CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

Comité permanent de la sécurité publique et nationale

SECU • NUMÉRO 145 • 1re SESSION • 42e LÉGISLATURE

TÉMOIGNAGES

Le lundi 28 janvier 2019

Président

L'honorable John McKay

Comité permanent de la sécurité publique et nationale

Le lundi 28 janvier 2019

● (1530)

[*Traduction*]

Le président (L'hon. John McKay (Scarborough—Guildwood, Lib.)): Chers collègues, nous allons commencer. Je vois que nous avons le quorum, alors je vais déclarer la séance ouverte.

Bienvenue à la première séance du Comité visant à étudier la cybersécurité dans le secteur financier comme un enjeu de sécurité économique nationale, une étude qui s'avère très opportune à la lumière des événements des dernières semaines.

Pour entamer l'étude, nous recevons M. MacKillop et son collègue, M. Lambert. Ils ont tous deux une grande expérience des témoignages devant les comités parlementaires.

Nous nous réjouissons à la perspective d'entendre votre exposé de 10 minutes. Ensuite, mes collègues poseront des questions.

Monsieur MacKillop.

M. Barry MacKillop (sous-directeur, Opérations, Centre d'analyse des opérations et déclarations financières du Canada): Merci, monsieur le président. Bonjour, chers membres.

Je suis heureux d'être parmi vous en compagnie de M. Lambert. Nous sommes également accompagnés de M. Juneau qui nous aidera à faire défiler les diapositives. Il m'aurait été très difficile d'accomplir ces deux tâches en même temps.

Au nom du CANAFE, j'aimerais vous remercier de l'occasion qui m'est donnée d'exposer ce qu'est le CANAFE et qui nous sommes. Je sais que notre organisme n'est pas particulièrement bien connu. Par conséquent, j'espère qu'aujourd'hui, je serai en mesure de vous renseigner un peu plus sur la nature de nos activités et sur la façon dont nous les exerçons.

Le CANAFE est le Centre d'analyse des opérations et déclarations financières du Canada.

[*Français*]

En passant, la présentation sera probablement plus en anglais, mais évidemment, nous pourrons répondre aux questions en français aussi.

[*Traduction*]

Notre organisme a été fondé en 2000. Sa loi habilitante est la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes, dont je n'énumérerai pas toutes les versions et toutes les modifications. Le CANAFE est un organisme indépendant qui rend des comptes au Parlement par l'entremise du ministre des Finances. C'est l'URF du Canada, c'est-à-dire l'Unité du renseignement financier, et c'est également l'organisme de réglementation de la conformité des entreprises qui sont assujetties à la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes. Notre administration se trouve à Ottawa, et nous avons trois bureaux régionaux, dont un à Montréal, un à Toronto et un à Vancouver. Les bureaux régionaux s'occupent de nos activités de conformité, de nos examens et de l'évaluation des entités déclarantes qui relèvent de nous. Notre bureau d'Ottawa s'occupe de toutes nos activités liées au renseignement. Notre budget s'élève à environ 55 millions de dollars par année.

Le centre n'est pas — et c'est là un point important qui n'est pas toujours compris — un organisme d'enquête. C'est une unité administrative du renseignement financier, ce qui signifie que nous recevons des déclarations. Nous ne pouvons pas solliciter et recueillir activement des déclarations. Nous ne pouvons pas demander aux entités déclarantes de nous fournir des déclarations particulières portant sur des personnes ou des entités particulières. Nous n'effectuons aucun travail secret sur le Web. Nous ne menons aucune activité sinistre ou secrète sur le Web, ou quoi que ce soit de ce genre. Notre objectif est d'analyser les déclarations que nous recevons des entités déclarantes, des déclarations que les entités déclarantes sont tenues de produire en vertu de la loi.

La loi limite également les renseignements particuliers que nous pouvons divulguer. Si vous me demandiez si j'ai communiqué des renseignements sur une personne ou un cas particulier, je ne serai pas en mesure de vous répondre selon la loi. Si je le faisais, cela constituerait essentiellement une communication illégale, pour laquelle je serais passible d'une peine d'emprisonnement de cinq ans. Comme vous pouvez le comprendre, ce n'est pas une chose que j'aimerais faire. Alors, malheureusement, nous ne pouvons pas vous parler des cas particuliers dont nous nous occupons, mais nous pouvons vous parler de la façon dont nous procédons et des activités que nous exerçons en général.

Comme vous pouvez le constater sur cette première diapositive, il y a un certain nombre de secteurs d'entités déclarantes. Il s'agit là des secteurs qui, en vertu de la loi, sont obligés de produire des déclarations et de nous les remettre. Au Canada, nos partenaires clés englobent un certain nombre d'organismes et de ministères qui sont tous responsables de certains aspects du régime de lutte contre le blanchiment d'argent et le financement des activités terroristes au Canada. Les destinataires des communications, c'est-à-dire les organismes auxquels je peux légalement communiquer des renseignements à condition que les seuils établis par la loi en matière de déclaration et de communication aient été atteints, figurent du côté gauche de la diapositive.

Au nombre des types de déclarations que le CANAFE reçoit, on retrouve les transferts électroniques de fonds de plus de 10 000 $, en provenance ou à destination du Canada, auxquels s'applique également une règle de 24 heures. Nous recevons également des déclarations d'opérations importantes en espèces de 10 000 $ ou plus, ainsi que des déclarations de déboursements de casino qui rendent compte des sommes de 10 000 $ ou plus qui sont versées à un casino ou par un casino. Enfin, nous recevons des déclarations d'activités liées à des biens appartenant à des groupes terroristes et des déclarations d'opérations douteuses.

Les déclarations d'opérations douteuses sont, en fait, ce que nous aimons appeler notre gagne-pain. Il n'y a pas de seuil financier à atteindre dans le cas de ces déclarations. Il revient donc aux entités déclarantes de produire une déclaration à notre intention chaque fois qu'elles soupçonnent qu'une opération pourrait être liée au blanchiment d'argent ou au financement d'activités terroristes. Habituellement, les entités nous fournissent également un exposé des faits. Ces exposés nous apportent des renseignements importants de grande qualité que nous pouvons ensuite communiquer à nos partenaires de l'application de la loi lorsque sont remplis nos propres critères du doute raisonnable lié au blanchiment d'argent ou au financement d'activités terroristes.

De plus, bien que l'ASFC ne soit pas une entité déclarante, l'agence nous fait parvenir des déclarations de mouvements transfrontaliers d'espèces et des rapports de saisie visant des opérations transfrontalières. En outre, nous recevons aussi des déclarations de renseignements transmis volontairement de la part d'organismes d'application de la loi et de sécurité nationale, et nous pouvons en obtenir auprès d'autres organismes gouvernementaux et de membres du public, s'ils souhaitent exposer leurs propres soupçons ou présenter leurs propres renseignements sur ce qu'ils pensent être du blanchiment d'argent ou du financement d'activités terroristes, ou ce qu'ils perçoivent comme tel.

● (1535)

Nous recevons également des demandes de renseignements et des communications de la part de nos partenaires internationaux. Nous avons signé 105 PE avec des unités étrangères du renseignement. Ces unités peuvent nous communiquer des renseignements, et nous sommes libres de faire de même, selon les PE que nous avons signés.

Que faisons-nous exactement? Nous obtenons nos rapports auprès des entités déclarantes. Au chapitre de la conformité, nous utilisons des examens, des évaluations et différentes techniques pour nous assurer que les entités respectent les règles établies par la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes. Une fois les déclarations reçues, nous effectuons nos propres recherches de renseignements et nous procédons à nos propres analyses de ces déclarations. Il va de soi que nous relions ces travaux aux déclarations de renseignements transmis volontairement que nous pourrions avoir reçues des organismes d'application de la loi et de sécurité nationale. Si le seuil en matière de communication est atteint, nous communiquons le renseignement financier tactique pour appuyer les enquêtes en cours ou, dans certains cas, nous lançons des enquêtes de façon préventive.

De plus, nous exerçons des activités de renseignement stratégique en examinant surtout les tendances, les topologies et les recherches que nous menons sur les technologies nouvelles et à venir et sur les menaces émergentes qui planent sur les institutions financières et sur le régime de lutte contre le blanchiment d'argent et le financement des activités terroristes.

En tout, nous recevons approximativement 25 millions de déclarations par année, et c'est ce sur quoi nous fondons notre analyse. Comme je l'ai indiqué plus tôt, le centre n'est pas un organisme d'enquête. Par conséquent, nous ne pouvons pas rechercher des renseignements supplémentaires. Bien entendu, avant de communiquer des renseignements aux organismes d'application de la loi ou de sécurité nationale, nous utilisons de l'information de source ouverte pour compléter notre analyse.

Comme je l'ai mentionné, nous élaborons des produits de renseignement financier stratégique. Ils sont habituellement liés à des cibles, des personnes, des entités ou des enquêtes particulières. Nous fournissons ces produits aux services de police. Par ailleurs, nous pouvons les fournir aux organismes d'application de la loi et de sécurité nationale, selon les seuils établis. Nous pouvons aussi les fournir à l'ARC en cas d'évasion fiscale, par exemple, ou à l'ASFC en cas d'inadmissibilité. De plus, nous pouvons fournir ces produits à nos partenaires internationaux si un lien a été établi entre le Canada et un partenaire international ou un autre pays. Enfin, si nous avons conclu un PE et que nous avons obtenu le pouvoir et l'autorisation de nos partenaires canadiens de l'application de la loi, nous pouvons aussi les fournir à nos URF internationales.

Nous recueillons également une assez importante quantité de renseignements stratégiques afin de pouvoir examiner des perspectives d'analyse portant sur la nature et la portée des menaces dans ce secteur. La lutte contre le blanchiment d'argent et le financement des activités terroristes est manifestement un univers qui évolue rapidement. Nous nous efforçons donc de rester aussi vigilants que nous le pouvons à cet égard. Nous disposons d'une unité du renseignement stratégique qui s'occupe de cet enjeu.

En ce qui concerne nos contributions, nous avons fourni des communications sur tous les types de fraude, y compris les arnaques romantiques. Nous allons aborder directement cette question en parlant du partenariat public-privé que nous avons établi avec la Banque HSBC et le Centre antifraude du Canada, ainsi qu'avec les organismes d'application de la loi et les principales banques de l'ensemble du Canada. Le projet Chameleon a été lancé en 2017, en s'appuyant sur le succès du projet Protect, qui visait le blanchiment d'argent lié à la traite des personnes. En revanche, le projet Chameleon est axé sur le blanchiment d'argent lié aux stratagèmes d'arnaque romantique. Selon le Centre antifraude du Canada, ces stratagèmes sont l'un des types de fraude les plus importants et les plus lucratifs au Canada. Comme vous pouvez l'imaginer, ces stratagèmes ont tendance à viser les personnes âgées. Je ne pense pas devoir expliquer en quoi consiste une arnaque romantique étant donné que nous le savons probablement tous. Toutefois, si la question est soulevée pendant les séries de questions, nous y répondrons à ce moment-là. Compte tenu du temps écoulé, nous allons passer à la prochaine diapositive.

Je précise encore une fois qu'au lieu de passer en revue tous ces aspects, nous allons examiner notre rôle au chapitre du renseignement stratégique qui nous permet de cerner les technologies émergentes. Nous suivons l'évolution des technologies financières novatrices, des tendances et des développements. Certains membres de notre personnel sont chargés d'effectuer ce genre de recherche. Nous travaillons également avec nos partenaires internationaux par l'intermédiaire du Groupe Egmont ou du Groupe d'action financière. Nous collaborons aussi avec d'autres partenaires internationaux afin d'élaborer des tendances, des topologies et des rapports, ainsi que de repérer les menaces potentielles qui pèsent sur le régime — ces menaces pourraient déjà peser sur le régime ou pourraient le faire dans les années à venir —, en examinant les secteurs où les technologies émergentes surgissent et leurs liens avec la lutte contre le blanchiment d'argent et le financement des activités terroristes.

● (1540)

Monsieur le président, je pense m'être arrêté un peu avant l'expiration du temps qui m'était imparti. Je vais donc en rester là. Toutefois, je suis disposé à répondre à toutes les questions que vous pourriez avoir.

Le président: Merci, monsieur MacKillop. Vous êtes manifestement très professionnel. Vous avez dépassé de deux secondes le temps qui vous était imparti.

Monsieur Picard, vous avez la parole pendant sept minutes.

M. Michel Picard (Montarville, Lib.): Monsieur MacKillop, je vous invite à répondre à mes questions dans la langue de votre choix. Cependant, pour pouvoir m'exprimer de façon aussi technique que possible, permettez-moi de poser mes questions en français.

[*Français*]

Vous avez clairement expliqué que le CANAFE n'est pas une agence d'enquête mais une agence d'analyse, comme son nom l'indique.

Ai-je raison de dire que, parce que vous faites de l'analyse, vous êtes en mesure de détecter les comportements anormaux ou les stratagèmes frauduleux, quels qu'ils soient? Dans les nouveaux stratagèmes utilisés, quel est l'aspect technologique qui a évolué dans les cinq à dix dernières années? Quelle évolution technologique avez-vous vue dans les stratagèmes que vous analysez?

M. Barry MacKillop: Nous sommes en position de faire cela. Comme vous l'avez dit, nous faisons de l'analyse stratégique, mais nous regardons aussi l'aspect tactique. Selon les cas, nous pouvons voir les changements qui sont survenus.

Dans les dernières années, nous avons surtout vu des modes de paiement différents et le désir d'anonymat, par exemple en utilisant les cryptomonnaies. Pour que les transactions soient encore plus anonymes, on a maintenant recours à ce qu'on appelle des « mélangeurs ». Il devient ainsi de plus en plus difficile de détecter les comportements anormaux, qui existent tant au Canada qu'à l'échelle internationale.

Cela représente un défi au regard de l'application de la loi ainsi que pour les organismes qui luttent contre le blanchiment d'argent. Il est certain que c'est l'évolution des modes de paiement qui pose le plus de défis.

● (1545)

M. Michel Picard: Dans un stratagème de blanchiment d'argent, on pourrait dire que toute la chaîne de transactions est légale, sauf l'origine criminelle de l'argent qu'on doit blanchir. Il m'apparaît que les moyens techniques utilisés pour blanchir l'argent, en dépit des progrès technologiques, ne servent qu'à accélérer les transactions et, de ce fait, à mieux effacer leur trace. Ces moyens techniques nuisent à la capacité d'enquêter, car les transactions passent par différents pays.

Selon vous, les nouvelles technologies utilisées servent-elles simplement à augmenter l'efficacité et la rapidité des transactions, ou sont-elles plutôt utilisées comme outils de fraude ou de crime dans le milieu cybernétique? J'exclus ici la cryptomonnaie, car c'est un monde un peu particulier. La technologie utilisée est-elle un moyen d'augmenter la rapidité des transactions ou y a-t-il d'autres technologies qui sont carrément des outils d'attaque directe?

M. Barry MacKillop: C'est une bonne question et je vais y répondre en anglais, parce que cela commence à être un peu plus technique.

[*Traduction*]

Comme vous le savez, une grande partie de ces activités se déroulent en anglais à l'échelle mondiale. Par conséquent, si je parle de cryptomonnaies — je pense que c'est l'équivalent français de *cryptocurrencies* —, nous observons quelques tendances. Oui, ces activités se déroulent plus rapidement. Certes, ces opérations sont effectuées plus rapidement.

Si vous analysez certains types de fraude comme les arnaques romantiques, par exemple, oui, l'argent blanchi a tendance à être un produit de la criminalité. Cependant, en ce qui concerne les arnaques romantiques, leurs produits sont déjà présents dans le système financier. Ces arnaques consistent à utiliser des médias sociaux et différentes façons de se rendre anonyme ou d'assumer une fausse identité afin de tirer profit de gens qui vous envoient de l'argent, que vous blanchissez par ces moyens. Le crime est peut-être lié à une fausse représentation de votre identité, plutôt qu'à la commission d'un crime physique comme le fait de cambrioler une banque et de tenter de blanchir l'argent recueilli.

Vous avez raison. Ces opérations sont plus rapides, et elles peuvent contourner... Si vous utilisez des outils du genre de la cryptomonnaie, vous pouvez contourner le système financier en tant que tel.

Nous remarquons également que la vitesse à laquelle les opérations peuvent être effectuées augmente. En ce qui concerne les types de crimes, grâce à l'utilisation des médias sociaux et des outils de ce genre pour voler des identités ou assumer de fausses identités — comme en créant un faux profil dans Facebook et en prenant des mesures de ce genre pour devenir « ami » avec des gens et tirer parti d'eux —, nous observons de plus en plus fréquemment ce genre de crimes. Il est certain que les criminels profitent également de la possibilité d'utiliser Internet et de l'information de source ouverte pour repérer des victimes potentielles.

Ensuite, il y a les autres secteurs comme ceux des rançongiciels, par exemple, dans lesquels le criminel peut envoyer un faux courriel ou prendre le contrôle de l'ordinateur de quelqu'un et exiger qu'une somme soit versée avant de lui redonner l'accès à son ordinateur. Nous avons observé des cas d'utilisation de rançongiciels à l'échelle internationale. Ce domaine semble être en pleine croissance en ce moment, en ce sens que les criminels sont en mesure de prendre le contrôle d'ordinateurs et d'exiger des versements. De plus en plus fréquemment, ces criminels exigent que les sommes soient versées en cryptomonnaies plutôt qu'en espèces ou au moyen d'un virement par courriel.

Oui, la possibilité d'utiliser des ordinateurs accroît la capacité.

M. Michel Picard: J'ai quelques questions rapides à poser.

[*Français*]

Vous entrez en jeu quand une transaction entrante ou sortante de 10 000 $ vous est rapportée. Vos algorithmes se limitent-ils aux transactions de 10 000 $ ou analysent-ils aussi les cas où un stratagème est utilisé pour répartir un montant s'élevant à beaucoup plus que 10 000 $ en plusieurs transactions, afin que cela passe sous le radar?

M. Barry MacKillop: Les entités déclarantes sont obligées de déclarer les transactions qui dépassent le seuil de 10 000 $, mais quand elles utilisent la déclaration d'opération douteuse, il n'y a pas de limite. Il peut s'agir de transactions de 200 $ à raison de trois ou quatre fois par semaine. Ce sont les entités déclarantes qui peuvent détecter qu'un stratagème a été utilisé, et nous recevons ces rapports. Notre analyse ne se limite pas à ce seuil.

M. Michel Picard: Je vous remercie.

Le président: Merci, monsieur Picard.

Monsieur Paul-Hus, vous avez sept minutes, s'il vous plaît.

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

Messieurs, je vous remercie de votre présence.

Notre étude n'a pas pour but de faire de l'analyse de fraude. Ce n'est pas tant l'aspect financier qui nous intéresse que l'impact sur la cybersécurité des transactions.

Nous avons bien compris que, maintenant, le CANAFE est vraiment plus un centre qui reçoit de l'information de la liste des agences que nous avons vue. Par exemple, les grands bureaux de comptables sont obligés de vous envoyer de l'information sur leurs clients. Est-ce exact?

● (1550)

M. Barry MacKillop: Oui.

M. Pierre Paul-Hus: On sait que, depuis quelques années, il y a une augmentation des transactions criminelles par Internet. De votre côté, avez-vous vu un changement? Les entreprises ne vous rapportent pas de l'information sur les transactions douteuses de personnes par bonne volonté, mais parce qu'elles ont une obligation légale de le faire. Cependant, on peut utiliser Internet pour faire des transactions et contourner cela. Si personne ne vous envoie cette information, vous ne pouvez pas en avoir connaissance. Les transactions en cryptomonnaie ou faites dans le *Dark Web*, ou le Web profond, se font à votre insu. Est-ce bien cela?

M. Barry MacKillop: Oui.

M. Pierre Paul-Hus: On ne peut pas dire que le CANAFE soit en première ligne. C'est plutôt les agences ou les entreprises qui le sont. Dans le cas qui nous occupe, ce sont les banques canadiennes et les organismes financiers qui doivent vous informer des transactions douteuses qui se font dans leur réseau.

M. Barry MacKillop: C'est bien cela.

M. Pierre Paul-Hus: Selon votre travail d'analyse, qu'est-ce qui a le plus changé depuis cinq ou dix ans? Est-ce que ce sont les transactions en cryptomonnaie? S'agissant de cybersécurité, qu'est-ce qui a changé de façon spectaculaire sur Internet?

M. Barry MacKillop: Je ne peux pas dire que ce soient les cryptomonnaies en ce moment. Ce que nous voyons surtout, c'est qu'on peut transférer de l'argent internationalement et rapidement en utilisant une banque ou ce qu'on appelle le *peer-to-peer*. On peut faire des transactions de cette façon. L'Internet permet de faire des transactions rapides et complexes et de contourner l'institution financière.

M. Pierre Paul-Hus: Le premier élément est donc le transfert d'argent. Si, par exemple, une personne veut envoyer 100 000 $ à quelqu'un d'autre au moyen d'Internet, elle va pouvoir se protéger avec des codes pour que la transaction soit cachée. Est-ce bien cela? Pourtant, à un moment donné, la somme aboutit dans un compte en banque et va donc être remarquée.

M. Barry MacKillop: Exactement. Les banques sont obligées de garder l'oeil ouvert et de suivre cela de près. Elles savent comment repérer ces transactions.

M. Pierre Paul-Hus: Les banques disposent-elles de mécanismes automatiques de détection? Sont-elles toujours prévenues si une transaction dépasse le seuil de 10 000 $?

M. Barry MacKillop: Oui. Elles le sont aussi lorsque la transaction est de moins de 10 000 $, mais qu'elle a lieu dans les 24 heures ou de façon répétitive.

Nous travaillons beaucoup et de très près avec les banques pour déterminer les indicateurs de blanchiment d'argent.

M. Pierre Paul-Hus: Je classifierais ce volet sous la rubrique de « fraude au moyen d'Internet ».

En ce qui a trait à la cybersécurité, nous visons à assurer la protection des citoyens. Nous avons parlé tantôt d'hameçonnage et d'autres méthodes du genre. En gardant à l'esprit la protection des citoyens, avez-vous constaté une augmentation marquée du nombre de rapports depuis 4 ou 5 ans, ou même depuis déjà plus de 10 ans? À quel moment cette croissance a-t-elle eu lieu? Nous avons appris qu'il y avait eu une progression de 41 % depuis 2013. S'agit-il d'un phénomène récent? Les banques sont-elles en mesure de le contrôler, ou cela devient-il un problème majeur?

M. Barry MacKillop: Je dirais que le problème est majeur, effectivement, mais que les banques font un très bon travail. Le pourcentage de nos divulgations des cinq dernières années portant sur la fraude et le blanchiment d'argent lié à la fraude est constant et se situe autour de 34 à 35 %.

M. Pierre Paul-Hus: D'accord.

En ce qui a trait au contrôle dans le contexte d'une divulgation, prenons l'exemple d'un problème dont vous êtes informé par la Banque Royale. Les autorités comme la GRC sont-elles informées? Sont-elles informées en même temps que vous? Comment cela fonctionne-t-il?

M. Barry MacKillop: Les autorités ne sont pas nécessairement alertées. Cela dépend de la situation. Les banques peuvent effectivement envoyer de l'information à la GRC.

Notre rôle, par contre, c'est de recevoir les déclarations de transactions douteuses et d'en faire l'analyse. Une fois que nous avons fini, nous pouvons prévenir soit la GRC soit un autre corps policier.

● (1555)

M. Pierre Paul-Hus: Donc, en cas de fraude, la banque va poser des gestes à l'interne, faire rapport au CANAFE et essayer de régler le problème.

M. Barry MacKillop: Oui.

M. Pierre Paul-Hus: Il n'y a donc pas nécessairement d'enquête policière à ce stade. Est-ce bien ce que vous me dites?

M. Barry MacKillop: C'est plus ou moins cela.

M. Pierre Paul-Hus: Cela dépend de l'importance de la fraude, j'imagine.

M. Barry MacKillop: C'est cela. Les banques travaillent depuis longtemps à combattre la fraude.

M. Pierre Paul-Hus: D'accord.

Êtes-vous en mesure de nous parler des menaces externes? Nous tentons d'établir comment nous protéger au Canada, mais la menace peut provenir de l'interne ou de l'externe. Pouvez-vous nous dire d'où elle vient, principalement?

M. Barry MacKillop: Nous voyons surtout des cas de fraude par des tiers.

Sur le plan de la cybersécurité, je pense que ce serait plutôt à la GRC de vous dire si la menace est principalement interne ou externe.

M. Pierre Paul-Hus: D'accord. Ce n'est pas dans votre domaine de compétence.

M. Barry MacKillop: Non.

M. Pierre Paul-Hus: Y a-t-il des choses que le gouvernement pourrait améliorer — et que vous pouvez mentionner au Comité — qui rendraient le travail de votre organisme plus efficace?

[*Traduction*]

Le président: La question est presque inappropriée étant donné que vous êtes fonctionnaire. Je vais l'autoriser au cas où vous souhaiteriez émettre des hypothèses, mais, en général...

M. Barry MacKillop: Nous n'émettons pas d'hypothèses.

Le président: Oui.

M. Barry MacKillop: Vous avez raison.

[*Français*]

Le règlement sur les bourses de monnaies numériques qui découle du projet de loi C-31 de 2014 est à l'étape de l'ébauche en ce moment. Il devrait être bientôt en vigueur et cela va nous aider sur le plan des cryptomonnaies.

[*Traduction*]

Des règlements concernant les devises virtuelles seront bientôt présentés. Nous avons mené des consultations à leur égard en juin dernier, en collaboration avec le ministère des Finances, qui est responsable des politiques liées à ce régime canadien. De vastes consultations ont été menées l'été dernier. La rédaction de ces règlements est en cours en ce moment, et les règlements régiront les devises virtuelles et leur échange, par exemple.

[*Français*]

Cela va nous aider grandement.

M. Pierre Paul-Hus: D'accord, je vous remercie.

Le président: Merci, monsieur Paul-Hus.

Nous passons maintenant à M. Dubé pour sept minutes.

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

Je remercie les témoins d'être ici.

J'ai des questions sur le mandat et les responsabilités que vous avez et qu'ont d'autres agences ou les forces policières. Plus précisément, je fais référence aux diapositives 5, 6 et 7 de votre présentation. Je vais revenir au projet Chameleon tout à l'heure.

Comment procédez-vous pour obtenir l'information que vous communiquez? Par exemple, vous avez mentionné Facebook et le fait que de plus en plus de personnes partagent des renseignements comme ceux-là.

Est-ce que c'est vous qui déterminez ces informations? Avez-vous des employés qui suivent ce qui se passe sur les réseaux sociaux? Communiquez-vous ensuite avec la police pour qu'elle agisse et qu'elle cible un individu en particulier?

La façon dont tout cela fonctionne n'est pas claire. Vous avez mentionné plusieurs éléments, mais ce n'est pas clair. Qu'est-ce qui relève de la police, et qu'est-ce qui relève de votre organisme?

M. Barry MacKillop: Toutes les enquêtes relèvent de la police. Ce que nous fournissons, c'est de l'information et des renseignements propres à une entité ou à une personne. Nous pouvons recevoir jusqu'à 25 millions de rapports par année, y compris les déclarations de transactions douteuses. Nous avons deux personnes qui y travaillent. Leur travail de tous les jours est d'étudier ces rapports.

La technologie nous permet d'identifier certains mots-clés afin de déceler une transaction douteuse particulièrement intéressante. Nous pouvons ensuite consulter notre banque de données pour voir si elle contient d'autres rapports reliés à la personne visée. Si nous atteignons notre seuil, nous pouvons divulguer la transaction à la police, de façon proactive. Il reviendrait alors à la police de décider si elle veut lancer une enquête.

Si nous recevons de l'information de la police dans le cadre d'une enquête en cours, nous allons consulter notre banque de données, ainsi que Facebook ou autre, pour voir si nous pouvons trouver d'autres liens à inclure dans le rapport que nous remettrons au corps policier. Notre rapport ne contient que de l'information tirée de notre banque de données ou de sources publiques, que nous colligeons pour la police. Par contre, c'est à elle de décider ou non de mener enquête.

● (1600)

M. Matthew Dubé: Je ne veux pas trop me limiter à un seul exemple, parce que je sais que la situation peut varier.

Quand vous dites que vous cherchez des connexions sur Facebook, cherchez-vous des liens par rapport au contenu, par exemple un site d'hameçonnage reconnu qui cherche à soutirer de l'information financière, ou aux personnes, comme les relations d'affaires qu'un individu coupable de transactions suspectes pourrait avoir avec un ami sur Facebook? Comment identifiez-vous ces gens et les connexions qu'ils ont?

Je ne vois pas beaucoup de différence entre le travail d'enquête de la police et ce que semble faire votre organisme.

M. Barry MacKillop: Nous nous bornons à fournir des renseignements, pas des éléments de preuve. Vous touchez ici aux secrets du métier.

Supposons que la police effectue une enquête à votre sujet, vous, Matthew Dubé. Si nous consultions votre page Facebook — parce que nous sommes en train de préparer un rapport à votre sujet — et que vous êtes assis à côté de M. Jim Eglinski dans une ou deux photos et qu'il semble y avoir un lien entre vous deux, nous pourrions vérifier dans notre banque de données si vous vous êtes déjà transféré de l'argent et établir s'il existe un lien financier entre vous.

Nous ne prenons pas tout ce qu'il y a sur Facebook. Il faut que cela ait un lien avec notre banque de données. Il est certain que si nous voulions établir des liens et identifier des membres de votre gang, nous pourrions le faire, mais il faudrait que cela se retrouve aussi dans notre banque de données pour que nous puissions le communiquer à la police.

M. Matthew Dubé: Je ne veux pas trop déborder du cadre de notre étude.

Dans la lutte au terrorisme, la façon dont travaillent les policiers suffit généralement à protéger les personnes innocentes et à empêcher qu'elles ne soient trouvées coupables par association. Dans l'exemple que vous venez de donner, celui d'une transaction avec moi, qui ai connu des problèmes par le passé, cet individu serait protégé par le travail des policiers. Vous vous contenteriez de dire à la police qu'il y a eu des transferts d'argent entre lui et moi, et ce serait ensuite à elle de vérifier s'il y a matière à enquête.

M. Barry MacKillop: Absolument.

Comme je vous l'ai dit, nous recevons environ 25 millions de déclarations par année, et de ce nombre, la plupart sont légitimes. Nous ne divulguons pas cela.

M. Matthew Dubé: À la page 6, vous parlez de partenariat public-privé et de blanchiment d'argent.

M. Barry MacKillop: Oui.

M. Matthew Dubé: Dans le domaine de la cybersécurité, il y a un grand débat à savoir lequel, entre public et privé, est le meilleur, et où devrait se situer l'équilibre entre les deux. Par exemple, les banques se vantent beaucoup de ce qu'elles ont fait, mais j'imagine qu'elles travaillent souvent en collaboration avec vous. Votre organisation a-t-elle une idée sur la façon de trouver cet équilibre?

Vous n'êtes pas nécessairement ici pour élaborer les politiques, mais vous les mettez en oeuvre. Y a-t-il un équilibre qui, à votre avis, vous permettrait de bien faire votre travail et permettrait au secteur privé de continuer à innover pour protéger les consommateurs?

M. Barry MacKillop: Nous réalisons déjà trois projets dans le cadre de partenariats public-privé. Dans ce contexte, nous travaillons avec la police et le secteur privé pour élaborer des indicateurs, qu'il s'agisse de blanchiment d'argent relié à la traite de personnes, à la fraude ou à la vente de fentanyl. Jusqu'à maintenant, cela donne de très bons résultats. Tous les gens semblent travailler dans leur domaine et y faire ce qu'ils peuvent. Ils travaillent très bien ensemble. Nous recevons beaucoup plus de déclarations d'opérations douteuses. Nous avons constaté que le fait d'avoir élaboré des indicateurs aussi spécifiques que possible liés à une catégorie de crime augmentait la qualité et la quantité de déclarations d'opérations douteuses que nous recevons.

[*Traduction*]

Le président: Merci, monsieur Dubé.

Pour une raison quelconque, la bande Dubé-Eglinski ne nous apparaît pas comme un élément inspirant la terreur.

Des voix: Oh, oh!

M. Barry MacKillop: J'ai simplement pensé que je devrais rapprocher un peu les membres du Comité.

Le président: Oui. C'est un drôle d'arrangement.

Monsieur Spengemann, vous disposez de sept minutes.

● (1605)

M. Sven Spengemann (Mississauga—Lakeshore, Lib.): Merci, monsieur le président.

Je remercie nos deux témoins de leur présence aujourd'hui.

Je veux d'abord prendre quelques instants pour parler du financement des activités terroristes, de la création du CANAFE en 2000 et des suites du 11 septembre 2001.

De 2003 à 2005, j'ai eu la chance de m'occuper de réglementation intelligente au sein de la fonction publique. Le CANAFE était l'un de nos interlocuteurs dans le cadre de cet exercice au sein du périmètre de sécurité de l'Amérique du Nord. Nous sommes rendus en 2019. Pouvez-vous nous parler des tendances qui semblent se dégager en matière de financement du terrorisme ainsi que du travail que vous accomplissez pour que les Canadiens continuent de vivre en sécurité? Je fais aussi partie du comité de la défense. Il y a une connexion directe avec le travail qui se fait de ce côté-là également. Quelle est l'importance de vos efforts actuels pour contrer le financement des activités terroristes et quelles tendances êtes-vous à même d'observer?

M. Dan Lambert (directeur adjoint, Renseignement et opérations, Centre d'analyse des opérations et déclarations financières du Canada):

Le financement des activités terroristes est une problématique en pleine évolution pour le CANAFE. Comme le disait M. MacKillop, nous travaillions au départ avec des banques et des institutions semblables qui avaient l'habitude de composer avec les cas de fraude et pouvaient facilement nous présenter des rapports à ce sujet. Le contexte de la menace a évolué depuis. Les banques demandent de plus en plus l'aide d'organisations comme le CANAFE pour pouvoir faire le suivi du financement des activités terroristes, d'autant plus que les sommes d'argent en cause sont généralement peu élevées.

Au fil des dernières années, nous avons travaillé en étroite collaboration avec les banques en leur fournissant des indicateurs clairs quant aux transactions à surveiller. Parallèlement à cela, nous collaborons de très près avec le Service canadien du renseignement de sécurité et les services de sécurité nationale de la GRC. Il y a donc évolution de nos relations avec les banques quant aux modes de divulgation utilisés.

M. Sven Spengemann: Il demeure quand même encore aujourd'hui que la perturbation des réseaux de financement est l'un des éléments clés dans notre lutte contre le terrorisme.

M. Dan Lambert: Tout à fait.

M. Sven Spengemann: Selon vous, est-ce que le seuil de déclaration de 10 000 $ demeure adéquat? Y a-t-il moyen de contourner cette règle en cumulant des sommes qui transitent via d'autres canaux? Ce seuil fait-il en sorte qu'une partie des montants en circulation échappent à votre analyse?

M. Barry MacKillop: Le plus souvent, le seuil établi demeure utile. Dans le cas du financement des activités terroristes, ce seuil n'est pas vraiment significatif, car bon nombre des transactions en la matière sont d'un montant moindre, comme vient tout juste de l'indiquer M. Lambert.

Nos efforts sont surtout consacrés à l'analyse et à la collaboration avec les entités déclarantes de même qu'à la sensibilisation, au rayonnement et à l'établissement d'indicateurs que nous devons diffuser concernant les différents types de crimes, y compris le financement du terrorisme. Nous venons tout juste de publier un guide sur la manière de remplir une déclaration d'opérations douteuses, les secteurs auxquels nous pouvons nous intéresser, comme les sociétés de transferts de fonds, et les indicateurs qui sont propres à chacun. C'est en travaillant ainsi de façon proactive en partenariat avec nos entités déclarantes que nous pouvons continuer à produire des rapports de qualité.

M. Sven Spengemann: D'accord.

En matière de justice pénale, est-ce que votre mandat se limite aux infractions liées au blanchiment d'argent et à la cyberfraude?

M. Barry MacKillop: Le blanchiment d'argent, le financement des activités terroristes et les menaces pour la sécurité du Canada.

M. Sven Spengemann: Est-ce que votre mandat comprend le piratage de données à proprement parler, soit le vol de données, plutôt que le vol d'argent ou le détournement de fonds?

M. Barry MacKillop: Non, à moins qu'une banque soit visée par le piratage et que l'on s'empare d'idées importantes ou de sommes d'argent, ou encore que l'on utilise un rançongiciel. Pour ce genre de piratage, il est effectivement possible que nous recevions une déclaration d'opérations douteuses.

M. Sven Spengemann: S'il s'agit d'une infraction hybride, soit un piratage assorti d'une fraude, comment se fait le partage des responsabilités entre votre organisation et les autres agences s'intéressant aux activités de piratage?

M. Barry MacKillop: Nous n'interviendrions pas en pareil cas.

Comme nous l'indiquions, nous pouvons analyser uniquement les déclarations que nous recevons, puis produire nos propres rapports à l'issue de ces analyses. En l'absence de lien entre une telle infraction et une déclaration d'opérations douteuses, par exemple, nous n'en serions sans doute jamais informés.

M. Sven Spengemann: Est-ce que vous travaillez en étroite collaboration avec nos partenaires et alliés internationaux, notamment au sein du Groupe des cinq, dans le domaine de la cybersécurité?

M. Barry MacKillop: Non, pas en matière de cybersécurité, si ce n'est pour comprendre l'utilisation des cryptomonnaies et des mélangeurs, le mode de transfert des fonds dans un monde virtuel et des éléments semblables. Nous travaillons avec eux pour dégager notamment les tendances et les structures topologiques.

M. Sven Spengemann: Où situez-vous le Canada au sein du Groupe des cinq, et peut-être à l'échelle planétaire, quant à l'efficacité de notre travail à ce chapitre? Y a-t-il des lacunes sur lesquelles notre comité pourrait vouloir se pencher?

M. Barry MacKillop: Je ne suis pas certain de pouvoir vous parler de la perception générale concernant l'efficacité du Canada en matière de cybersécurité. Peut-être que les gens de la GRC seraient mieux placés pour le faire. Pour ce qui est des services de renseignement financier, notre travail est très apprécié.

M. Sven Spengemann: J'aimerais aborder en terminant le principe voulant qu'un degré élevé de cybersécurité soit bénéfique pour les affaires au Canada. Autrement dit, si nous parvenons à établir des conditions de base propices à la cybersécurité au moyen de partenariats public-privé, le Canada pourra attirer des investissements étrangers directs en offrant un contexte d'affaires sécuritaire.

Dans quelle mesure parvenons-nous à atteindre un tel résultat en partenariat avec les banques pour les protéger contre les attaques et les autres formes de cyberfraude financière? Y a-t-il d'autres moyens que nous pourrions mettre en oeuvre et auxquels nous devrions nous intéresser de plus près?

M. Barry MacKillop: Malheureusement, ces enjeux ressortent un peu du cadre de mon mandat. Notre collaboration avec les banques se limite aux exigences qu'elles ont à remplir quant aux rapports à produire en vertu de la LRPCFAT. Pour ce qui est de la cybersécurité, je dois malheureusement vous répondre que vous devriez vous adresser directement aux banques.

M. Sven Spengemann: D'accord.

M. Barry MacKillop: Chacune fonctionne à sa manière, et je suis persuadé qu'elles ont des problèmes qui leur sont propres. Je sais que les banques prennent très au sérieux les questions de cybersécurité, mais je ne saurais vous dire dans quelle mesure elles se tirent bien à ce niveau.

M. Sven Spengemann: À votre point de vue, c'est aux banques elles-mêmes qu'il incombe de s'occuper de leurs propres plateformes de sécurité.

M. Barry MacKillop: C'est ce que je crois.

M. Sven Spengemann: Il n'y a aucun soutien qui vienne directement du gouvernement?

M. Barry MacKillop: Aucun soutien qui vienne du CANAFE en tout cas. Je ne saurais vous dire pour le reste du gouvernement.

M. Sven Spengemann: D'accord. Merci pour ces précisions.

Monsieur le président, je crois que je suis arrivé au bout du temps à ma disposition.

● (1610)

Le président: Merci.

Peut-être pourrais-je profiter des 15 secondes qui restent à M. Spengemann pour vous poser une question. Le temps que vous receviez les rapports, que vous procédiez à votre analyse et que vous renvoyiez le tout, le mal n'est-il pas déjà fait?

M. Barry MacKillop: Tout dépend de la situation. Il n'est pas rare en effet qu'il soit trop tard et que le crime ait déjà été perpétré, mais il y a aussi des cas où les criminels ne sont pas arrivés à leurs fins ultimes. Il y a une distinction à faire entre les différents stratagèmes visant le blanchiment d'argent et les activités de financement qui doivent aboutir à la perpétration d'un acte terroriste. Selon moi, l'argent qui est blanchi est souvent un produit de la criminalité, ce qui fait que le crime a déjà été commis, alors que nous pouvons contribuer à empêcher qu'un acte terroriste se produise lorsque le financement vise de telles fins.

Le président: Merci pour cette réponse.

Monsieur Motz, vous avez cinq minutes.

M. Glen Motz (Medicine Hat—Cardston—Warner, PCC): Merci, monsieur le président, et merci, messieurs, de votre présence aujourd'hui.

Vous avez indiqué très clairement — et en insistant sur ce point — que vous n'êtes pas là pour effectuer des enquêtes. Vous recevez des informations, mais vous n'en faites pas la collecte. Vous les recevez puis les transmettez aux agences chargées de faire enquête ou de faire appliquer la loi.

Dans ce contexte, pouvez-vous nous expliquer comment se font les échanges d'information et quel moyen vous prenez pour veiller à ce que les services de sécurité nationale, si la situation l'exige, ou les corps de police disposent de tous les renseignements nécessaires, à partir de ce qui vous a été communiqué, pour mettre un frein aux activités criminelles? Sans nous révéler de secrets, pouvez-vous nous dire comment tout cela se passe dans les faits?

M. Barry MacKillop: Je ne vais pas vous révéler les secrets du métier.

Nous recevons les déclarations. Nous avons une base de données étanche. Contrairement à la plupart des autres services de renseignement financier dans le monde, personne n'a accès à notre base de données, pas même les corps policiers et les autres instances chargées d'appliquer les lois. L'accès est limité aux employés du CANAFE, et plus particulièrement à ceux du service du renseignement tactique qui travaillent sur le dossier concerné. Le principe du « besoin de savoir » s'applique au sein même de notre organisation.

Nous recevons donc l'information. Dans le cas d'une déclaration d'opérations douteuses, par exemple, l'un des deux employés affectés au dossier peut détecter certains mots clés. On peut notamment penser au projet Protect qui cible la traite de personnes. Après avoir pris connaissance de la déclaration, on la transmet à un chef d'équipe du secteur géographique. Nos équipes sont en effet constituées en fonction des différentes régions. Le chef d'équipe de la région du Centre, par exemple, peut alors faire quelques recherches rapides dans la base de données pour voir si l'on y trouve des transactions correspondantes. Le dossier est ensuite remis à l'un de nos analystes.

Il n'est pas rare qu'il soit indiqué dans la déclaration d'opérations douteuses, surtout dans le cas du projet Protect, que des sommes d'argent sont passées du compte X au compte Y, ou d'une adresse Internet à une autre. Nous tenons alors compte de ces indications et procédons à une recherche dans l'ensemble de la base de données pour voir si d'autres transactions pourraient être associées à celles-là de telle sorte que les forces de l'ordre puissent compter sur un portrait complet de la situation.

Après cela, nous montons notre propre dossier. Nous avons des relevés récapitulatifs, des tableaux des transactions, des graphiques i2 et des fiches techniques indiquant qui est visé par la divulgation et pour quels motifs. Nous consultons certaines sources ouvertes d'information. Nous vérifions également dans notre base de données pour déterminer si l'affaire peut être reliée à un dossier précédent au sujet duquel nous avons fait une divulgation. Le cas échéant, nous l'ajoutons à notre rapport. Nous transmettons ensuite le tout à l'agence chargée de faire appliquer la loi en pareil cas.

● (1615)

M. Glen Motz: Compte tenu de ce que vous venez de nous dire — et merci pour ces précisions très utiles —, quelle forme prend votre collaboration avec l'Agence de consommation en matière financière du Canada? Quels renseignements communiquez-vous à cette agence?

M. Barry MacKillop: Aucun.

M. Glen Motz: Travaillez-vous avec des agences d'évaluation du crédit comme Equifax ou TransUnion, ou quoi que ce soit de semblable, de manière à pouvoir protéger les consommateurs grâce aux informations qui vous sont transmises? Si vous recevez de l'information...

Si j'en crois votre signe de tête, vous ne communiquez pas de renseignements à ces agences-là non plus.

M. Barry MacKillop: C'est exact.

M. Glen Motz: S'il en est ainsi, lorsque vous recevez des renseignements au sujet de formes répandues de fraude pouvant toucher les Canadiens, dois-je comprendre que votre mandat ne vous amène pas à communiquer ces renseignements aux agences qui pourraient mettre les Canadiens à l'abri de ces fraudes?

M. Barry MacKillop: Ce n'est pas applicable à cette étape.

M. Glen Motz: Disons qu'il est question d'une escroquerie amoureuse ou d'une arnaque semblable. Est-ce que vous diffusez des bulletins pour alerter les gens via les agences de protection du consommateur ou d'évaluation du crédit de telle sorte que le Canadien moyen puisse mieux savoir à quoi s'en tenir?

M. Barry MacKillop: Oui, mais pas du point de vue tactique. Nous essayons de dégager les grandes stratégies et les structures topologiques. Nous avons produit des rapports à ce sujet. Dans une perspective opérationnelle, nous avons aussi diffusé des fiches et des alertes. Dans certains cas, ces documents peuvent être rendus publics et accessibles sur notre site Web. Ils peuvent être envoyés à nos entités déclarantes ou même à une instance internationale qui s'en sert pour créer un produit accessible à plus grande échelle.

M. Glen Motz: Je vais profiter des quelques secondes qu'il me reste pour vous demander de vous engager à transmettre par écrit au Comité des précisions sur les mesures prises par le CANAFE pour protéger les Canadiens à l'égard d'escroqueries semblables. Est-ce chose possible?

M. Barry MacKillop: Le mandat du CANAFE ne consiste pas nécessairement à... Cela ne fait pas partie de notre mandat. Nous sommes là pour détecter et prévenir le blanchiment d'argent et le financement des activités terroristes, et dissuader ceux qui voudraient se livrer à de telles activités. La plus grande partie de notre travail s'effectue dans une perspective tactique. Du point de vue stratégique, tout ce qui est affiché sur notre site Web est accessible à tous. Est-ce que nous transmettons directement ces renseignements à l'Agence de consommation en matière financière, par exemple? Non. Est-ce que nous leur divulguons des renseignements de nature tactique? Absolument pas. Ce serait illégal pour nous de le faire.

Si nous émettons des fiches ou des alertes opérationnelles, toutes nos entités déclarantes vont les recevoir... À titre d'exemple, notre alerte concernant le fentanyl est accessible à tous. Des renseignements peuvent aussi être consultés relativement au projet Project, au partenariat public-privé et aux indicateurs liés au blanchiment d'argent aux fins de la traite de personnes. Ces renseignements sont accessibles, mais il n'y a rien de plus.

Le président: Merci, monsieur Motz.

Madame Dabrusin, vous avez cinq minutes.

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

Je vais revenir un peu en arrière, car vous avez indiqué dès le départ que vous n'effectuez pas vous-même d'enquêtes...

M. Barry MacKillop: C'est exact.

Mme Julie Dabrusin: ... si bien que vous devez compter sur d'autres instances pour compiler de l'information en fonction de certains paramètres. Je présume que vous aidez ces autres intervenants à déterminer dans quelle mesure ils doivent pousser leurs enquêtes et quels renseignements ils doivent rechercher. Ils vous transmettent ensuite le tout. Est-ce que c'est à peu près...

M. Barry MacKillop: Si je puis me permettre, toutes les modalités concernant les rapports requis sont établies dans la loi ou le règlement.

Mme Julie Dabrusin: Oui.

M. Barry MacKillop: La loi les oblige à nous signaler les transactions de ce genre.

Mme Julie Dabrusin: Est-ce que vous leur fournissez certaines indications? J'avais cru comprendre tout à l'heure que vous les aidiez à déterminer quelles transactions peuvent sembler suspectes ou à savoir comment s'y prendre pour remplir leurs déclarations, notamment.

M. Barry MacKillop: Tout à fait.

Mme Julie Dabrusin: C'est ensuite à ces entités qu'il incombe de concevoir leurs propres algorithmes ou modes de recherche pour obtenir les renseignements qu'elles doivent vous transmettre.

M. Barry MacKillop: C'est exact.

Mme Julie Dabrusin: Y a-t-il des écarts quant à la qualité de l'information qui vous est communiquée? Est-ce que certaines institutions sont mieux équipées pour vous fournir cette information?

À titre d'exemple, il y a les banques, mais aussi ces petits établissements qui prêtent de l'argent ou encaissent les chèques de paye. Est-ce que la qualité de l'information qui vous est transmise est la même dans les deux cas?

● (1620)

M. Barry MacKillop: Non. En général, les grandes banques mettent à profit leurs capacités et leur expérience pour nous fournir des renseignements de qualité. La quantité est également au rendez-vous, car près de 90 % de nos déclarations nous viennent de ces banques.

Mme Julie Dabrusin: La qualité et le niveau de complexité des rapports peuvent varier d'une institution à l'autre.

M. Barry MacKillop: Tout à fait.

Mme Julie Dabrusin: Est-ce que certaines institutions font appel à la sous-traitance pour la collecte de ces renseignements? Il est possible que celles qui sont de plus petite taille ne disposent pas des capacités nécessaires à l'interne. Est-ce que l'on a recours à des sous-traitants à cette fin?

M. Barry MacKillop: C'est effectivement chose possible.

Mme Julie Dabrusin: Il a été question à quelques reprises des individus qui pouvaient être en cause. Les algorithmes utilisés permettent également le suivi des transactions faites par différents individus pour obtenir les renseignements requis et voir s'il y a certaines opérations douteuses dont vous devriez être avisés.

Est-ce que vous conseillez ces entités quant à la manière d'assurer la confidentialité et l'intégrité des informations ainsi obtenues?

M. Barry MacKillop: Parlez-vous de ce qui se passe dans leur organisation ou dans la nôtre?

Mme Julie Dabrusin: Je veux parler de leur organisation, mais vous pouvez nous dire également ce qu'il en est de la vôtre.

M. Barry MacKillop: Nous ne les conseillons pas à proprement parler. Nous avons certaines exigences en matière de conservation des dossiers, mais il revient à chaque entité de mettre en place les mesures nécessaires à la protection des renseignements personnels.

Mme Julie Dabrusin: J'aimerais aussi savoir comment vous vous y prenez pour protéger cette information, car vous recevez un très grand nombre de déclarations financières — je crois que vous avez parlé de 25 millions.

M. Barry MacKillop: Nous excellons à ce chapitre. Nous avons des mesures de sécurité très rigoureuses, tant du point de vue technique que personnel. Nous devons également composer avec des menaces à l'interne. Tous les employés du CANAFE, du commis à la salle de courrier jusqu'au directeur, doivent détenir une attestation de sécurité de niveau très élevé qui doit être renouvelée régulièrement. Personne n'a accès à notre base de données qui est tout à fait étanche. À tous les deux ans, nous faisons l'objet d'un examen par le commissaire à la protection de la vie privée qui s'assure que nous divulguons uniquement les renseignements que nous sommes autorisés à divulguer.

Nous avons également mis en place des politiques très strictes relativement aux rapports que nous devons conserver, puis détruire après une période de 10 ans. Nous avons des politiques et des procédures extrêmement rigoureuses pour la protection des renseignements personnels, un aspect fondamental pour que le CANAFE puisse s'acquitter de son mandat.

Mme Julie Dabrusin: Comme il est question de cybersécurité, j'aimerais savoir si vous avez noté une augmentation des attaques externes ou des tentatives pour avoir accès aux renseignements compilés par le CANAFE? Est-ce un phénomène à la hausse?

M. Barry MacKillop: Non.

Mme Julie Dabrusin: Non; la situation est donc stable.

M. Barry MacKillop: Oui, et nous n'avons jamais été victimes d'une intrusion.

Mme Julie Dabrusin: C'est également une bonne chose.

Merci.

M. Barry MacKillop: Oui, je suis très fier de ce bilan.

Le président: Monsieur Eglinski, vous avez la parole pour cinq minutes.

M. Jim Eglinski (Yellowhead, PCC): Vous ne devriez jamais affirmer que vous n'avez jamais été victimes d'une intrusion; vous feriez mieux d'espérer ne jamais en subir une.

M. Barry MacKillop: J'ai dit que nous n'avions jamais été victimes d'intrusion. Je ne fais pas de projection; j'énonce un fait.

M. Jim Eglinski: J'aimerais poursuivre sur le sujet que ma collègue a abordé un peu plus tôt. Vous avez parlé de votre partenariat avec diverses organisations, comme des entités financières, les comptables et la GRC. Les banques sont censées vous signaler toute transaction inhabituelle. Vous dites recevoir 25 millions de signalements par année.

M. Barry MacKillop: Ce chiffre correspond à tous les signalements reçus, dont 19 millions concernent des transferts de fonds électroniques en partance ou à destination du Canada.

M. Jim Eglinski: Voilà qui me préoccupe. Les banques sont-elles tenues de vous aviser, comme je pense que vous l'avez dit, si des transactions inhabituelles de plus de 10 000 $ ont été effectuées? La réglementation les oblige-t-elle à avertir les autorités policières locales ou seulement à vous aviser?

M. Barry MacKillop: Non. En vertu de la loi, elles sont obligées de nous signaler ces transactions. Elles peuvent certainement adopter leur propre...

M. Jim Eglinski: Je veux seulement vous présenter un scénario, et j'utiliserai Julie, puisqu'elle s'est servie de moi.

● (1625)

Mme Julie Dabrusin: Je vous ai vu le faire.

M. Jim Eglinski: Julie est piégée par une entité étrangère qui l'oblige à lui envoyer 300 000 $. La banque vous informe de la situation et vous examinez l'affaire. Si vous pensez qu'il s'agit d'une fraude, ce qui est le cas, vous en avisez la GRC. Le criminel oeuvrant depuis l'extérieur du Canada s'expose-t-il à des répercussions et Mme Dabrusin a-t-elle la moindre chance de revoir son argent?

Pouvez-vous me parler de cas où l'argent a été récupéré?

M. Dan Lambert: Nous collaborons très étroitement avec les agences de sécurité du monde pour continuer de suivre l'argent à la trace dans des affaires semblables, comme le font d'ailleurs les organismes d'application de la loi.

Si nous n'appliquons pas la loi, alors, comme vous le dites, dans des situations où l'argent est transféré à l'étranger, est-ce que l'enquête se poursuit au chapitre de l'information? Oui.

Pour ce qui est des questions sur le retour de l'argent et les poursuites, les organismes d'application de la loi seraient mieux à même d'y répondre.

M. Jim Eglinski: Vous dites que c'est un organisme étranger qui interviendrait.

M. Dan Lambert: Eh bien, si l'affaire concerne un pays étranger, on aurait...

M. Jim Eglinski: Une fois l'argent transféré à l'extérieur du Canada, de manière réaliste, la probabilité de le ramener au pays est probablement nulle, n'est-ce pas?

M. Dan Lambert: Les organismes d'application de la loi déploient des efforts dans de telles situations.

M. Jim Eglinski: J'ai eu vent d'une situation alarmante qui s'est produite entre Noël et le jour de l'An dans une affaire identique à celle que j'ai évoquée. Un aîné de ma circonscription a été victime de fraude. Sa conjointe s'en est aperçue et a communiqué avec la GRC, qui lui a répondu qu'elle n'avait aucun moyen de récupérer l'argent et qu'elle ne pouvait s'occuper de l'enquête. Cette dame ne reverrait jamais la couleur de son argent. La GRC lui a conseillé de communiquer avec son député pour porter plainte en espérant qu'il puisse faire quelque chose. C'est donc ce que je fais en rendant cette affaire publique.

Nous devons nous attaquer à ces situations, et j'essaie seulement d'obtenir une réponse honnête. Serons-nous capables d'accomplir quelque chose avec nos divers programmes, vos programmes et le soutien des organismes sur lesquels vous comptez pour vous fournir de l'information? Les banques n'ont été d'aucune aide. Elles ont envoyé le chèque ou la traite à l'étranger, et il est presque impossible de rectifier la situation après les faits. C'est ce qui me préoccupe. Nous devons intervenir avant les faits et pouvoir nous tenir informés. Y a-t-il un moyen de nous tenir au courant des activités de ces fraudeurs étrangers et de mettre la main au collet des coupables?

M. Barry MacKillop: C'est très difficile, notamment quand il est question de ces genres de stratagèmes. Si la personne concernée, Julie, envoie l'argent volontairement, le banquier peut difficilement déterminer s'il s'agit d'une fraude si elle affirme qu'elle veut vraiment transférer les fonds.

Nous collaborons avec les banques et travaillons beaucoup avec d'autres entités de signalement pour nous assurer d'avoir des indicateurs que nous mettons au point avec elles pour qu'elles puissent poser les bonnes questions. Cependant, si Julie répond à ces questions d'une certaine manière, je ne suis pas certain qu'elle aurait la chance que la banque l'empêche de transférer l'argent si c'est vraiment ce qu'elle veut faire.

Le président: Madame Damoff, vous disposez de deux ou trois minutes.

Mme Pam Damoff (Oakville-Nord—Burlington, Lib.): Ma question concerne peut-être plus la GRC que vous, mais si une entreprise canadienne recourt aux services d'un centre d'appels ou d'une compagnie situés à l'étranger pour agir en son nom et qu'une fraude survient, quelles lois s'appliquent en l'espèce? Est-ce que ce sont les lois canadiennes? Par exemple, si la RBC utilise une entreprise indienne pour effectuer des appels et qu'une fraude ou une atteinte à la sécurité se produit, quelles lois s'appliquent. Le savez-vous?

M. Barry MacKillop: Non. Je pense que vous avez raison de dire que cette question concernerait davantage nos amis de la GRC ou peut-être les juristes du ministère de la Justice. Je n'en suis pas certain.

Mme Pam Damoff: D'accord.

Comme mon collègue, j'ai entendu parler, au cours de la période des fêtes, d'une femme de Milton qui s'est retrouvée dans une situation semblable. Elle a toutefois été délestée d'un montant bien plus substantiel, mais comme les transferts s'élevaient à moins de 10 000 $, cette arnaque sentimentale n'a pas été détectée en cours de route.

Pour donner suite à ce que Sven disait, ce seuil est-il trop élevé? Si les gens doivent envoyer 5 000, puis 7 000 $, la banque n'y voit que du feu, car les clients répondent correctement. Les banques seraient-elles alertées si le montant était plus élevé?

● (1630)

M. Barry MacKillop: S'il était plus bas, si le seuil était de 1 000 $, nous serions avisés de tous les transferts de 1 000 $ et plus à l'étranger.

Mme Pam Damoff: C'est vrai.

M. Barry MacKillop: Voilà qui nous obligerait à examiner beaucoup de transactions.

L'expérience nous a montré que nous ferions probablement mieux de faire de la formation et de la sensibilisation, et de collaborer avec les grandes banques pour établir les tendances et établir des indicateurs pour qu'elles puissent déceler les fraudes. Il importe aussi de détecter les victimes potentielles à l'aide d'indicateurs et de nous aviser de la situation. Nous pourrions alors faire appel à la police. Nous l'avons fait, transmettant le dossier aux autorités policières afin qu'elles parlent avec la victime pour l'empêcher d'envoyer continuellement de l'argent.

Je ne suis pas certain que ce soit nécessairement une question de seuil, à moins que vous ne vouliez éliminer ce seuil. Ici encore, la base de données contient de nombreuses transactions, et lorsqu'on analyse les données, il est parfois difficile de trouver le poisson quand l'océan est trop vaste.

Le président: Merci, messieurs MacKillop et Lambert. Voilà qui lance notre étude sur une note intéressante.

Sur ce, nous suspendrons la séance quelques instants pendant que les témoins de la GRC s'installent à la table.

Merci encore.

● (1630)

_____(Pause)_____

● (1634)

Le président: Chers collègues, nous reprenons la séance. Notre deuxième groupe de témoins est composé de Chris Lynam et Mark Flynn, de la GRC, qui se présenteront certainement.

Est-ce vous qui prendrez la parole en premier, monsieur Flynn? Votre rang ne figure pas dans notre liste. Cette dernière indique que vous êtes directeur général, mais...

Surintendant principal Mark Flynn (directeur général, Criminalité financière et la cybercriminalité, Opérations criminelles de la police fédérale, Gendarmerie royale du Canada):

Mon rang officiel est celui de « surintendant principal ».

● (1635)

Le président: Vous êtes surintendant principal. Le policier membre de notre comité sait ce que cela signifie, mais je ne prétends pas le savoir.

Vous avez la parole.

Surint. pr. Mark Flynn: Monsieur le président et honorables membres du Comité, bonjour et merci de m'avoir donné aujourd'hui la possibilité de faire un exposé sur la question de la cybercriminalité dans le secteur financier au Canada.

Comme le président l'a indiqué, je m'appelle Mark Flynn, surintendant principal et directeur général, Crime financier et cybercriminalité, au sein des Opérations criminelles de la Police fédérale.

Je suis accompagné aujourd'hui de mon collègue Chris Lynam, directeur général par intérim de l'Unité nationale de coordination de la lutte contre la cybercriminalité, qui fera également un bref exposé après mon allocution.

[*Français*]

Je vais commencer par décrire ce que sont la cybercriminalité et les types d'activités que réalisent les cybercriminels.

[*Traduction*]

La cybercriminalité englobe des cas de criminalité où la technologie est la principale cible, de même que la criminalité où la technologie est un important outil ou un catalyseur pour commettre d'autres types de crimes, notamment des infractions financières, comme la fraude et le blanchiment d'argent, ou encore des infractions liées aux drogues illicites et à la sécurité nationale.

La cybercriminalité est un problème mondial complexe aux multiples facettes, dont les éléments chevauchent plusieurs administrations. Elle exploite de nouvelles technologies en constante évolution et a des répercussions sur la sécurité et le bien-être économique des citoyens et des entreprises du Canada. Les entreprises et les particuliers canadiens — surtout les membres vulnérables de notre société comme les personnes âgées et les jeunes —sont la cible de cybercriminels en raison de la richesse relative de la population et de notre économie ouverte et axée sur Internet. En particulier, les cybercriminels ciblent le secteur financier directement et indirectement. Autrement dit, les systèmes des institutions financières canadiennes sont attaqués sur deux fronts, c'est-à-dire par l'entremise de l'infrastructure informatique de l'entreprise et de l'accès des clients.

Pour vous expliquer davantage la question, j'entrerai plus dans les détails. 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 malveillants et à de nouveaux cybergroupes du crime organisé de lancer des attaques à une échelle sans précédent.

La grande disponibilité d'une toute nouvelle gamme d'outils cybernétiques illicites a donné naissance à un tout nouvel environnement cybernétique, qui comprend un large éventail d'acteurs entrepreneuriaux, y compris des développeurs de logiciels malveillants, des fournisseurs et des administrateurs d'infrastructures, et des revendeurs de plateformes de données qui collaborent avec d'autres dans des réseaux mondiaux ou qui offrent de manière indépendante des services et de l'expertise à d'autres intervenants à des fins lucratives par l'entremise d'lnternet. C'est ce que nous appelons l'écosystème numérique criminel ou la cybercriminalité en tant que service.

Dans les secteurs financier et commercial du Canada, le volume et la gravité de la cybercriminalité dont les Canadiens et les entreprises sont victimes sont considérables. Les institutions et les services financiers mondiaux continuent d'être ciblés par un éventail de cyberattaques malveillantes qui génèrent des profits illicites importants pour les contrevenants qui en sont responsables.

De plus, en raison des progrès technologiques qui peuvent faciliter les crimes traditionnels comme le vol, la fraude ou le blanchiment de l'argent, les organismes d'application de la loi ont dû modifier la manière dont ils réagissent aux actes criminels financiers de grande envergure. Essentiellement, il s'agit de nouveaux cybercrimes et de vieux crimes perpétrés à l'aide de nouveaux outils.

Les groupes du crime organisé, les blanchisseurs d'argent professionnels et les contrôleurs monétaires internationaux ne sont plus limités aux méthodes traditionnelles de blanchiment d'argent et de transfert des produits de la criminalité.

● (1640)

Les marchés du Web invisible, la multiplication des monnaies virtuelles et les stratagèmes complexes de blanchiment d'argent par l'entremise d'activités commerciales sont des exemples des progrès technologiques chez les criminels qui ont réellement effacé les frontières et permis aux organisations criminelles de s'implanter véritablement partout dans le monde.

Les cybercriminels cherchent à faire des profits grâce au déploiement de logiciels malveillants, comme les chevaux de Troie bancaires, une multitude d'activités frauduleuses en ligne, la compromission de courriels ou l'extorsion, notamment grâce aux rançongiciels ou aux attaques par déni de service distribué. Tous ces crimes peuvent être perpétrés au Canada ou à l'étranger.

Ces techniques novatrices de cybercriminalité révèlent que la majorité de la cybercriminalité actuelle est motivée par un gain financier, comme c'est le cas pour bien des crimes. Les criminels cherchent à s'approprier l'argent pour en profiter.

Même si la GRC a acquis une meilleure compréhension de la portée et de l'ampleur de la menace, des défis demeurent. Par exemple, la portée mondiale des cybercriminels oblige les forces de l'ordre à se préoccuper des criminels du monde entier et pas seulement de ceux qui oeuvrent à l'intérieur du pays. Il s'agit d'une priorité internationale qui continuera de prendre de l'ampleur pour de nombreux organismes d'application de la loi.

De plus, les efforts de maintien de l'ordre dans le domaine cybernétique continuent de faire face à des défis en grande partie en raison de la nature transversale et transnationale de la cybercriminalité, laquelle, comme je l'ai indiqué, s'applique à tous les types de crimes. La nature transnationale de la cybercriminalité permet aux cybercriminels de commettre leurs crimes dans de nombreux pays, et un cybercriminel peut s'en prendre à de nombreuses personnes à grande échelle, ce qui n'est pas possible dans le monde physique.

En réaction aux menaces et aux défis auxquels nous sommes confrontés, la Stratégie de lutte contre la cybercriminalité de la GRC guide les efforts d'enquête et d'application de la loi pour réduire la menace et contribuer à atténuer la victimisation et les répercussions de la cybercriminalité au Canada. Cette approche repose sur trois piliers: le premier consiste à déterminer les menaces liées à la cybercriminalité et en établir l'ordre de priorité au moyen de la collecte et de l'analyse de renseignements, alors que le deuxième vise à contrer la cybercriminalité en menant des activités ciblées d'enquête et d'application de la loi; et le troisième a pour but de soutenir les enquêtes liées à la cybercriminalité au moyen d'habiletés, d'outils et de formation spécialisés

La Stratégie de lutte contre la cybercriminalité comprend un cadre opérationnel élaboré dans le but d'orienter les mesures prises par la GRC pour combattre la cybercriminalité à titre de service de police fédérale. Comme la cybercriminalité transcende tous les types de criminalité, le recours à des équipes d'enquête spécialisées est essentiel. Les enquêtes numériques réalisées par la police fédérale de la GRC sont principalement menées par l'Équipe d'enquête sur la cybercriminalité de la Division nationale. Toutefois, cette dernière tire parti de l'expertise d'autres équipes de soutien aux enquêtes spécialisées, comme les opérations d'infiltration et le soutien opérationnel tactique sur Internet, qui sont nécessaires pour améliorer les résultats des enquêtes.

La GRC joue un rôle crucial au chapitre de la priorité générale du gouvernement du Canada qui consiste à assurer la sécurité des Canadiens.

Je céderai maintenant la parole à mon collègue pour qu'il puisse présenter un exposé sur le nouveau centre pour la cybersécurité qui est mis en place pour assurer l'application de la loi.

Le président: Merci, surintendant Flynn.

Monsieur Lynam, vous disposez d'un peu plus d'une minute.

M. Chris Lynam (directeur général par intérim, Coordination nationale contre la cybercriminalité, Gendarmerie royale du Canada): Monsieur le président, bonjour et merci de m'offrir l'occasion de vous parler aujourd'hui.

Comme mon collègue l'a souligné, les organismes d'application de la loi font face à plusieurs défis dans leur lutte contre la cybercriminalité. Le modèle de service de police traditionnel canadien se fonde sur l'hypothèse selon laquelle le délinquant, la victime et le système de justice relèvent pour la plupart de la même administration. Cependant, comme nous le savons, la plupart des cybercrimes concernent plusieurs administrations, voire plusieurs pays, et ont des répercussions sur les victimes dans toutes les administrations traditionnelles, d'où le besoin d'avoir un mécanisme de coordination.

Il faut que les organismes d'application de la loi puissent recueillir des renseignements, peu importe l'administration, et aient un mécanisme pour coordonner les efforts d'enquête. Il est inefficace que les multiples services de police affectent des ressources d'enquête limitées à la même activité criminelle chacun de leur côté.

Ce qui est également préoccupant, c'est que la cybercriminalité soit sous-déclarée et qu'il existe une panoplie de mécanismes de signalement, ce qui sème la confusion au sein du public.

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 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.

La sous-déclaration empêche les organismes d'application de la loi d'établir des corrélations et de lutter contre la cybercriminalité sur une échelle plus grande et de façon plus coordonnée et plus ciblée. Elle empêche également les gouvernements de comprendre l'ampleur et l'étendue du problème auquel nous sommes confrontés.

● (1645)

[*Français*]

En réponse aux défis et pour renforcer la capacité du Canada à lutter contre la cybercriminalité, 116 millions de dollars sur cinq ans et 23,2 millions de dollars par année consacrés à la création de l'Unité nationale de coordination de la lutte contre la cybercriminalité ont été annoncés dans le budget de 2018.

[*Traduction*]

L'Unité sera un service de police national, supervisé par la GRC, appuyant les organismes d'application de la loi dans l'ensemble du Canada et travaillant étroitement avec eux. Elle agira à titre de carrefour de coordination des enquêtes sur les cybercrimes au Canada et unira ses efforts à des partenaires étrangers pour lutter contre la cybercriminalité.

Le président: Je crois que je dois vous arrêter là. Vous allez devoir essayer d'inclure le reste de votre exposé dans vos réponses aux questions de Mme Damoff et des autres députés.

Madame Damoff, vous disposez de sept minutes.

Mme Pam Damoff: Je vous remercie beaucoup, monsieur le président.

Un électeur a porté à mon attention certaines questions. Vous avez dit que vous allez collaborer avec d'autres pays. Un grand nombre de nos banques sous-traitent certains services à d'autres pays. Si une banque canadienne fait affaire, par exemple, avec un centre d'appels en Inde qui devient victime d'un piratage ou d'une atteinte à la protection des données, on appliquerait les lois de quel pays dans ce cas-là? Qui mènerait une enquête? Comment les Canadiens peuvent-ils avoir confiance que leurs données détenues par des compagnies canadiennes seront protégées si elles sont transmises à d'autres pays?

Surint. pr. Mark Flynn: C'est difficile de répondre, car tout dépend des détails techniques du contrat. Tout dépend de l'entité qui est propriétaire des données et du pays où se trouvent les cybercriminels lorsqu'ils commettent leurs infractions. Il n'y a pas une seule réponse pour toutes les situations.

S'il s'agit d'un contrat avec un centre d'appels et que toutes les données se trouvent dans un autre pays et que la personne qui a commis l'infraction se trouve dans un autre pays également, il ne s'agirait pas d'une infraction en vertu du Code criminel canadien. Cependant, dans bien des cas, il est difficile de même déterminer, en raison des technologies modernes utilisées pour stocker les données, dans quel pays se trouvent les données. Il existe de nombreux services infonuagiques où sont stockées des données à la fois au Canada et dans d'autres pays. Dans certaines situations, il pourrait y avoir des infractions au Code criminel. Dans d'autres situations, ce ne serait tout simplement pas le cas. Toutefois, nous travaillons avec nos partenaires étrangers lorsque l'incident concerne le Canada afin de nous assurer que ce qui est fait pour mener l'enquête et tenir les individus responsables de leurs actes n'aille pas à l'encontre des intérêts du Canada.

Mme Pam Damoff: Les lois canadiennes ou les règlements régissant ce que les institutions financières transmettent à d'autres pays, si ces données... il est possible que vous ne puissiez pas porter d'accusations contre quiconque en ce qui a trait à une atteinte à la protection des données.

Surint. pr. Mark Flynn: En ce qui concerne les lois, il ne serait pas approprié que je fasse...

Mme Pam Damoff: C'est très bien. Je vous remercie. Je vais maintenant m'adresser à votre collègue.

Je voudrais vous interroger à propos de l'Unité de coordination de la lutte contre la cybercriminalité. Pourriez-vous terminer ce que vous étiez en train de dire, particulièrement en ce qui concerne le secteur financier et son incidence sur l'économie canadienne.

M. Chris Lynam: L'un des principaux objectifs de la nouvelle Unité nationale de coordination de la lutte contre la cybercriminalité est de travailler avec le secteur financier sur quelques aspects, notamment s'assurer que l'information à propos des menaces soit communiquée. En outre, si l'institution financière est une victime ou qu'elle compte des victimes parmi ses clients, elle disposera d'un moyen facile de porter ce problème à l'attention des responsables de l'application de la loi afin que des mesures soient prises.

Jusqu'à maintenant, à de nombreux égards, les relations entre les institutions financières, les responsables de l'application de la loi et la GRC sont très bonnes. Grâce à cette nouvelle unité et à d'autres ressources dont la GRC disposera pour les enquêtes, il sera plus facile de travailler avec les institutions financières pour gérer les nouvelles menaces ou les situations où les institutions seront victimes de cybercriminalité.

● (1650)

Mme Pam Damoff: Quels sont les défis auxquels vous êtes constamment confrontés lorsque vous réagissez aux menaces?

M. Chris Lynam: Par exemple, si une institution financière signale...

Mark, voulez-vous répondre?

Surint. pr. Mark Flynn: Oui.

Le plus grand défi auquel nous sommes confrontés de nos jours est le nombre important de victimes et le fait que l'anonymat que permet Internet et dont tirent profit les cybercriminels rend beaucoup plus difficile la tâche de les retracer. Toutefois, nous surmontons ce défi grâce à notre collaboration avec les autres pays et aux relations étroites que nous entretenons avec le secteur financier. Nous utilisons les ressources dont bon nombre de grandes banques et d'autres institutions financières disposent pour protéger leurs propres réseaux lorsque nous menons nos enquêtes afin de contrer l'anonymat ou de tirer profit des erreurs qui surviennent lorsque des cybercriminels utilisent Internet pour commettre leurs crimes. Nous pouvons ainsi être plus efficaces.

Nous ne sommes plus du tout à l'époque où les policiers se contentaient de dire: « Merci pour votre déclaration. » Maintenant, nous procédons à une enquête et nous disons aux gens ce qu'ils doivent savoir. Nous travaillons en collaboration beaucoup plus qu'auparavant. En effet, dans le cadre d'une enquête à propos d'un incident important survenu récemment, nous collaborons avec des responsables de la sécurité, notamment au sein de l'institution financière, ainsi qu'avec des experts en cybersécurité, et cela s'avère très profitable.

Mme Pam Damoff: Il y a les répercussions sur le secteur bancaire, mais il y a aussi l'incidence sur l'économie lorsque des entreprises sont victimes de piratage. Il peut s'agir de petites ou de très grandes entreprises. Récemment, une chaîne hôtelière a été victime d'une atteinte à la protection de ses données. Est-ce que toutes les entreprises gèrent ces situations de la même façon? Y a-t-il des écarts sur le plan des mesures de sécurité qui sont prises pour protéger leurs systèmes?

Surint. pr. Mark Flynn: Je ne dirais pas qu'elles gèrent toutes ces situations de la même façon. Nous voyons différentes façons de réagir dans de tels cas.

Nous travaillons fort à convaincre les entreprises qu'elles peuvent avoir confiance que les autorités policières sont en mesure de faire quelque chose. En ce qui a trait à l'exemple que la députée a donné, je peux dire que ce n'est pas utile qu'on réponde à une personne qui s'adresse aux autorités policières « Nous sommes désolés, mais nous ne pouvons rien faire pour vous. »

Nous travaillons très fort pour bâtir la confiance. Cela fait en sorte que davantage de gens signalent des incidents. La sous-déclaration des cybercrimes est un problème pour nous et nous devons éliminer les préjugés associés à la victimisation lorsqu'il s'agit de cybercriminalité afin que nous puissions améliorer nos connaissances et bien gérer ces situations.

Mme Pam Damoff: Je vous remercie.

Le président: Merci, madame Damoff.

Monsieur Motz, vous disposez de sept minutes.

M. Glen Motz: Je vous remercie, monsieur le président, et je vous remercie, messieurs, pour votre présence.

Il y a environ un an, le Comité a été chargé de mener une étude sur le projet de loi C-59, un projet de loi sur la sécurité nationale. Dans le cadre de cette étude, nous avons entendu le témoignage du général à la retraite Michael Day, qui a déclaré être nullement confiant que le Canada soit prêt à réagir à des menaces émergentes comme l'utilisation de l'intelligence artificielle dans des cyberattaques et le piratage de systèmes de sécurité en l'espace de quelques secondes grâce à l'informatique quantique.

Cela étant dit, comment la GRC se prépare-t-elle à ce genre de situation et comment aide-t-elle d'autres organismes au sein de l'industrie à se préparer à faire face à ces menaces émergentes?

Surint. pr. Mark Flynn: Au sein de la GRC, nous avons pour mandat d'enquêter sur des infractions criminelles. Le Centre canadien pour la cybersécurité et d'autres organismes donnent des conseils en matière de protection des systèmes et fournissent une aide technologique.

En ce qui a trait aux enquêtes et à la sécurité publique, nous nous employons à éduquer les gens et à nous assurer qu'ils soient au courant de ce qui peut se passer et qu'ils prennent des mesures en présumant qu'il y a aura une atteinte, qu'ils fassent des efforts pour déceler les intrusions dans leurs réseaux et qu'ils déclarent ces incidents. Même si nous ne pouvons rien faire en ce qui concerne un cas en particulier, le fait de recueillir des informations au sujet de ce cas et d'obtenir des renseignements de la part d'autres victimes peut nous permettre à un moment donné de tenir responsables ceux qui ont porté atteinte à la protection des données à de multiples reprises.

● (1655)

M. Glen Motz: Je vous remercie.

Je vais poursuivre dans la même veine que ma collègue, madame Damoff. Je sais dans quelle position vous êtes en ce qui concerne l'application de la loi, mais je dois vous dire d'après mon expérience — et je suis certain que Jim est d'accord — que, si nous étions à votre place, nous dirions des choses comme « Nous aurions souhaité que le gouvernement pense à cela » ou « Nous aurions voulu que la loi tienne compte de ceci. » C'est vous qui êtes sur le terrain. Je ne veux pas vous mettre dans une mauvaise situation, alors je vais poser ma question différemment.

La présente étude concerne la protection des Canadiens. Elle vise à s'assurer que la législation en vigueur permet aux responsables de l'application de la loi d'accomplir ce travail d'une manière qui protégera mieux les Canadiens et qu'elle permet au CANAFE et aux autres organismes semblables de mieux faire leur travail à cet égard. Vous n'avez pas à être précis, mais compte tenu du rôle que vous jouez maintenant, donnez-nous une idée générale des lacunes que vous observez, de sorte que le Comité puisse se pencher sur ces lacunes pour veiller à ce que tout... Tout est une question de sécurité publique. Notre comité se penche sur la sécurité publique et votre rôle est d'assurer la sécurité publique.

Je ne veux pas vous offenser, mais parfois il est facile de simplement dire « Eh bien, je ne peux pas parler de cela », mais je pense que vous pouvez en fait parler de cela. D'après mon expérience, vous pouvez dire « Voici les lacunes que j'observe sur lesquelles peuvent se pencher les responsables de l'application de la loi, le gouvernement ou quiconque. » Je vous offre le courage de nous en faire part.

Des voix: Oh, oh!

Le président: Je ne crois pas que c'est une question de courage; c'est une question de respect du rôle que les fonctionnaires doivent jouer, mais étant donné la passion avec laquelle M. Motz a posé sa question, je suis tout à fait disposé à vous laisser répondre comme bon vous semble.

Surint. pr. Mark Flynn: D'accord, nous voulons tous les deux répondre, mais je vais laisser M. Lynam commencer.

M. Chris Lynam: Je dirais que le simple fait que le Comité se penche sur la cybersécurité et la cybercriminalité nous amène à parler de la difficulté qu'ont le Canada et d'autres pays à déterminer comment gérer ces deux enjeux. Si on s'intéresse davantage aux défis auxquels sont confrontés les responsables de l'application de la loi, à la façon d'y faire face ou à la façon dont les ministères, y compris le nouveau Centre canadien pour la cybersécurité, vont s'assurer que les Canadiens et les entreprises sachent comment mieux se protéger et ce qu'ils doivent faire lorsqu'ils sont victimes de cybercriminalité... À mon avis, il est important d'accorder une plus grande attention à ces aspects.

Surint. pr. Mark Flynn: J'ajouterai que l'attention qu'on accorde doit permettre d'éliminer, comme je l'ai dit plus tôt, les préjugés associés à la cybercriminalité, car, au cours des dernières années, en travaillant dans le domaine de la cybercriminalité, j'ai observé que de nombreuses organisations ne signalent pas les cybercrimes en raison des préjugés qui y sont associés. Lorsqu'il y a une atteinte à la protection des données que détient une grande entreprise, si celle-ci ne signale pas l'incident aux autorités policières ou à d'autres organismes auprès desquels nous pouvons obtenir l'information, nous ne pouvons rien faire. Plus nous les montrons du doigt, contrairement au cybercriminel qui a commis l'infraction, moins elles auront tendance à déclarer les incidents et moins nous serons en mesure de mener des enquêtes qui aboutiront à des résultats.

M. Glen Motz: Je vous remercie pour vos réponses. Étant donné ce que vous venez de dire, et compte tenu du fait que moins de 10 % des entreprises signalent les cybercrimes, y a-t-il lieu de proposer d'obliger le signalement des cybercrimes? Serait-il possible de dire aux entreprises, petites, moyennes ou grandes, qui sont victimes de cybercriminalité, qu'elles ont la responsabilité de signaler les incidents aux autorités, peu importe l'incidence sur leur image? Est-ce que les Canadiens pourraient s'attendre raisonnablement à ce que cela se produise?

Surint. pr. Mark Flynn: Cela pourrait poser un défi intéressant.

● (1700)

M. Glen Motz: Oui.

Surint. pr. Mark Flynn: Comme mon collègue du CANAFE l'a dit tout à l'heure, il faut qu'il y ait un équilibre en ce qui a trait au seuil à partir duquel les incidents devraient être signalés. Le système pourrait être inondé de signalements.

Nous nous concentrons beaucoup sur la confiance envers les responsables de l'application de la loi et sur le juste équilibre à atteindre en ce qui concerne le nombre de signalements. Dans le cadre de l'initiative visant la création d'une unité nationale de coordination de la lutte contre la cybercriminalité, nous allons mettre en place un mécanisme de signalement public. Si des gens s'adressent aux autorités policières pour signaler des cybercrimes et que les autorités policières ne sont pas en mesure de recevoir ces signalements et d'offrir des conseils judicieux, comme vous l'avez constaté ainsi que votre électeur, le seul fait de signaler l'incident ne contribuera pas à régler le problème. Il faut qu'il y ait un équilibre entre les signalements et la capacité de réagir, alors nous devons mettre en place les systèmes nécessaires pour recevoir les signalements et y donner suite comme il se doit.

M. Glen Motz: Je vous remercie.

Le président: Je vous remercie, monsieur Motz.

Monsieur Dubé, vous avez sept minutes.

M. Matthew Dubé: Je vous remercie, monsieur le président.

J'ai quelques questions à poser au sujet des signalements.

Je veux d'abord vous interroger sur le mécanisme de signalement qu'établira l'unité nationale. Je me demande comment ce mécanisme fonctionnera compte tenu notamment des nouvelles obligations en vertu de la LPRPDE de signaler les incidents au commissaire à la protection de la vie privée. Dans certains cas, il s'agira toujours de crimes, je présume, mais y a-t-il une différence entre certains des crimes qui pourraient vous être signalés et la nonchalance à l'égard de l'application de correctifs à des logiciels. Comment ces deux mécanismes de signalement fonctionnent-ils ensemble?

M. Chris Lynam: En réalité, ils ne fonctionnent pas ensemble. Les obligations en vertu de la LPRPDE concernent les atteintes à la protection des données et les règlements connexes tandis que le nouveau mécanisme de signalement public que nous allons mettre en place est de nature volontaire. Il s'adresse aux personnes ou principalement aux petites et moyennes entreprises qui souhaitent avoir un moyen de faire savoir aux responsables de l'application de la loi qu'elles sont victimes de cybercriminalité. La capacité de faire un signalement peut contribuer à aider les policiers à mener leurs enquêtes et à appuyer leurs efforts sur le plan du renseignement.

En ce qui concerne l'exemple qui a été donné, je dois dire que, malheureusement, il y aura toujours des cas dans lesquels l'argent ne sera pas récupéré, mais en 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 au Canada pour lutter contre la cybercriminalité. En ce moment, ce n'est pas possible de fonctionner ainsi.

M. Matthew Dubé: Si c'est de nature volontaire, il est difficile pour moi de comprendre pourquoi une entreprise, si elle a déjà l'obligation de signaler une atteinte, n'en profiterait pas pour la signaler également aux autorités policières, mais il peut exister toutes sortes de raisons pour lesquelles elle pourrait ne pas le faire.

Est-ce que votre unité examine ce qui a été signalé au commissaire à la protection de la vie privée mais qui n'a pas nécessairement été signalé aux autorités policières? C'est probablement public et le commissaire va en faire rapport. Que pouvez-vous faire ensuite?

M. Chris Lynam: Nous allons communiquer avec le commissaire à la protection de la vie privée afin de mieux comprendre comment il gère les signalements d'atteinte à la protection des données. Je le répète, il n'y a aucune obligation de divulguer l'information aux autorités policières. Il peut y avoir des renseignements qui permettent de faire de la prévention ou qui peuvent être utiles, mais nous allons de l'avant avec un mécanisme de nature volontaire qui permet au public et aux entreprises de faire directement des signalements.

Vous avez raison, certaines entreprises pourraient faire un signalement auprès du commissaire et par l'intermédiaire de notre mécanisme, et c'est ce que nous encourageons.

M. Matthew Dubé: Je présume que c'est dans le but de les rendre publics qu'on rend obligatoires les signalements au commissaire à la protection de la vie privée en vertu de la LPRPDE, car un grand nombre d'entreprises cachaient ses atteintes, qui étaient révélées finalement seulement deux ans plus tard. C'est la même chose en ce qui concerne les policiers. Si les autorités policières ne reçoivent aucune plainte ou aucun signalement, même si elles constatent les problèmes, elles ne peuvent pas nécessairement y réagir.

Est-ce que je comprends bien?

Surint. pr. Mark Flynn: Je vais répondre.

Si on entend parler d'une atteinte qui a une incidence considérable sur le Canada, nous devons faire quelque chose. Nous allons faire un suivi auprès des entreprises et les encourager à nous faire part des détails.

Le simple fait de savoir qu'il y a eu une atteinte ne nous permet pas de mener efficacement une enquête criminelle. Nous avons besoin de beaucoup plus d'informations que cela. C'est parfois difficile, mais nous travaillons avec certaines des grandes entreprises, car il n'est souvent pas facile de communiquer avec la bonne personne pour obtenir l'information dont nous avons besoin. Nous entrons en communication avec l'entreprise; nous n'avons pas besoin d'attendre qu'elle s'adresse à nous. Cependant, nous pouvons mener une enquête efficace seulement si l'entreprise est disposée à collaborer avec nous au cours des différentes étapes de l'enquête sur l'incident.

● (1705)

M. Matthew Dubé: Est-ce que l'unité dispose de capacités supplémentaires? Autrement dit, d'un point de vue technique, est-ce que l'unité dispose de capacités qui n'existaient pas au sein de la GRC lorsque celle-ci s'occupait de ce domaine? Je présume qu'il s'agit du même type de collaboration, mais sous un nom différent.

M. Chris Lynam: Oui. L'unité comptera un certain nombre de personnes qui s'emploieront à faciliter la collaboration avec les services de police et le secteur privé, et elle sera appuyée par un nouveau système de gestion de l'information et de technologie de l'information qui permettra la communication des renseignements entre les responsables de l'application de la loi aux fins de l'analyse, comme je l'ai mentionné, des signalements du public, de sorte que les capacités à l'échelon régional ou provincial en matière d'application de la loi dans les cas de cybercriminalité seront plus grandes.

M. Matthew Dubé: Pendant les 30 secondes qu'il me reste, j'aimerais parler des gens. Y a-t-il des difficultés...

Le président: Il vous reste plus que 30 secondes.

M. Matthew Dubé: D'accord. C'est bien, mais il ne me reste plus beaucoup de temps.

J'aimerais savoir, en ce qui concerne le personnel, s'il y a des défis qui se posent lorsqu'il s'agit de trouver des personnes qui possèdent un ensemble de compétences spécialisées et auxquelles on peut attribuer la cote de sécurité appropriée. Nous avons entendu parler de cet enjeu dans différents domaines liés à la cybersécurité. Est-ce un défi auquel l'unité et plus précisément la GRC doivent faire face?

M. Chris Lynam: Je dirais que lorsqu'il s'agit d'embaucher des talents dans le domaine de la sécurité, que ce soit dans le secteur public ou le secteur privé, le bassin de candidats est actuellement assez restreint. Des initiatives sont en cours pour tenter d'accroître ces bassins, afin de trouver des gens qui ont les connaissances techniques appropriées ou la capacité de raisonnement critique et analytique voulue, afin de les embaucher et de les former au niveau approprié. Cet aspect présente quelques défis.

Un grand nombre des approches que nous avons élaborées jusqu'ici tirent parti de cela. En effet, un grand nombre de Canadiens souhaitent aider les organismes d'application de la loi à appréhender les cybercriminels. Par contre, ils ont moins envie de travailler dans le secteur de la cybersécurité ou dans un autre secteur. Ils veulent aider à servir leur pays. Ils ne font peut-être pas autant d'argent que s'ils le faisaient dans le secteur privé, mais cette approche nous a permis d'obtenir un certain succès.

Le président: Merci, monsieur Dubé.

Avant de donner la parole à Mme Sahota, j'aimerais rappeler que 28 000 cybercrimes ont été signalés. Combien d'entre eux ont fait l'objet d'accusations?

M. Chris Lynam: Monsieur le président, je n'ai pas cette donnée avec moi. Nous pouvons vous la faire parvenir.

Le président: En pourcentage, serait-ce 1 %, 2 %?

Surint. pr. Mark Flynn: Le nombre d'accusations portées représente probablement une petite fraction, en pourcentage, du nombre de délits.

Le défi qui se pose lorsqu'on répond à cette question, c'est qu'il faut revenir à la définition de cybercrime, car elle englobe tous les crimes qui profitent du soutien cybernétique, qu'il s'agisse de menaces de fraude par courriel, de grands systèmes compromis, etc.

Le président: Je me fonde seulement sur la description que vous faites d'un cybercrime. Moins de 5 % et moins de 1 %? Suis-je dans la bonne fourchette?

M. Chris Lynam: En ce qui concerne le point qu'a fait valoir M. Flynn, c'est probablement un petit nombre. Si vous le souhaitez, monsieur le président, nous pourrions faire parvenir au Comité...

Le président: Vous dites essentiellement que du point de vue criminel, c'est un crime à faible risque.

M. Chris Lynam: Oui. Malheureusement, de nombreux cybercriminels mènent leurs activités en toute impunité.

Le président: D'accord.

Madame Sahota, vous avez sept minutes.

Mme Ruby Sahota (Brampton-Nord, Lib.): Merci.

Aujourd'hui, vous avez souvent parlé des lacunes potentielles que vous avez cernées. J'aimerais me concentrer sur votre exposé, plus précisément lorsque vous avez parlé des investissements dans le budget de 2018 pour la création d'une nouvelle unité nationale de coordination de la lutte contre la cybercriminalité au sein de la GRC.

Cela semble une excellente chose, et je sais qu'il faudra probablement du temps pour que cette unité soit pleinement opérationnelle. À votre avis, est-elle actuellement opérationnelle, et si ce n'est pas le cas, combien de temps faudra-t-il attendre avant qu'elle le soit? De plus, j'aimerais savoir ce qu'on faisait avant la création de cette unité.

● (1710)

M. Chris Lynam: Je commencerai à répondre, et je pourrai ensuite donner la parole à M. Flynn, qui pourra vous parler des ressources de la GRC qui sont actuellement affectées à la cybercriminalité.

La nouvelle unité atteindra sa capacité opérationnelle initiale en avril 2020 et se renforcera ensuite pendant trois ou quatre ans pour atteindre sa pleine capacité opérationnelle en 2023. C'est également l'année pendant laquelle le système de signalement public sera pleinement mis en oeuvre.

Il s'agit d'une nouvelle unité, comme vous pouvez l'imaginer, pour la GRC. Nous embauchons et nous formons de nouveaux employés et nous établissons des partenariats avec des services de police de partout au Canada, ainsi qu'avec des intervenants du secteur privé et du secteur non gouvernemental. De plus, comme je l'ai mentionné, nous mettons en oeuvre un nouveau système de GI-TI pour soutenir ses opérations.

Mme Ruby Sahota: Dans votre exposé, vous avez dit que des consultations étaient menées, et qu'il y avait un relâchement dans deux domaines et que c'était la raison pour laquelle nous sommes dans cette situation.

Que faisait-on avant la création de cette unité?

Surint. pr. Mark Flynn: Actuellement, dans la division des opérations criminelles de la police fédérale, dont je suis responsable, plusieurs efforts sont en cours pour aider à gagner la confiance et à établir des relations avec les institutions financières, les banques et les entreprises de cybersécurité privées, et pour tirer parti du Centre antifraude du Canada, du groupe de consultation du public de la police fédérale et des efforts de sensibilisation à l'égard des services de police contractuels et autochtones, afin de veiller à ce qu'une approche multidimensionnelle soit adoptée dans l'établissement de ces partenariats. Nous profitons de ce qui existe déjà au sein de l'industrie de la cybersécurité, que ce soit dans les banques ou dans les entreprises de sécurité privées, et nous établissons ces relations, afin de comprendre le problème.

Comme je l'ai mentionné plus tôt, nous serions submergés par les signalements. J'aimerais vous parler de mon premier jour de travail dans la division de la cybercriminalité au sein de la police fédérale. À l'époque, j'avais demandé qu'on me signale chaque incident et chaque attaque technologique contre les systèmes du gouvernement du Canada. Deux rapports ont suffi à submerger mon système de courrier électronique; le volume est donc trop élevé.

Nous devons collaborer pour prendre des mesures à cet égard. Nous déployons de gros efforts. J'ai très hâte que le nouveau centre soit prêt, afin que nous puissions lui transférer, de façon appropriée, certaines de ces responsabilités, afin que ses intervenants exécutent ces mesures au nom de tous les organismes d'application de la loi au Canada, car...

Mme Ruby Sahota: C'est intéressant. Vous dites que les particuliers et d'autres entreprises ne font pas suffisamment de signalements, mais vous êtes submergés par la quantité de signalements qui existent déjà ou par les incidents qui se produisent. C'est très intéressant.

Je crois que M. Dubé a abordé la question des difficultés liées à l'embauche de spécialistes en matière de cybersécurité. Vous avez parlé des initiatives qui sont en cours pour accroître le nombre d'experts dans ce domaine. Quelles sont ces initiatives? Pouvez-vous nous les décrire? Qui sont vos partenaires?

M. Chris Lynam: Je sais qu'il existe, au sein du gouvernement, une initiative qui vise à recruter et à embaucher, de façon collective, des informaticiens. Ces gens passent des entrevues. Il y a un processus de triage. Ensuite, les ministères peuvent assurer un suivi auprès de ces personnes pour vérifier si elles peuvent répondre aux besoins de l'organisation. Dans l'ensemble du gouvernement fédéral, on a mis sur pied une initiative pour attirer des informaticiens.

Mme Ruby Sahota: A-t-on établi un partenariat avec des universités dans ce domaine? Formons-nous suffisamment de gens au Canada? Y a-t-il une lacune à cet égard?

M. Chris Lynam: Je crois que, comme nous l'avons vu dans de nombreux secteurs, on tente d'augmenter le nombre d'employés du domaine de la cybersécurité dans les secteurs publics ou privés au Canada. Je sais qu'au sein de la GRC, nous avons eu plusieurs discussions à cet égard et que nous avons exploré des options en collaboration avec divers établissements d'enseignement pour créer des occasions de stage coopératif, afin de faire participer les étudiants au début de leurs études. Cela pourrait ensuite mener à un emploi à temps plein après l'obtention de leur diplôme. Nous avons également discuté avec les intervenants du secteur privé de la possibilité de faire des échanges. En effet, les intervenants du secteur privé souhaitent que leurs employés en matière de sécurité de la TI puissent travailler avec les organismes d'application de la loi et vice versa, afin d'échanger des compétences, etc.

Nous nous efforçons de mettre en oeuvre une stratégie multidimensionnelle en matière de ressources humaines qui permettra d'obtenir la participation d'universités et d'employés actuels du secteur public et privé.

Mme Ruby Sahota: Embauchez-vous des gens à l'extérieur de nos frontières pour vous aider dans ce domaine?

M. Chris Lynam: Les employés de la fonction publique sont principalement des citoyens canadiens. Je sais que dans certaines provinces et ailleurs, des initiatives permettent l'embauche d'experts en cybersécurité de l'étranger, mais ce n'est pas mon domaine d'expertise.

● (1715)

Mme Ruby Sahota: Ma dernière question a trait à la coordination avec les forces policières locales dont vous avez parlé. Vous avez parlé — ou quelqu'un en parlé précédemment — de la cybersécurité associée aux fraudes amoureuses. Il me semble que ces crimes étaient commis avant même que la cybersécurité ne soit mise en oeuvre. D'après ce que je comprends, avec ou sans la cybersécurité, les forces policières ne peuvent pas faire grand-chose pour lutter contre ces fraudes. Les gens donnent de l'argent de leur plein gré à une personne qui disparaît ensuite. Qu'allez-vous faire pour porter plus d'accusations dans ce domaine? Le président en a parlé plus tôt.

Surint. pr. Mark Flynn: Je vais aborder un point, puis je passerai la parole à Chris, parce qu'il sera responsable de certains autres volets.

À l'heure actuelle, nous avons le Centre antifraude du Canada. Je ne sais pas si vous connaissez cette organisation qui se trouve à North Bay, qui se veut un partenariat entre la DGPRO, le Bureau de la concurrence et la GRC. Le Centre fait un excellent travail pour lutter contre la fraude et comprendre le problème. Le taux de signalement est extrêmement bas: nous croyons qu'il est de 10 % ou moins... probablement moins de 5 %. Toutefois, lorsqu'on regroupe les renseignements, on peut s'en servir pour orienter nos opérations internationales en vue de traiter avec les centres d'appel des autres administrations, par exemple. On obtient des résultats concrets. Il faut comprendre le problème, recueillir les renseignements et offrir de l'aide aux victimes.

J'ai entendu certains des appels faits au Centre antifraude du Canada. Les intervenants de première ligne peuvent aider ces gens qui viennent de perdre une importante somme d'argent, ou même une petite somme... Ils sont gênés parce qu'ils ont été victimes de fraude. Les intervenants font un excellent travail et font comprendre à ces gens qu'ils ne sont pas seuls. Ils déstigmatisent leur situation et les aident à trouver des ressources pour les guider. C'est un travail très important.

Ils ont aussi un...

Le président: Je suis désolé. Nous allons devoir nous arrêter là. Notre temps est compté, malheureusement.

Monsieur Paul-Hus, vous avez la parole.

[*Français*]

M. Pierre Paul-Hus: Merci, monsieur le président.

Messieurs, il est question depuis tantôt de la mise sur pied d'un centre national, qui n'est pas encore prêt mais qui va l'être bientôt. En matière d'affaires gouvernementales, la lourdeur administrative qui affecte tous les ministères est ce qui me dérange toujours. On parle maintenant de la cybercriminalité, soit d'un monde opérationnel très rapide. Les acteurs qui interviennent là-dedans sont soit des organisations soit des individus, qui agissent à partir de chez eux. Cette forme de terrorisme financier vient d'un peu partout.

Croyez-vous que la mise sur pied du centre, qui va coûter plus de 125 millions de dollars aux Canadiens, va donner lieu à une bonne efficacité opérationnelle ou que nous allons faire face encore une fois à des structures administratives lourdes faisant en sorte que, pendant ce temps, les criminels vont continuer à sévir?

Je sais qu'il est difficile pour vous de répondre par oui ou par non, mais vous pouvez peut-être me dire que certaines choses pourraient être faites pour améliorer la situation.

[*Traduction*]

Surint. pr. Mark Flynn: Je peux répondre en premier, Chris.

Lorsque vous parlez du Centre, je suppose que vous...

[*Français*]

M. Pierre Paul-Hus: Je parle de l'Unité.

[*Traduction*]

M. Chris Lynam: Il est vrai que

[*Français*]

les menaces, en matière de cybercriminalité, évoluent tout le temps. Il est donc important que les systèmes et les structures du gouvernement et de la GRC soient flexibles et adaptés aux nouvelles menaces.

[*Traduction*]

Ce que je dirais en tant que personne responsable de mettre sur pied cette nouvelle unité, c'est que nous avons largement consulté les services policiers et le secteur privé afin de comprendre comment — surtout dans le secteur privé — les intervenants abordaient cette menace sur le plan de la cybersécurité. Ce qu'on a retenu, surtout, c'est qu'il faut toujours évoluer.

En créant cette unité, nous avons l'occasion de miser sur l'innovation et d'établir une culture d'adaptation. Nous avons réussi à obtenir le financement nécessaire pour embaucher un nombre suffisant de concepteurs de TI pour modifier le système au besoin. Si une nouvelle menace fait son apparition et que nous devons modifier les systèmes de signalement destinés à la population et aux entreprises canadiennes, alors nous pourrons le faire.

Ce sera toujours un défi de suivre le rythme de la cybercriminalité. D'un point de vue culturel, nous allons faire tout ce que nous pouvons pour éviter de créer une structure bureaucratique qui ne peut pas bouger.

● (1720)

[*Français*]

M. Pierre Paul-Hus: En septembre dernier, j'ai eu l'occasion d'aller aux États-Unis. J'ai pu voir le côté gouvernemental et le côté privé. Les Américains font face aux mêmes difficultés. La structure gouvernementale est partout la même, mais leur approche inclut le secteur privé, notamment des entreprises comme HackerOne, à qui le gouvernement américain accorde des contrats en vue d'être plus efficace.

Vous parlez beaucoup du secteur privé depuis tantôt. A-t-on déjà ciblé des entreprises canadiennes qui seront des partenaires de premier plan du gouvernement canadien en matière de cybersécurité?

M. Chris Lynam: Oui. Comme je l'ai mentionné déjà, les partenariats avec le secteur privé sont très importants pour la nouvelle Unité. Le secteur public, le secteur privé, les policiers et d'autres intervenants travailleront ensemble pour lutter contre ces menaces.

M. Pierre Paul-Hus: Depuis le début, nous sommes en mode réactif ou défensif. Les attaques se produisent et il faut alors déterminer si nos systèmes sont efficaces. Pour votre part, vous répondez présentement à des plaintes. Vous trouvez qu'il n'y en a pas suffisamment et vous aimeriez qu'il y en ait davantage de façon à pouvoir intervenir plus largement.

Selon la GRC, les structures de cybersécurité des entreprises financières canadiennes, soit les banques et tout ce qui concerne l'argent, sont-elles d'un bon niveau? On peut encore faire mieux, c'est certain, mais croyez-vous que les banques en font assez pour les citoyens?

[*Traduction*]

Le président: Vous devrez en parler dans une autre réponse. Malheureusement, le temps de M. Paul-Hus est écoulé.

[*Français*]

Je m'excuse.

[*Traduction*]

Le président: Monsieur Picard, vous avez la parole.

M. Michel Picard: Merci, messieurs.

J'aimerais qu'on se centre sur certains éléments plus restreints, puisque cette étude est très vaste: qu'est-ce qui a déclenché la création de l'unité... l'élément facilitant de la technologie, la possibilité d'établir une cible, un nouveau secteur d'activité? Qu'est-ce qui a motivé la décision de créer une unité de lutte contre le cybercrime?

M. Chris Lynam: Il y a plusieurs raisons, et vous en avez évoqué quelques-unes. En fait, d'après les statistiques dont nous disposions et nos connaissances sur la sous-déclaration, nous savions que ce type de crime faisait des victimes au Canada et que nous n'avions pas suffisamment de ressources pour gérer la situation. La population et les entreprises canadiennes l'ont dit au gouvernement. Lorsqu'il a tenu des consultations en 2016, la lutte contre la cybercriminalité et la mise en place d'un solide mécanisme de coordination faisaient partie des attentes.

De plus, par l'entremise de l'Association canadienne des chefs de police, les policiers de l'ensemble du Canada ont demandé la création d'une telle unité dans une résolution et dans une étude ciblée sur le cybercrime réalisée en 2015. C'est ce qui a mené à la création de l'unité et à l'ajout de nouvelles ressources par la GRC pour accroître sa capacité d'exécution.

M. Michel Picard: Merci.

Si l'on regarde les cas de fraude dans le passé... Norbourg pour 135 millions de dollars et Norshield pour 400 millions de dollars. Dans le secteur des cartes de crédit, on signale près de 1 milliard de dollars de fraude chaque année. Les chiffres sont élevés, mais ils visent principalement les entreprises.

Est-ce qu'on doit s'attaquer aux crimes — le piratage ou la fraude — qui placent les entreprises à responsabilité limitée en situation de risque ou est-ce qu'on doit maintenant songer à l'incidence de la fraude sur l'ensemble du secteur d'activité? Disons qu'une personne attaque le marché boursier et qu'il y a déni de service; que le marché boursier ferme pendant une semaine. Imaginez l'incidence que cela pourrait avoir sur notre économie. Ce pourrait être un enjeu de sécurité nationale.

Où en sommes-nous aujourd'hui par rapport à cette menace?

● (1725)

Surint. pr. Mark Flynn: Ma plus grande crainte, c'est la menace générale relative aux petites compromissions qui se passent ou au nombre de petites compromissions qui sont utilisées pour recueillir des renseignements qui servent à attaquer les banques et d'autres fournisseurs de services en ligne.

Lorsqu'on additionne toutes ces petites infractions, les chiffres sont assez importants. Lorsqu'on parle de fraude de façon générale... on n'a qu'à regarder le cas des aînés en 2017: ce sont 22 millions de dollars de pertes déclarées, sur le petit nombre de signalements qui sont faits. C'est un nombre considérable. Il faut comprendre que cela a une grande incidence dans la vie de toutes ces personnes.

C'est en regroupant ces renseignements pour mieux les comprendre et en recueillant des renseignements techniques à des fins d'enquête que nous allons pouvoir aider les Canadiens. De plus, il est important d'aller au-delà de la simple sécurité, et de penser aux grandes sociétés et à l'argent qu'elles investissent dans la cybersécurité. Les plateformes d'attaque dans le monde et le nombre de criminels qui peuvent utiliser l'Internet pour causer des préjudices devraient tous nous préoccuper.

Bien sûr, nous ne sommes pas du côté de la défense; nous sommes responsables des enquêtes. Il faut atteindre un équilibre entre les deux pour mieux protéger les Canadiens sur le plan de la sécurité et poursuivre les responsables. Lorsqu'on se limite à la sécurité, les criminels peuvent continuer de commettre des crimes sans en subir les conséquences. Nous devons enquêter de manière efficace.

C'est la même chose que pour les vols de banque. On ne se contenterait pas de sécuriser davantage les banques en laissant les voleurs libres dans la rue. Il faut que quelqu'un les poursuive et il faut le faire de manière collaborative.

M. Michel Picard: Il me reste 30 secondes.

Vous n'avez pas pour mandat de récupérer l'argent, mais bien d'enquêter sur le plan criminel. Est-ce que le défi consiste à éviter que la fraude ne soit commise? Si vous récupérez l'argent, il est remis au Trésor et non aux victimes.

Surint. pr. Mark Flynn: C'est exact. Nous tentons toujours de réduire le nombre de victimes. En fait, la GRC a amorcé un changement en ce sens lors de nos conversations sur l'application de la loi internationale. Habituellement, dans le cadre des enquêtes, nous laissons un crime se produire afin de ne pas compromettre une enquête. Nous allons changer les choses. Nous communiquons directement avec les institutions financières, par exemple, lorsque nous enquêtons, pour lui transmettre tous les renseignements possibles.

Même si cela risque de nuire à notre capacité de mener l'enquête, nous jugeons qu'il est plus important de réduire le nombre de crimes et le nombre de pertes le plus tôt possible. Nous collaborons avec les institutions pour assurer la viabilité des poursuites également.

M. Michel Picard: Merci.

Le président: Merci.

Si le cybercrime est sans risque pour les criminels, et qu'il est commis par l'entremise d'un réseau 3G ou 4G, de quelle façon vous préparez-vous à intervenir lorsque les réseaux 5G feront leur apparition? C'est inévitable.

Pouvez-vous répondre en moins de 30 secondes?

Surint. pr. Mark Flynn: Pour nous, la différence entre un réseau 3G, 4G ou 5G pour le cybercrime qui me préoccupe le plus, c'est la rapidité avec laquelle l'infraction peut être commise et le lieu de l'infraction. Il y a aussi des éléments technologiques. Nous nous préoccupons de l'anonymisation que cela permettra.

Le président: C'est donc la vitesse et l'anonymisation, et nous n'arrivons pas à arrêter ces gens à l'heure actuelle.

Surint. pr. Mark Flynn: Je ne voudrais pas que vous pensiez qu'il n'y a aucune conséquence. Nous sommes de plus en plus efficaces. Vous avez vu les communiqués publiés par l'équipe de cyberenquête de notre division nationale; vous savez que certaines de ses opérations ont été un succès. Je crois qu'on publiera d'autres articles bientôt sur certaines grandes réussites émanant des diverses collaborations.

Le président: Nous avons hâte d'entendre ces bonnes nouvelles.

Au nom du Comité, je vous remercie de votre présence et de votre contribution à cette étude.

Chers collègues, nous avons deux motions de régie interne.

Vous avez devant vous le budget associé à cette étude. Je suppose que vous le jugez acceptable. Est-ce que quelqu'un veut faire la proposition?

M. Dubé s'en charge.

Ensuite, je propose de fixer l'échéance pour la présentation des mémoires sur cette étude au 20 février.

Sur ce, la séance est levée.