurs dans lesquels nous investissons beaucoup d'argent : on pense surtout aux infrastructures essentielles comme les services gouvernementaux, l'électricité et d'autres services publics, les systèmes de transport et les villes intelligentes. Tertio, on assistera au vol de la propriété intellectuelle stratégique protégée par une cryptographie vulnérable à l'informatique quantique. Quarto, les emplois canadiens actuels et à venir subiront des perturbations dans les secteurs qui produisent ou utilisent des technologies vulnérables aux attaques quantiques et n'ont pas de plan pour assurer la sécurité quantique[71].

Les ordinateurs quantiques représentent donc une menace existentielle pour le secteur financier, qui compte sur l'infrastructure à clés publiques[72] pour fonctionner en toute sécurité. Comme l'a indiqué M. Jonathan Reiber, chef de la Stratégie de cybersécurité chez Illumio, l'informatique quantique va « changer complètement la nature de la cybersécurité[73] ».

---

70 La majeure partie de la cryptographie à clé publique repose sur des fonctions mathématiques que l'on appelle « unidirectionnelles », comme la factorisation des nombres premiers, c'est-à-dire qu'il est facile de les effectuer dans une direction, mais qu'il faut effectuer des calculs difficiles dans l'autre direction.

71 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Michele Mosca, directeur, Quantum-Safe Canada), 42e législature, 1re session, 27 février 2019.

72 Une infrastructure à clés publiques désigne un « Système de délivrance de clés et de certificats cryptographiques, qui permet de sécuriser les transactions électroniques et les échanges de renseignements de nature délicate à l'aide d'un système de tiers de confiance nommés "autorités de certification" », gouvernement du Canada, « Infrastructures à clés publiques », *Termium Plus*.

73 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Jonathan Reiber, chef, Stratégie de cybersécurité, Illumio), 42e législature, 1re session, 6 février 2019.

Même en présumant qu'il faudra attendre plus longtemps avant de voir apparaître un ordinateur quantique, nous devons tout de même commencer dès maintenant à effectuer la planification nécessaire en vue d'un monde post-quantique. Des témoins ont indiqué que des normes de cryptage résistantes à l'informatique quantique sont en cours d'élaboration dans le cadre d'un programme lancé en 2016 par le National Institute of Standards and Technology des États-Unis (il s'agit d'un programme de huit ans qui en est à sa troisième année[74]). Des chercheurs canadiens ont fourni une partie des 26 algorithmes de chiffrement proposés. Selon les témoins, lorsque la validité de chaque algorithme proposé aurait fait l'objet d'une évaluation approfondie, on peut s'attendre à ce que l'adoption internationale des normes qui ressortiront de ce processus prenne une décennie ou plus.

Entre-temps, il faut bâtir des infrastructures habilitantes comme un système de distribution des clés quantiques (DCQ)[75]. Or, le Canada, qui a inventé la DCQ, a l'occasion de montrer au monde entier comment bâtir un système inviolable qui peut fournir une capacité de communication sécurisée sur l'ensemble de son vaste territoire[76]. À l'heure actuelle, il y a des centres de collaboration en matière de DCQ à Calgary, à Ottawa, à Waterloo et à Québec, qui fonctionnent sur des réseaux distincts de fibre optique et qui en sont à différentes étapes de planification et de développement[77]. Quantum-Safe Canada espère relier les réseaux de ces centres de collaboration via satellite afin de permettre la mise en place d'un réseau national de DCQ qui pourrait éventuellement se joindre à un réseau mondial[78]. Quantum-Safe Canada croit que pour mettre à l'essai les communications par satellite entre ces centres de recherche canadiens qui travaillent en collaboration, il est « de toute évidence nécessaire » que le

74 Pour en apprendre davantage, voir : National Institute of Standards and Technology, *Post-Quantum Cryptography* [DISPONIBLE EN ANGLAIS SEULEMENT].

75 La distribution de clés quantiques (DCQ) désigne l'utilisation d'effets quantiques pour établir un agrément de clé entre des parties afin de sécuriser une communication.

76 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Michele Mosca, directeur, Quantum-Safe Canada), 42e législature, 1re session, 27 février 2019.

77 Dr Michele Mosca, Brian O'Higgins et Bill Munson, Quantum-Safe Canada, *La menace quantique pour la cybersécurité : Danger et possibilité : Soumis à l'appui d'une présentation au Comité permanent de la sécurité publique et nationale sur la cybersécurité dans le secteur financier en tant que question de sécurité économique nationale*, 22 février 2019, p. 3.

78 Dr Michele Mosca, Brian O'Higgins et Bill Munson, Quantum-Safe Canada, *La menace quantique pour la cybersécurité : Danger et possibilité : Soumis à l'appui d'une présentation au Comité permanent de la sécurité publique et nationale sur la cybersécurité dans le secteur financier en tant que question de sécurité économique nationale*, 22 février 2019, p. 3.

Canada intègre la DCQ aux infrastructures de réseau de ces centres d'ici trois à cinq ans[79].

Le Canada est confronté à une rude concurrence dans ce domaine. La Chine, par exemple, a dit souhaiter devenir une superpuissance quantique d'ici 2030 et travaille d'arrache-pied pour créer son propre système national de DCQ, en commençant par une ligne principale de 2 000 km entre Beijing et Shanghai[80]. De plus, la Chine a récemment connu du succès en ce qui concerne la distribution de clés à des distances intercontinentales à l'aide de son satellite Micius[81].

Il faudra également prendre des décisions, tant au niveau national qu'au niveau international, concernant l'établissement de l'ordre de priorité pour les systèmes qui effectueront la transition vers la norme de cryptage résistante à l'informatique quantique. Comme le professeur Mosca l'a indiqué, étant donné que l'Internet repose en grande partie sur le chiffrement à clé publique, il fera partie des infrastructures qui devront être considérées comme prioritaires. Pendant la transition graduelle, les normes résistantes à l'informatique quantique devront fonctionner parallèlement aux normes cryptographiques actuelles. Il sera difficile de mettre en œuvre correctement cette structure opérationnelle parallèle du point de vue de la cybersécurité.

Des témoins ont exhorté le gouvernement à lutter contre cette tendance et à commencer la planification dès maintenant pour éviter le chaos plus tard. Le professeur Mosca a mis le Comité en garde contre les conséquences potentielles associées au fait de remettre cette tâche à plus tard :

> [Si] nous agissons de façon réactive, nous serons vulnérables aux attaques quantiques. Nous serons également vulnérables aux attaques banales qui ont cours actuellement et qui exploitent les failles qui proviennent de notre gestion de crise précipitée […] Voilà ce qui va se produire si nous gérons la situation de façon réactive. Si nous ne sommes pas proactifs, les nouvelles possibilités dans lesquelles nous avons investi pendant des

79 Dr Michele Mosca, Brian O'Higgins et Bill Munson, Quantum-Safe Canada, *La menace quantique pour la cybersécurité : Danger et possibilité : Soumis à l'appui d'une présentation au Comité permanent de la sécurité publique et nationale sur la cybersécurité dans le secteur financier en tant que question de sécurité économique nationale*, 22 février 2019, p. 3.

80 John Costello, *Chinese Efforts in Quantum Information Science: Drivers, Milestones, and Strategic Implications*, Témoignage devant la U.S.-China Economic and Security Review Commission, 16 mars 2017, p. 13-14.

81 « Chinese satellite uses quantum cryptography for secure videoconference between continents », *MIT Technology Review*, 30 janvier 2018.

> dizaines d'années nous échapperont et une grande portion de notre économie, dans sa forme actuelle, sera en danger[82].

Les organisations canadiennes du secteur public et du secteur privé doivent prendre le taureau par les cornes rapidement pour réussir la transition de leurs infrastructures et fonds de données vers la cryptographie à l'épreuve de l'informatique quantique.

De fait, M. Brian O'Higgins, fondateur du logiciel canadien de chiffrement Entrust et président de Quantum-Safe Canada, a souligné que le défi lié à l'informatique quantique offre des occasions formidables. Il a rappelé que le Canada a longtemps joui d'une excellente réputation pour ce qui est des compétences en cryptographie. Il a ajouté ce qui suit :

> Nous continuons de nous inspirer de ce genre d'aura selon laquelle les Canadiens sont bons en technologie de chiffrement. Il y a aujourd'hui une occasion à saisir avec la résistance quantique. Le chiffrement doit changer du tout au tout dans le monde. Il doit pouvoir résister à une attaque quantique. Devinez quoi? La technologie quantique canadienne de l'Université de Waterloo et d'ailleurs est de calibre mondial. L'occasion est bonne de répéter ce genre d'effet[83].

Finalement, selon les témoins, pour préparer le Canada à se tailler une place dans un monde post-quantique, le pays devra pouvoir compter sur une main-d'œuvre possédant des compétences encore plus rares que celles requises pour les activités générales de cybersécurité. Les témoins ont indiqué que comme le Canada investit depuis des décennies dans la science quantique et la cryptographie, il a la chance de posséder un petit noyau de talents de classe mondiale. Avec le soutien nécessaire, ce noyau pourrait contribuer à bâtir la main-d'œuvre spécialisée en informatique quantique dont le Canada aura besoin à l'avenir.

Recommandation 4

Le Comité recommande que le gouvernement du Canada augmente la capacité actuelle du Canada en matière de compétences informatiques quantiques et qu'il continue d'appuyer la recherche et le développement de technologies quantiques et de normes de cryptage qui assureront la sécurité de l'information et des systèmes d'information électroniques du Canada dans un monde post-quantique.

---

82 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Michele Mosca, directeur, Quantum-Safe Canada), 42e législature, 1re session, 27 février 2019.

83 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Brian O'Higgins, président, Quantum-Safe Canada), 42e législature, 1re session, 27 février 2019.

CHAPITRE 5 — REMÉDIER À LA PÉNURIE DE COMPÉTENCES EN CYBERSÉCURITÉ

Les experts en cybersécurité sont en grande demande. De par le monde, les pays rivalisent pour attirer et garder dans leurs rangs des candidats qualifiés et compétents dans le domaine, et le Canada ne fait pas exception. En fait, nos banques investissent massivement dans la tenue de « hackathons », des programmes de recherche post-secondaires et d'autres activités vouées à dénicher et à séduire les talents canadiens de la cybersécurité. D'après M. Charles Docherty, avocat général adjoint, Association des banquiers canadiens (ABC),

> [Les membres de l'ABC] ont financé des laboratoires de cybersécurité à l'Université de Waterloo. Des membres ont investi à l'étranger, notamment à l'Université Ben-Gurion, en Israël, un centre de cybersécurité de renommée mondiale. Un autre membre a conclu une alliance stratégique avec la Banque Leumi, d'Israël, ainsi qu'avec la Banque nationale d'Australie, afin de coopérer dans les domaines des services bancaires numériques, de la technologie financière et de la cybersécurité[84].

Le Comité a invité des témoins qui étaient en mesure de lui parler des efforts déployés en Australie et en Israël en vue de bâtir un effectif compétent en cybersécurité. Leurs commentaires sont présentés dans les deux sections suivantes.

A. Australie

Le Comité voulait connaître l'approche adoptée par l'Australie. Il a ainsi invité le professeure Jill Slay à faire valoir son point de vue sur les programmes d'enseignement en cybersécurité. Elle a indiqué que le gouvernement australien tente d'éveiller les jeunes le plus tôt possible à la cybersécurité, expliquant ceci :

> 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[85].

---

84 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Charles Docherty, avocat général adjoint, Association des banquiers canadiens), 42e législature, 1re session, 18 mars 2019. Voir aussi, Banque Royale du Canada, « La Banque Royale du Canada et l'Université Ben-Gurion établissent un partenariat axé sur la cybersécurité », communiqué de presse, 26 juin 2018.

85 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Jill Slay, professeure, présidente de la cybersécurité La Trobe Optus, La Trobe University, Melbourne), 42e législature, 1re session, 20 février 2019.

Des changements sont aussi prévus au cadre d'enseignement post-secondaire en cybersécurité. Le professeure Slay a fait savoir que l'Australian Computer Society, qui est l'association professionnelle du pays pour le secteur de l'information, des communications et de la technologie (ICT), a entrepris d'adapter son programme national d'ICT pour en faire un programme qui soit davantage interdisciplinaire. Elle a déclaré ce qui suit :

> [N]ous avons un programme national en [ICT]. 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[86].

B. Israël

Les témoins entendus par le Comité ont souvent fait référence à l'écosystème israélien en matière de cybersécurité. Par exemple, Glenn Foster, chef de la sécurité de l'information à la Banque Toronto Dominion, a indiqué qu'il tentait de recruter des cybertalents en Isarël[87]. Cybersecure Catalyst, une nouvelle organisation sans but lucratif établie à Brampton, en Ontario, a offert l'exemple suivant pour illustrer à quel point les institutions financières canadiennes dépendent aujourd'hui des cybertalents israéliens :

> Il y a une façon intéressante de voir le problème du manque de travailleurs en cybersécurité au Canada, et c'est de se rendre en Israël. Ce pays est généralement reconnu pour posséder le plus solide écosystème technologique en matière de cybersécurité dans le monde. Le gouvernement israélien a récemment créé un grand centre d'activités de cybersécurité dans une petite ville du désert du Néguev appelée Beersheba, à environ une heure en voiture de Tel-Aviv. En janvier, je suis allé à Beersheba non pas pour rencontrer des représentants de sociétés israéliennes, mais des représentants d'institutions financières canadiennes qui ont établi des bureaux là-bas parce qu'il leur est beaucoup plus facile de trouver des talents en cybersécurité en Israël qu'au Canada[88].

L'Israël entreprend de sensibiliser les enfants à de bonnes cyberhabitudes – c'est-à-dire des mesures à prendre pour se protéger contre les cyber-risques – beaucoup plus tôt

86 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Jill Slay, professeure, présidente de la cybersécurité La Trobe Optus, La Trobe University, Melbourne), 42e législature, 1re session, 20 février 2019.

87 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Glenn Foster, chef de la sécurité de l'information, Banque Toronto Dominion), 42e législature, 1re session, 3 avril 2019.

88 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages*, (Charles Finlay, directeur exécutif, Cybersecure Catalyst), 42e législature, 1re session, 1er avril 2019.

que l'Australie. Selon Yuval Shavitt, professeur à l'École de génie électrique de l'Université de Tel-Aviv :

> 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 […] Il semble que cela fonctionne[89].

Pour ce qui est de l'enseignement de la cybersécurité, là aussi, les programmes commencent tôt en Israël. M. Yuval a expliqué ceci :

> 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[90].

C. Canada

En septembre 2018, l'Université Ryerson a annoncé son intention d'établir à Brampton un centre sans but lucratif appelé « Cybersecure Catalyst », qui aura pour mission d'offrir des programmes de formation et de certification, de recherche et développement, d'incubation commerciale et de sensibilisation du public; il participera également à l'élaboration de politiques[91]. Le Comité a invité le directeur exécutif de Cybersecure Catalyst, M. Charles Finlay, à venir discuter du rôle que jouera le centre dans la création d'un effectif compétent en cybersécurité au Canada.

M. Finlay a indiqué que lors de la planification de son catalogue de cours, Cybersecure Catalyst a sollicité les commentaires du secteur financier. Il en est ressorti que le secteur doit composer avec des pénuries de main-d'œuvre à plusieurs échelons. Il a résumé les commentaires obtenus comme suit :

> Quand nous avons demandé aux grandes institutions financières et à d'autres organismes du secteur privé de nous préciser ce qu'un centre universitaire de cybersécurité pouvait faire de plus utile pour eux, ils n'ont pas parlé d'un outil technologique particulier ou de progrès précis dans les sciences. Ils ont répondu massivement qu'il leur fallait plus de gens […] En particulier, des institutions financières

89 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Yuval Shavitt, professeur, Université de Tel-Aviv), 42e législature, 1re session, 20 février 2019.

90 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Yuval Shavitt, professeur, Université de Tel-Aviv), 42e législature, 1re session, 20 février 2019.

91 Will Sloan, « University Launches Cybersecurity Centre » (tiré de *Ryerson Today*), Université Ryerson, *Research News*, 6 septembre 2018.

> ont indiqué qu'il fallait mettre à niveau les compétences de leur personnel existant pour répondre aux menaces émergentes, et qu'il fallait que plus de gens fassent leur entrée dans le secteur pour qu'ils puissent doter les postes de premier échelon au sein de leurs organisations. Toutes les grandes institutions financières au Canada ont de nombreux postes à doter dans le domaine de la cybersécurité[92].

M. Finlay a poursuivi en citant un rapport publié en juillet 2018 par Deloitte et la Toronto Financial Services Alliance, qui indiquait qu'il faudrait doter 8 000 postes en cybersécurité d'ici 2021[93]. Il a salué le budget de 2019 du gouvernement fédéral, qui accorde 80 millions de dollars aux établissements postsecondaires pour qu'ils offrent des cours en cybersécurité, tout en ajoutant qu'il y a plus à faire encore. Pressant le gouvernement de se concentrer sur les groupes démographiques qui sont gravement sous-représentés dans le secteur de la cybersécurité, M. Finlay a déclaré :

> Nous n'arriverons pas à résoudre le problème de la pénurie de personnel de cybersécurité des institutions financières ou de n'importe quel autre type d'institutions si nous n'ouvrons pas le secteur de la cybersécurité de manière à avoir plus de femmes, de membres de groupes racialisés, de nouveaux Canadiens, d'Autochtones, de vétérans et de personnes qui ont perdu leur emploi dans des secteurs existants[94].

Le Comité est d'accord pour dire que le Canada ne peut pas se permettre de passer outre quelque source que ce soit de cybertalents. Il appuie aussi les efforts de Cybersecurity Catalyst, qui cherche à adapter ses programmes afin de pouvoir répondre à un large éventail de besoins. M. Finlay a confirmé au Comité que Cybersecurity Catalyst collabore avec le réputé SANS Institute, des États-Unis. Le Comité souligne que le SANS Institute établit lui-même le catalogue de cours offerts au National Institute of Standards and Technology (NIST), pour le cadre de la National Initiative of Cybersecurity Education (NICE). Ce cadre « établit une taxonomie et un lexique commun qui décrivent le travail et les travailleurs dans le domaine de la cybersécurité, quels que soient le lieu et l'employeur[95] ». Aucune mesure n'est écartée si elle peut aider un employeur à bien cerner les lacunes en fait de compétences ou à évaluer correctement les qualifications d'un candidat.

---

92 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages*, (Charles Finlay, directeur exécutif, Cybersecure Catalyst), 42e législature, 1re session, 1er avril 2019.

93 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages*, (Charles Finlay, directeur exécutif, Cybersecure Catalyst), 42e législature, 1re session, 1er avril 2019.

94 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages*, (Charles Finlay, directeur exécutif, Cybersecure Catalyst), 42e législature, 1re session, 1er avril 2019.

95 National Institute of Standards and Technology, *NICE Cybersecurity Workforce Framework* [DISPONIBLE EN ANGLAIS SEULEMENT].

Les témoins ont également salué les efforts du Nouveau-Brunswick pour devenir l'épicentre de la cybersécurité au pays, indiquant que les grandes entreprises « s'arrachent »[96] les diplômés des programmes d'études secondaires en cybersécurité de CyberNB. Devant une vive concurrence dans le recrutement de cybertalents, la Banque Toronto Dominion a indiqué qu'elle établit aussi des partenariats avec des établissements d'enseignement qui offrent des cours dans ce domaine, dont l'Université du Nouveau-Brunswick[97].

À savoir comment le Centre canadien pour la cybersécurité contribue à renverser la pénurie de main-d'œuvre au Canada, Scott Jones a indiqué que son organisation avait participé à des initiatives de mentorat et parrainé des événements comme le Hackergal afin d'inciter les filles à faire de la programmation. Il a cependant ajouté que vu l'immensité du Canada, il est difficile de reproduire le programme de sensibilisation du Centre à grande échelle[98].

On reconnaît que toute stratégie visant à bâtir un effectif qualifié en cybersécurité doit s'accompagner d'un plan pour encourager l'acquisition d'aptitudes en programmation et de compétences numériques chez les enfants, et ce, dès les premières années du primaire. Dans la mesure du possible, compte tenu de la compétence provinciale et territoriale en matière d'éducation, le gouvernement fédéral s'est efforcé de contribuer à cet objectif.

Le programme CodeCan[99] d'Innovation, Science et Développement économique Canada est un exemple de la façon dont le gouvernement fédéral soutient l'acquisition de cybercompétences chez les jeunes. CodeCan finance des organismes sans but lucratif afin qu'ils puissent offrir des programmes de formation en compétences numériques à des élèves et leurs enseignants à l'échelle du Canada. À ce jour, le programme a rejoint 1,3 million d'élèves et quelque 61 000 enseignants[100], leur permettant d'acquérir des compétences numériques, notamment en programmation et en analyse de données. Les critères d'évaluation constituant un atout pour être admissible au financement de

96 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (David Masson, directeur, Sécurité d'entreprise, Darktrace), 42e législature, 1re session, 18 mars 2019.

97 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Glenn Foster, chef de la sécurité de l'information, Banque Toronto Dominion), 42e législature, 1re session, 3 avril 2019.

98 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Jones, dirigeant principal, Centre canadien pour la cybersécurité, Centre de la sécurité des télécommunications), 42e législature, 1re session, 30 janvier 2019.

99 Innovation, Science et Développement économique Canada, *CodeCan*.

100 *Ibid*.

CodeCan privilégient les organisations qui ont démontré être en mesure de rejoindre les groupes généralement sous-représentés, comme les filles, les jeunes Autochtones et les jeunes handicapés[101]. Le Comité appuie cette approche, qui met l'accent sur les populations sous-représentées et qui s'étend à l'échelle du Canada.

Les critères d'évaluation de CodeCan ne font toutefois pas mention des pratiques de cyberhygiène et de programmation éthique, qui doivent faire partie des compétences à transmettre aux élèves et aux enseignants. Le Comité estime qu'il s'agit là d'une omission à corriger.

Recommandation 5

Le Comité recommande au gouvernement du Canada d'élaborer une stratégie globale en matière de compétences et de formation dans le domaine de la cybersécurité qui inculquera des pratiques de codage éthiques et rigoureuses dès le début et créera une main-d'œuvre en cybersécurité qui s'appuie sur de l'expérience diversifiée, répond aux normes internationales reconnues et est prête à relever les défis actuels et futurs en matière de cybersécurité.

CHAPITRE 6 — SIGNALEMENT DES INCIDENTS

D'après les témoignages entendus, le Canada n'a pas toutes les données nécessaires pour mesurer avec exactitude sa situation en matière de cybersécurité. Les meilleures données disponibles semblent être celles compilées par Statistique Canada dans le cadre d'une enquête sur les entreprises canadiennes, menée en 2017[102].

D'après M. Chris Lynam, directeur général par intérim de la Coordination nationale contre la cybercriminalité, à la GRC, l'enquête de Statistique Canada montre que malgré les avancées des quelques dernières années, les cybercrimes sont encore peu signalés. Il a déclaré ceci :

> L'Enquête canadienne sur la cybersécurité et le cybercrime de 2017, menée par Statistique Canada, a révélé qu'environ 10 % des entreprises touchées par un incident de cybersécurité ont signalé l'incident à un service de police en 2017. Malgré la sous-déclaration, le nombre de cybercrimes signalés à la police au Canada a augmenté au

101 Innovation, Science et Développement économique Canada, *Critères d'évaluation de CodeCan*.

102 Voir Howard Bilodeau, Mohammad Lari et Mark Uhrbach, *Les défis des entreprises canadiennes quant à la cybersécurité et au cybercrime, 2017*, Statistique Canada, 28 mars 2019.

> cours des dernières années. En 2017, près de 28 000 cybercrimes ont été signalés à la police canadienne, une hausse de 83 % par rapport à 2014[103].

Sachant que la judiciarisation contribue à contrer la criminalité, le Comité a été quelque peu surpris d'apprendre que la police serait rapidement submergée si le signalement de tous les cybercrimes devenait obligatoire[104].

Étant donné que beaucoup de ces activités criminelles prennent source un peu partout au Canada ou même à l'étranger, où la GRC n'a peut-être pas accès à des accords d'entraide juridique, il est encore plus difficile d'enquêter et d'intenter des poursuites pénales. Bien que la GRC et les autres services de police du Canada n'ont pas tourné le dos aux poursuites, le surintendant principal Flynn a déclaré : « nous jugeons qu'il est plus important de réduire le nombre de crimes et le nombre de pertes le plus tôt possible[105] ».

Voulant savoir comment l'Unité nationale de coordination de la lutte contre la cybercriminalité de la GRC pourra améliorer la situation, le Comité a entendu que la nouvelle unité agirait comme point central pour encourager le signalement des cybercrimes et qu'elle faciliterait la coordination des enquêtes connexes, de façon à assurer une utilisation efficace des ressources policières en place. M. Lynam a indiqué que l'unité aidera les services de police municipaux et provinciaux à améliorer leur rendement dans ce domaine, non seulement en augmentant l'échange d'informations entre les intervenants, mais aussi en utilisant l'IA pour évaluer les rapports publics d'incidents. En ce qui concerne ce dernier point, il a expliqué que :

> [E]n ayant un mécanisme de signalement public moderne et robuste qui a une grande capacité d'analyse, nous pourrons très rapidement savoir que, par exemple, 10 autres personnes au Canada ont été des victimes de la même personne ou de la même entité, identifiable par un nom ou une adresse courriel. Puisque ce mécanisme aura une incidence à l'échelle nationale, nous pourrons travailler avec d'autres services de police

---

103 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Chris Lynan, directeur général par intérim, Coordination nationale contre la cybercriminalité, Gendarmerie royale du Canada), 42e législature, 1re session, 28 janvier 2019.

104 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (surintendant principal Mark Flynn, directeur général, Criminalité financière et la cybercriminalité, Opérations criminelles de la police fédérale, Gendarmerie royale du Canada), 42e législature, 1re session, 28 janvier 2019.

105 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (surintendant principal Mark Flynn, directeur général, Criminalité financière et la cybercriminalité, Opérations criminelles de la police fédérale, Gendarmerie royale du Canada), 42e législature, 1re session, 28 janvier 2019.

> au Canada pour lutter contre la cybercriminalité. En ce moment, ce n'est pas possible de fonctionner ainsi[106].

Le Comité en conclut que même s'il sera crucial d'accroître l'échange d'informations et la coordination pour combattre la cybercriminalité – puisqu'il sera ainsi plus facile pour les services de police et les agences nationales de sécurité de détecter les incidents mineurs qui font partie d'une vaste campagne de cybermenace, et qu'ils pourront collaborer plus efficacement –, l'immensité du phénomène, de par sa nature et son volume, fait en sorte qu'il ne sera pas toujours possible d'intenter des poursuites. Néanmoins, le Comité est préoccupé par le fait que, selon le surintendant principal Flynn, seul un « une petite fraction, en pourcentage » de la cybercriminalité perpétrée contre des Canadiens mène à des accusations[107].

Recommandation 6

Afin d'assurer l'exactitude et l'exhaustivité des statistiques, le Comité recommande que le gouvernement du Canada encourage les citoyens et les entreprises du Canada à signaler tous les cas de cybercriminalité.

A. Signalement des atteintes à la vie privée

Le Commissariat à la protection de la vie privée du Canada (CPVP) croit que la déclaration obligatoire des atteintes à la vie privée a déjà des retombées positives pour la cybersécurité. La déclaration obligatoire par les organisations du secteur privé des atteintes substantielles à la sécurité des renseignements personnels[108] est entrée en vigueur le 1er novembre 2018. Selon le CPVP, cette exigence permet de brosser un tableau plus clair de la nature et de l'ampleur des enjeux de cybersécurité au Canada. Gregory Smolynec, sous-commissaire du Secteur des politiques et de la promotion du

106 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Chris Lynan, directeur général par intérim, Coordination nationale contre la cybercriminalité, Gendarmerie royale du Canada), 42e législature, 1re session, 28 janvier 2019.

107 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Surintendant principal Mark Flynn, directeur général, Criminalité financière et cybercriminalité, Opérations criminelles de la police fédérale, Gendarmerie royale du Canada), 42e législature, 1re session, 28 janvier 2019.

108 En vertu de l'article 10.1 de la *Loi sur la protection des renseignements personnels et les documents électroniques*, toute atteinte à la vie privée doit être déclarée si elle présente un risque réel de préjudice à l'endroit des personnes concernées.

CPVP, a indiqué que depuis que la déclaration de ces atteintes est obligatoire, le CPVP a constaté qu'il y avait quatre fois plus de signalements de la part du secteur privé[109].

Six mois après l'entrée en vigueur de la disposition, M. Smolynec indiquent que les choses se précisent quant à la nature des pratiques du secteur privé en matière de cybersécurité. « Les institutions ne sont pas toujours au courant des renseignements personnels qu'elles détiennent, de l'endroit où ils sont acheminés et des personnes qui y ont accès », a-t-il déclaré, ajoutant que les pratiques organisationnelles de cybersécurité négligent souvent la menace interne. À ce sujet, il a noté ce qui suit :

> Souvent, dans la course à la protection contre les pirates informatiques, la menace interne est négligée; pourtant, les atteintes à la vie privée impliquent non seulement la perte de renseignements personnels au profit de forces externes, mais aussi un accès inapproprié par des acteurs internes. Les exigences de déclaration obligatoire des atteintes peuvent permettre aux institutions de répondre au caractère adéquat – ou à son absence – des plans et des préparatifs en matière de cybersécurité[110].

Le CPVP s'intéressent aussi aux avancées technologiques, telles que les systèmes bancaires ouverts[111], a dit M. Smolynec. « Il est possible de bénéficier de services bancaires ouverts dans d'autres pays, ce qui va bientôt se faire au Canada aussi et qui changera les modèles d'affaires et la façon dont les renseignements personnels et les données circulent entre institutions financières. » Précisant que ces changements seront lourds de conséquences pour les droits à la vie privée, M. Smolynec a affirmé que les normes, les règlements et les lois du Canada devront être adaptés en conséquence avant l'introduction de ces changements[112].

En ce qui concerne le rythme auquel les changements sont introduits, le Comité tient à souligner l'importance de la consultation de toutes les parties prenantes. À cet égard, le Comité note que le président de l'Association canadienne des sociétés mutuelles d'assurance, M. Norman Lafrenière, a indiqué que son organisation avait été encouragée

---

109 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Gregory Smolynec, sous-commissaire, Secteur des politiques et de la promotion, Commissariat à la protection de la vie privée du Canada), 42e législature, 1re session, 3 avril 2019.

110 *Ibid*.

111 Le Comité consultatif sur un système bancaire ouvert, formé par le ministère des Finances le 26 septembre 2018, dénifit la notion de système bancaire ouvert comme « un cadre où les consommateurs et les entreprises peuvent autoriser des tiers fournisseurs de services financiers à avoir accès aux données sur leurs opérations financières au moyen de canaux sécurisés en ligne ». Voir ministère des Finances, *Examen des mérites d'un système bancaire ouvert : Document de consultation*, janvier 2019.

112 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Gregory Smolynec, sous-commissaire, Secteur des politiques et de la promotion, Commissariat à la protection de la vie privée du Canada), 42e législature, 1re session, 3 avril 2019.

« à ne pas parler aux députés » de leurs préoccupations concernant les services bancaires ouverts[113].

Le CPVP réclame également une réforme fondamentale de la loi sur la vie privée du Canada. En plus du pouvoir de rendre des ordonnances, semblable à celui détenu par l'homologue britannique du CPVP (le Bureau du commissaire à l'information), M. Smolynec a dit préconiser une « réforme fondée sur les droits », qu'il a expliquée comme suit :

> À l'heure actuelle, le droit régissant le secteur privé est fondé sur des principes et, en un sens, il est très vaste. Soit dit en passant, il est question de droit à la vie privée des Canadiens, mais une loi fondée en droit reconnaîtrait, comme le fait le Canada, que la vie privée est un droit de la personne internationalement reconnu et que des droits procéduraux sont associés aux droits de la personne. La loi reconnaîtrait également que les secteurs public et privé dans leur ensemble seraient visés. Les Canadiens devraient être informés de leurs droits et de la façon de les exercer. C'est à la fois un défi législatif et un défi connexe d'éducation du public[114].

CHAPITRE 7 — VERS UNE CYBERSÉCURITÉ ACCRUE

A. Divulgation des vulnérabilités

Il est extrêmement difficile, voire impossible, d'éliminer toutes les failles des logiciels, des micrologiciels et du matériel informatique. Il est certainement possible de resserrer les mesures pour éliminer les failles élémentaires, par exemple en changeant les mots de passe d'administrateur par défaut. Il n'en demeure pas moins que notre environnement numérique contient des systèmes archaïques à la sécurité défaillante, auxquels s'en ajoutent d'autres tous les jours[115]. Comme l'a expliqué M. Jobert Abma, le fondateur de HackerOne, un fournisseur de services de sécurité exploitant le potentiel des pirates informatiques :

---

113 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Normand Lafrenière, président, Association canadienne des sociétés mutuelles d'assurance), 42e législature, 1re session, 27 février 2019.

114 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Gregory Smolynec, sous-commissaire, Secteur des politiques et de la promotion, Commissariat à la protection de la vie privée du Canada), 42e législature, 1re session, 3 avril 2019.

115 Voir, par exemple, la référence aux risques posés par les systèmes existants non corrigés dans Comité permanent de la sécurité publique et nationale de la Chambre des communes, Mémoire, *Se défendre en amont et supposer qu'il y a eu intrusion : Préparer le Canada à un avenir cyberrésilient* (Jonathan Reiber, chef, Stratégie de cybersécurité, Illumio), 42e législature, 1re session, 10 avril 2019, p. 4.

> L'Internet est un système très complexe auquel un grand nombre de gens contribuent. Tous ses éléments sont liés entre eux. Les systèmes et les réseaux changent ou contiennent des centaines de milliers de logiciels ou de composantes et des milliers de lignes de code. Chaque fois qu'un code est mis à jour, ce qui peut se produire plusieurs fois par jour, de nouvelles vulnérabilités peuvent apparaître[116].

HackerOne offre des programmes de « prime aux bogues », qui permettent aux organisations clientes d'inviter des « hackers éthiques » à détecter et à corriger les vulnérabilités de leurs systèmes. Un « hacker éthique » est quelqu'un de très doué pour cerner les failles des systèmes de cyberdéfense, mais qui veut se servir de ses trouvailles pour prévenir une cyberattaque. La prime aux bogues est un moyen de récompenser les chapeaux blancs pour leur aide et de les encourager à continuer de divulguer de manière responsable les résultats de leurs recherches.

C'est un modèle qui repose sur la force du nombre. D'après la vice-présidente aux Politiques de HackerOne, M^me^ Deborah Chang, l'entreprise a plus de 300 000 pirates éthiques inscrits sur sa plateforme, et compte le Département de la Défense des États-Unis parmi ses clients[117]. M^me^ Chang a ajouté ce qui suit :

> Grâce à sa diversité et à son ampleur, la communauté des pirates éthiques arrive à trouver des failles que les détecteurs automatisés ou les équipes permanentes qui réalisent des tests de pénétration ne décèleront pas. Les modèles existants sont bons pour trouver les vulnérabilités prévisibles en matière de sécurité, mais il est encore plus important d'arriver à repérer les failles imprévisibles: l'inconnu des inconnus. Ainsi, si on lui en donne le temps, un groupe de pirates éthiques assez grand arrivera à détecter ces vulnérabilités[118].

PayPal, un client de HackerOne aux États-Unis, a indiqué au Comité que les entreprises peuvent déterminer les critères de ce qu'elles traiteront comme une divulgation responsable. Brian Johnson, directeur principal de la Sécurité de l'information, PayPal, a décrit la politique de son entreprise comme suit :

> S'il y avait une brèche dans le système, cela dénoterait une activité non autorisée et serait traitée comme un accès malveillant et illégitime comme pour tout autre cas de piratage mal intentionné. Nous ne demandons pas aux chapeaux blancs qui font la chasse aux bogues de mener des attaques ou des violations de système, et dans le cadre de notre politique, ils n'ont pas le droit d'accéder aux données des clients ni de faire des

116 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Jobert Abma, fondateur, HackerOne), 42^e^ législature, 1^re^ session, 4 février 2019.

117 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Deborah Chang, vice-présidente, Politiques, HackerOne), 42^e^ législature, 1^re^ session, 4 février 2019.

118 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Deborah Chang, vice-présidente, Politiques, HackerOne), 42^e^ législature, 1^re^ session, 4 février 2019.

> manipulations ou d'apporter des changements à l'information. Ces chercheurs peuvent divulguer les vulnérabilités qu'ils détectent dans le système et nous en faire rapport grâce au programme de divulgation responsable[119].

Le Comité note que, dans un cadre bien géré, les primes aux bogues peuvent s'avérer un moyen rentable pour les organisations, y compris les ministères, de détecter et de corriger les vulnérabilités. Le Comité reconnaît que certaines entreprises canadiennes ont déjà des programmes à cet effet, mais il est d'avis que le gouvernement pourrait en faire plus pour promouvoir cette importante mesure de cybersécurité.

Parallèlement, il faut veiller à ce que les organismes de sécurité nationale et les fournisseurs de produits respectent leur part du marché. Par exemple, il arrive parfois que les organisations n'interviennent pas immédiatement à la lumière des vulnérabilités qui leur ont été rapportées, ce qui met dans une situation intenable le chercheur qui a accepté de ne pas divulguer publiquement ce qu'il a découvert[120].

Chris Parsons, associé de recherche au Citizen Lab de la Munk School of Global Affairs, a noté que malgré ses grandes responsabilités en matière de cybersécurité, le Centre de la sécurité des télécommunications (CST) a intérêt à ne pas divulguer publiquement des données sur les vulnérabilités[121]. Il a indiqué que le CST tait parfois volontairement ce qu'il sait afin de pouvoir continuer à utiliser ces vulnérabilités pour remplir son mandat offensif, soit celui de recueillir des données étrangères. Pour déterminer s'il convient de divulguer les vulnérabilités ou de les taire au profit de son mandat offensif, le CST a recours à un processus d'évaluation des nouvelles capacités en matière de vulnérabilités[122]. Bien que M. Scott Jones ait assuré au Comité que le processus décisionnel du CST va toujours favoriser la défense[123], M. Parsons a fait valoir que

---

119 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Brian Johnson, directeur principal, Sécurité de l'information, PayPal Inc.), 42e législature, 1re session, 29 mai 2019.

120 Les délais d'exécution des mesures correctives sont habituellement prévus dans les ententes de non divulgation. Voir Comité permanent de la sécurité publique et nationale de la Chambre des communes, Mémoire (Chris Parsons, associé en recherche, Monk School of Global Affairs and Public Policy, Université de Toronto), 42e législature, 1re session, par. 18.

121 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Chris Parsons, associé en recherche, Monk School of Global Affairs and Public Policy, Université de Toronto), 42e législature, 1re session, 27 février 2019.

122 À noter que le terme utilisé en anglais par le Comité (« vulnerabilities equities process ») est calqué sur la terminologie employée par ses proches alliés. Voir, par exemple, Whitehouse, *Vulnerabilities Equities Policy and Process for the United States Government*, 15 novembre 2017; et Ian Levy, *Equities process*, (blogue) National Cyber Security Centre [DISPONIBLE EN ANGLAIS SEULEMENT].

123 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Jones, chef adjoint, Sécurité des technologies de l'information, Centre de la sécurité des télécommunications), 42e législature, 1re session, 20 septembre 2018.

contrairement à celui de certains de nos alliés, le processus du CST est totalement opaque. Il a ainsi formulé la recommandation suivante :

> Pour dissiper ces préoccupations, nous suggérons que le gouvernement canadien diffuse ses programmes actuels d'équité en matière de vulnérabilités et tienne des consultations sur l'efficacité de ceux-ci à protéger les logiciels et équipements utilisés dans le cadre d'activités financières. De plus, le gouvernement pourrait inclure des intervenants du milieu des affaires et de la société civile dans le programme – actuel ou mis à jour – d'équité en matière de vulnérabilités. L'inclusion de ces intervenants favoriserait une divulgation accrue des vulnérabilités, ce qui aurait pour effet d'accroître la disponibilité de logiciels bien rédigés et de réduire les menaces qui planent sur le secteur financier[124].

Certains de nos alliés, comme les États-Unis, ont déjà rendu public leur processus d'évaluation des nouvelles capacités en matière de vulnérabilités[125], ce qui donne à penser qu'il est peut-être temps d'envisager une plus grande transparence à ce sujet au Canada.

Recommandation 7

Le Comité recommande que le gouvernement du Canada appuie les programmes de divulgation responsable de la vulnérabilité.

B. Chiffrement rigoureux : aujourd'hui et demain

Un thème récurrent s'est imposé tout au long de l'étude du Comité : il faut en faire plus pour s'assurer que la sécurité fasse partie intégrante des appareils que nous utilisons, et qu'elle ne soit plus traitée comme une fonction optionnelle coûteuse. S'inspirant du concept de la « protection de la vie privée dès la conception » de l'ancienne commissaire à l'information et à la protection de la vie privée de l'Ontario, Ann Cavoukian, des témoins ont réclamé l'adoption d'une approche favorisant la « sécurité dès la conception »[126].

Reconnaissant que la cybersécurité commence par de bonnes pratiques d'ingénierie de la sécurité, le Comité constate avec inquiétude que les services de sécurité nationale et les

---

124 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Chris Parsons, associé en recherche, Monk School of Global Affairs and Public Policy, Université de Toronto), 42e législature, 1re session, 27 février 2019.

125 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Chris Parsons, associé en recherche, Monk School of Global Affairs and Public Policy, Université de Toronto), 42e législature, 1re session, 27 février 2019.

126 Voir, par exemple, Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (David Masson, directeur, Sécurité d'entreprise, Darktrace), 42e législature, 1re session, 18 mars 2019.

organismes d'application de la loi du monde entier envisagent encore d'affaiblir les systèmes de chiffrement pour permettre l'accès légal. C'est d'autant plus inquiétant que le secteur financier dépend fortement de cette technologie pour assurer la cybersécurité.

Une telle insistance en faveur d'un chiffrement moins rigoureux pour permettre un accès légal ne cadre pas avec les témoignages entendus par le Comité. En effet, on lui a fait part des préoccupations des organismes responsables de la sécurité nationale à l'égard de la menace que posent les systèmes informatiques quantiques. Même s'il n'a pas voulu donner de détails, le chef de la sécurité de l'information de Paiements Canada a confirmé que le CST a consulté son organisation au sujet des enjeux de sécurité que présente l'informatique quantique[127]. Si le CST s'inquiète de la menace que l'informatique quantique posera peut-être un jour pour le chiffrement à clé publique, ne devrait-il pas s'en faire tout autant pour les menaces qui planent aujourd'hui sur l'intégrité du chiffrement?

Certains considèrent que l'accès légal est une faiblesse intentionnelle officiellement autorisée. Un témoin a d'ailleurs recommandé de rejeter toute loi sur l'accès légal afin de garantir un accès public aux techniques de chiffrement robustes. Arguant en faveur d'une politique responsable en matière de chiffrement, Chris Parsons, a défini un chiffrement fort comme suit :

> Un chiffrement fort peut largement être défini comme des algorithmes de chiffrement pour lesquels aucune faiblesse ou vulnérabilité n'est connue ou n'a été intégrée, ainsi que des applications informatiques qui ne contiennent pas délibérément des faiblesses visant à miner l'efficacité des algorithmes susmentionnés[128].

D'une part, le Comité reconnaît qu'il est important, à des fins de sécurité et de protection de la vie privée, que tous les Canadiens aient accès à des techniques de chiffrement robustes. D'autre part, il est conscient que cela va engendrer des problèmes, notamment pour les organismes d'application de la loi non fédéraux, qui, contrairement à la GRC, ne peuvent pas faire appel au CST pour du soutien technique et opérationnel.

---

127 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Martin Kyle, chef de la sécurité de l'information, Paiements Canada), 42e législature, 1re session, 8 avril 2019.

128 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Chris Parsons, associé en recherche, Monk School of Global Affairs and Public Policy, Université de Toronto), 42e législature, 1re session, 27 février 2019.

Recommandation 8

Le Comité recommande que le gouvernement du Canada rejette les approches à l'accès légal qui affaibliraient la cybersécurité.

C. Aider les petites et moyennes entreprises à assurer leur cybersécurité

Comme au Canada, les petites et moyennes entreprises contribuent à l'économie de l'Australie. Selon le professeure Jill Slay, l'Australie dépend de ses PME à peu près autant que le Canada. Tout comme les PME canadiennes, les PME australiennes doivent souvent impartir des volets importants de leurs activités, y compris la cybersécurité. Et selon la professeure Slay, celle-ci ne fait pas nécessairement partie des ententes d'externalisation négociées par les entreprises australiennes. Le professeure Slay a indiqué que les PME australiennes peuvent s'en remettre à des fournisseurs de services pour leurs besoins généraux de technologie de l'information et de communication, mais que dans bien des cas « on ne comprend même pas la nécessité de se procurer la cybersécurité comme service[129] ».

Comme l'a mentionné le professeure Slay, le ministère de l'Industrie de l'Australie a créé un réseau de centres de cybercroissance (Australian Cyber Security Growth Network) afin de remédier à la situation. Elle a indiqué que cette initiative permet à l'Australie de développer son industrie de la cybersécurité, en finançant des petites entreprises qui créent des produits-créneaux, du matériel et des logiciels spécialisés.

En creusant un peu, le Comité a découvert que ce réseau organise également des événements appelés « GovPitch », qui permettent à des propriétaires de petite entreprise de faire un petit topo pour présenter leur produit à des dirigeants d'organismes gouvernementaux, des dirigeants principaux de l'information et des dirigeants principaux de la sécurité de l'information[130]. L'idée est non seulement d'aider les PME ayant des produits de cybersécurité innovants à décrocher des marchés publics, mais aussi d'alerter les pouvoirs publics sur des produits dont ils ignoraient l'existence.

Cette philosophie semble rejoindre celle adoptée par le CST avec le Centre canadien pour la cybersécurité. Juste avant d'être nommé à la tête du Centre, M. Scott Jones avait

129 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Jill Slay, professeure, présidente de la cybersécurité La Trobe Optus, La Trobe University, Melbourne), 42e législature, 1re session, 20 février 2019.

130 Australian Cyber Security Growth Network, *GovPitch*.

dit au Comité qu'il souhaitait que le Centre favorise l'innovation en jouant les « entremetteurs » entre les entreprises aux prises avec un problème de cybersécurité et celles qui ont une bonne solution à leur offrir[131]. Il a également expliqué que le Centre était conçu pour encourager les partenariats publics-privés :

> [N]ous visons à ce que les gens puissent venir travailler dans ce centre. À l'heure actuelle, quand les gens visitent le CST, nous leur retirons tous leurs appareils électroniques, parce qu'ils entrent dans un immeuble très secret. Ce ne sera pas le cas du cybercentre. Les gens pourront venir dans nos installations physiques pour y collaborer et y apporter carrément leurs appareils pour que nous puissions voir comment ils fonctionnent et développer des choses ensemble[132].

Comme l'Australie, le Canada doit non seulement améliorer le savoir-faire et les pratiques des PME en matière de cybersécurité, mais aussi veiller à ce que celles-ci aient accès aux meilleurs outils qui soient dans le domaine.

Comme le Comité l'a appris des témoins, notre pays a innové et continue d'innover dans des technologies clés de cybersécurité telles que le chiffrement, l'intelligence artificielle et l'informatique quantique. Ces innovations canadiennes naissent souvent d'une entreprise en démarrage ou d'une entreprise dérivée d'un projet de recherche universitaire. Le Comité est d'avis que le Canada ne devrait ménager aucun effort pour s'assurer que ces petites entreprises restent ici et réalisent leur plein potentiel.

Plutôt que de permettre à d'autres d'exploiter nos idées, le Canada doit s'engager à soutenir davantage l'innovation d'ici en matière de cybersécurité. Si le cybercentre du CST peut contribuer à cet objectif, ce sera tant mieux. Mais la meilleure chose à faire est de soutenir l'innovation en la mettant à l'œuvre. À cette fin, le Comité presse le gouvernement de s'inspirer de l'Australie et d'organiser des événements « topo », afin d'ouvrir son processus d'approvisionnement aux solutions et services de cybersécurité offerts par les jeunes entreprises canadiennes.

---

131 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Jones, chef adjoint, Sécurité des technologies de l'information, Centre de la sécurité des télécommunications), 42e législature, 1re session, 20 septembre 2018.

132 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Scott Jones, chef adjoint, Sécurité des technologies de l'information, Centre de la sécurité des télécommunications), 42e législature, 1re session, 20 septembre 2018.

CHAPITRE 8 — SOUVERAINETÉ DES DONNÉES

« Le meilleur allié lui-même protégera-t-il les intérêts de ses amis si ses propres infrastructures sont menacées? » Voilà la question qu'Andrew Clement, professeur émérite, de la Faculté d'information de l'Université de Toronto, a posée au Comité en ce qui a trait aux États-Unis.

Le professeur Clement dirige une équipe de recherche qui a élaboré un nouvel outil Web d'appairage à un point d'échange Internet[133] appelé « IX-Map ». Cet outil permet aux Canadiens de voir le chemin qu'empruntent leurs données lorsqu'ils consultent des sites Web. M. Clement a fourni au Comité des statistiques qui semblent indiquer clairement que le Canada n'a que très peu de contrôle sur cette portion de l'Internet. Selon lui, « environ 80 % des communications canadiennes avec d'autres pays que les États-Unis passent physiquement par les États-Unis[134] ».

Au moins un quart des communications Internet entre Canadiens finissent par passer par les États-Unis, a indiqué le professeur Clement. C'est ce qu'il appelle le « routage boomerang ». Il a expliqué comment son équipe avait découvert le phénomène :

> Au début de nos recherches, nous avons détecté un cheminement [qui] montre le chemin que parcourent les données entre mon bureau à l'Université de Toronto et le site Web du programme d'aide aux étudiants de l'Ontario, lequel est hébergé dans le complexe du gouvernement provincial, qui se trouve à quelques minutes de marche.
>
> Ce chemin nous a étonnés, d'autant plus que la voie que les données empruntaient pour entrer aux États-Unis et en revenir passait par le même édifice de Toronto, soit le plus grand centre d'échange Internet du Canada, sis au 151, rue Front. Voilà qui était pour le moins contraire à la présomption d'efficacité optimale du routage Internet; cela nous a incités à pousser plus loin notre étude afin de voir à quel point le phénomène était répandu et de comprendre les raisons de ce comportement contre-intuitif. [C'est] un phénomène qui s'avère fort commun. Nous estimons qu'au moins 25 % du trafic de données canadien passe par les États-Unis. Selon l'Autorité canadienne pour les enregistrements Internet, ou ACEI, ce chiffre serait bien plus élevé[135].

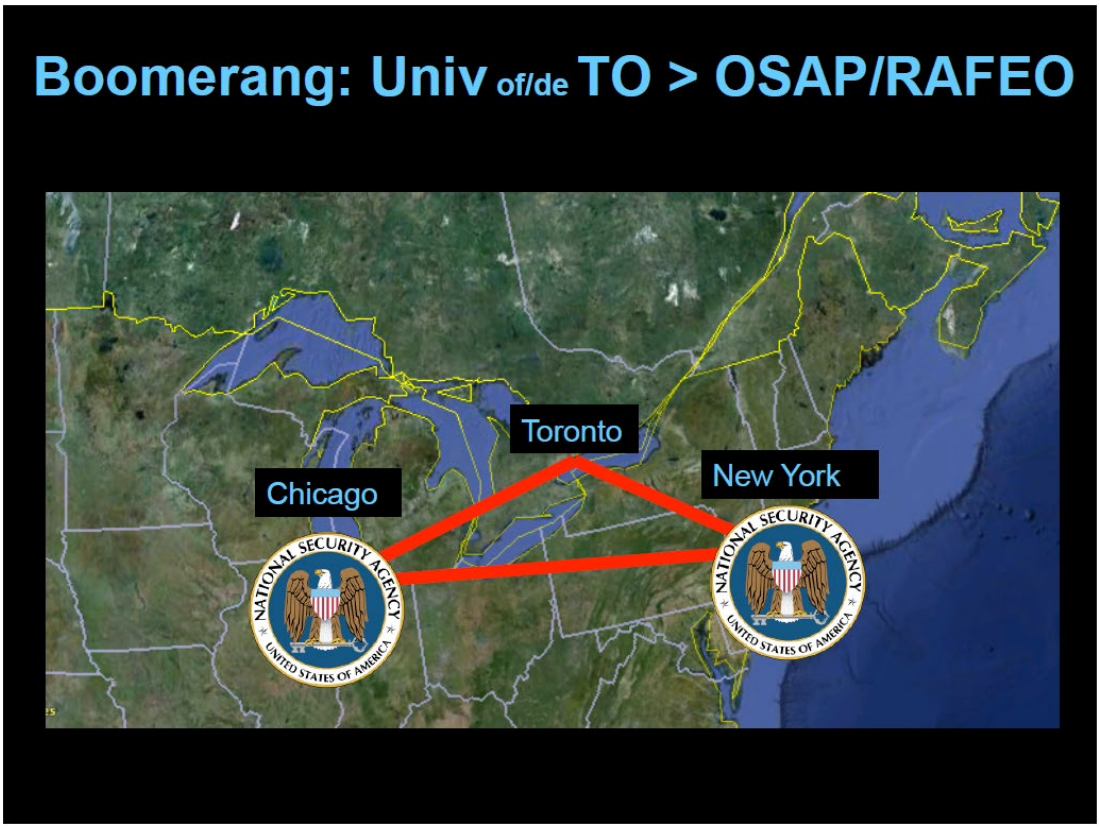
---

133 Selon l'Autorité canadienne pour les enregistrements Internet (ACEI) : « Un IXP (point d'échange Internet) est une plaque tournante où les réseaux indépendants ont la possibilité de s'interconnecter directement les uns aux autres, ce qui leur procure une importante largeur de bande et une faible latence à un coût inférieur à celui du transit traditionnel. » Voir ACEI, *Infrastructure Internet au Canada : Points d'échange Internet (IXP) canadiens*.

134 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Andrew Clement, professeur émérite, Faculty of Information, Université de Toronto), 42e législature, 1re session, 18 mars 2019.

135 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Andrew Clement, professeur émérite, Faculty of Information, Université de Toronto), 42e législature, 1re session, 18 mars 2019.

Graphique 1: Carte de routage "Boomerang":
Envoi d'un courriel de l'autre côté de la rue à Toronto via les États-Unis



Comme le témoin l'a décrit ci-dessus, l'image montre une carte du Canada et des États-Unis recouverte d'un triangle dont Toronto est au sommet et New York et Chicago aux deux angles de base. Les armoiries de la National Security Agency des États-Unis sont représentées sous les deux angles de base. L'image montre comment, une fois que les données quittent le territoire canadien, le Canada peut perdre sa juridiction légale sur celles-ci.

Source: Image soumise par le professeur Andrew Clement lors de son témoignage.

Puisque le Canada n'a pas de contrôle souverain sur ses flux de données, le professeur Clement a demandé au Comité d'imaginer ce qui arriverait si les États-Unis décidaient de couper toute connexion externe en réaction à une cyberattaque. Il a dit ceci :

> Si, pour une raison quelconque, notre connexion avec les États-Unis était coupée, même si c'était pour des motifs légitimes d'autodéfense, à quel point le réseau Internet du

> Canada s'avérerait-il résilient? Nous devrions le savoir, mais nous l'ignorons. Les preuves disponibles laissent penser qu'il serait très peu résilient[136].

Afin de remédier à la situation, le professeur Clement a formulé plusieurs recommandations. Il a entre autres recommandé que « toutes les données de nature essentielle et délicate du Canada soient entreposées, acheminées et traitées au Canada ». Il a aussi suggéré au gouvernement de « soutenir l'établissement et l'utilisation de points d'échange direct de données entre les réseaux en évitant le routage aux États-Unis », et d'inclure des exigences de reddition de comptes dans les normes de cybersécurité des institutions financières et des fournisseurs de services de télécommunications en ce qui concerne les pratiques de routage[137].

En ce qui concerne la recommandation du professeur Clement voulant que le Canada affirme sa souveraineté sur toutes les données nationales sensibles et critiques, il convient de noter que l'Association des banquiers canadiens a confirmé au Comité que les données canadiennes sont potentiellement exposées lorsqu'une institution financière canadienne confie certains de ses services à une entreprise située dans un territoire étranger. « S'il s'agit d'un tiers indépendant, les lois du pays où l'information est détenue par ce tiers pourraient s'appliquer », a indiqué M. Docherty[138]. PayPal est l'une des entités du secteur financier ayant confirmé que les données canadiennes sont entreposées aux États-Unis. Il semble que ce soit aussi le cas pour Mastercard, qui a dit au Comité : « la majorité des transactions s'effectuent à nos installations de St. Louis ou de Kansas City[139] ». Le chef de la sécurité de Mastercard Canada, M. Ron Green, a ajouté que les efforts déployés pour localiser les données pourraient compromettre son travail :

> D'où je suis, je peux voir les auteurs de menaces tenter d'agir contre le système de paiement, peu importe où ils se trouvent. Mais plus les pays localisent ou tentent de

136 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Andrew Clement, professeur émérite, Faculty of Information, Université de Toronto), 42e législature, 1re session, 18 mars 2019.

137 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Andrew Clement, professeur émérite, Faculty of Information, Université de Toronto), 42e législature, 1re session, 18 mars 2019.

138 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Charles Docherty, avocat général adjoint, Association des banquiers canadiens), 42e législature, 1re session, 18 mars 2019.

139 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Ron Green, vice-président exécutif et chef de la sécurité, Mastercard Canada), 42e législature, 1re session, 1er avril 2019.

> localiser les données, ce qui empêche d'utiliser ces données ailleurs, plus ma capacité d'analyser la situation et de suivre les mouvements des auteurs de menaces diminue[140].

De son côté, Terri O'Brien, agente principale de gestion des risques d'Interac Corporation, a déclaré que son entreprise conserve les données canadiennes strictement en sol canadien. Elle a dit ceci :

> Nous ne sommes pas disposés à permettre la sortie de données, compte tenu de la constitution canadienne et de nos racines. Notre société, qui a été constituée il y a environ un an, est solidement enracinée au Canada. Toutes nos données doivent demeurer au pays. Nous faisons également appel à des fournisseurs canadiens pour la prestation de tous nos services, mais nous concevons nos propres technologies[141].

S'ils sont exécutés avec soins, le Comité estime que les efforts visant à bâtir l'infrastructure numérique du Canada peuvent servir à la fois les intérêts économiques du pays et sa sécurité nationale. Un objectif important serait que le Canada améliore sa connectivité avec l'Europe et l'Asie, tout en réduisant sa dépendance envers les États-Unis. La région arctique du Canada pourrait ainsi offrir des possibilités à cet égard. Par exemple, le Comité a entendu parler d'une initiative qui propose d'accroître la connectivité à large bande dans le Nord du Canada en se reliant à un câble de télécommunications internationales situé dans les eaux internationales au large de l'Alaska et en développant la région de la Baie James en tant qu'épicentre de la technologie infonuagique[142]. Ce genre d'initiative contribuerait à la souveraineté du Canada dans le Nord et à sa souveraineté sur les données canadiennes en général.

Recommandation 9

Le Comité recommande que le gouvernement du Canada explore de nouveaux moyens pour s'assurer que toutes les données sensibles qui circulent au Canada suivent un chemin de routage domestique et ne sont pas exposées à une infrastructure réseau étrangère.

---

140 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Ron Green, vice-président exécutif et chef de la sécurité, Mastercard Canada), 42e législature, 1re session, 1er avril 2019.

141 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Terri O'Brien, agente principale de gestion des risques, Interac Corporation), 42e législature, 1re session, 8 avril 2019.

142 Comité permanent de la sécurité publique et nationale de la Chambre des communes, *Témoignages* (Tawich Development Corporation), 42e législature, 1re session, 15 mai 2019.

CONCLUSION

Le Canada devrait s'assurer de saisir toutes les occasions de soutenir la concurrence dans l'économie numérique internationale, tout en maximisant sa capacité de faire respecter le droit à la vie privée et la sécurité de ses citoyens dans ce domaine. Ceux qui comptent sur le secteur financier pour garantir leurs économies et leurs moyens de subsistance doivent savoir qu'ils ont raison d'avoir confiance en leurs pratiques en matière de cybersécurité.

ANNEXE A
LISTE DES TÉMOINS

Le tableau ci-dessous présente les témoins qui ont comparu devant le Comité lors des réunions se rapportant au présent rapport. Les transcriptions de toutes les séances publiques reliées à ce rapport sont affichées sur la page Web du Comité sur cette étude.

Organismes et individus	Date	Réunion
Centre d'analyse des opérations et déclarations financières du Canada	2019/01/28	145
Dan Lambert, directeur adjoint Renseignement et opérations		
Barry MacKillop, sous-directeur Opérations		
Gendarmerie royale du Canada	2019/01/28	145
Mark Flynn, directeur général Criminalité financière et la cybercriminalité, Opérations criminelles de la police fédérale		
Chris Lynam, directeur général par intérim Coordination nationale contre la cybercriminalité		
À titre personnel	2019/01/30	146
Christian Leuprecht, professeur Département de sciences politiques, Collège militaire royal du Canada		
Centre de la sécurité des télécommunications	2019/01/30	146
Eric Belzile, directeur général Gestion des incidents et atténuation des menaces, Centre canadien pour la cybersécurité		
Scott Jones, dirigeant principal Centre canadien pour la cybersécurité		
Forum des politiques publiques	2019/01/30	146
Satyamoorthy Kabilan, vice-président Politiques		

Organismes et individus	Date	Réunion
À titre personnel	2019/02/04	147
Steve Waterhouse, ancien officier de sécurité des systèmes d'information Ministère de la Défense nationale		
HackerOne	2019/02/04	147
Jobert Abma, fondateur		
Deborah Chang, vice-présidente Politiques		
FireEye, Inc.	2019/02/06	148
Christopher Porter, chef d'intelligence stratégique		
Illumio	2019/02/06	148
Jonathan Reiber, chef Stratégie de cybersécurité		
À titre personnel	2019/02/20	149
Yuval Shavitt, professeur, Tel Aviv University		
Jill Slay, professeure présidente de la cybersécurité La Trobe Optus, La Trobe University, Melbourne		
Association canadienne des compagnies d'assurance mutuelles	2019/02/27	151
Normand Lafrenière, président		
Citizen Lab	2019/02/27	151
Christopher Parsons, associé en recherche Munk School of Global Affairs and Public Policy, University of Toronto		
Quantum-Safe Canada	2019/02/27	151
Michele Mosca, directeur		
Brian O'Higgins, président		
SkyBridge Strategies	2019/02/27	151
Steve Masnyk, principal		
À titre personnel	2019/03/18	152
Andrew Clement, professeur émérite Faculty of Information, University of Toronto		

Organismes et individus	Date	Réunion
Association des banquiers canadiens	2019/03/18	152
Charles Docherty, avocat général adjoint		
Andrew Ross, directeur Paiements et Cybersécurité		
Chambre de commerce du Canada	2019/03/18	152
Scott Smith, directeur principal Propriété intellectuelle et politique d'innovation		
Trevin Stratton, économiste en chef		
Darktrace	2019/03/18	152
David Masson, directeur Sécurité d'entreprise		
Échange canadien de menaces cybernétiques	2019/04/01	154
Robert Gordon, directeur exécutif		
Cybersecure Catalyst	2019/04/01	154
Charles Finlay, directeur exécutif		
EY	2019/04/01	154
Thomas Davies, chef de fil mondial des services financiers et des affaires numériques		
Mastercard Canada	2019/04/01	154
Ron Green, vice-président exécutif et chef de la sécurité		
Commissariat à la protection de la vie privée du Canada	2019/04/03	155
Leslie Fournier-Dupelle, analyste stratégique des politiques et de la recherche		
Gregory Smolynec, sous-commissaire Secteur des politiques et de la promotion		
Banque Toronto Dominion	2019/04/03	155
Glenn Foster, chef de la sécurité de l'information		
Interac Corp.	2019/04/08	156
Terri O'Brien, agente principale de gestion des risques		
Paiements Canada	2019/04/08	156
Justin Ferrabee, chef des opérations		
Martin Kyle, chef de la sécurité de l'information		

Organismes et individus	Date	Réunion
À titre personnel	2019/04/10	157
Richard B. Fadden		
Groupe ADGA	2019/04/10	157
Steve Drennan, directeur Cybersécurity		
Amazon Web Services, Inc.	2019/04/10	157
Mark Ryland, directeur Bureau du dirigeant principal de l'information		
À titre personnel	2019/05/15	163
Luc Jarry, conseiller sénior en cybersécurité		
Tawich Development Corporation	2019/05/15	163
Tony Gull, président		
Sam W. Gull, conseiller		
Robert Milot, conseiller		
Jean Fernand Schiettekatte, conseiller		
PayPal, Inc.	2019/05/29	165
Brian Johnson, directeur principal Sécurité de l'information		

ANNEXE B
LISTE DES MÉMOIRES

Ce qui suit est une liste alphabétique des organisations et des personnes qui ont présenté au Comité des mémoires reliés au présent rapport. Pour obtenir de plus amples renseignements, veuillez consulter la page Web du Comité sur cette étude.

Citizen Lab

Cockfield, Arthur

Illumio

In Fidem

In-Sec-M

Jarry, Luc

Leuprecht, Christian

Quantum-Safe Canada

Skillicorn, David

DEMANDE DE RÉPONSE DU GOUVERNEMENT

Conformément à l'article 109 du Règlement, le Comité demande au gouvernement de déposer une réponse globale au présent rapport.

Un exemplaire des *procès-verbaux* pertinents (réunions nos 145 à 149, 151, 152, 154 à 157, 163, 165, 168 et 170) est déposé.

Respectueusement soumis,

Le président,
L'hon. John McKay, C.P., député