SENATE SÉNAT

CANADA

First Session
Forty-second Parliament, 2015-16-17

Proceedings of the Standing Senate Committee on

BANKING, TRADE AND COMMERCE

Chair:
The Honourable DAVID TKACHUK

Wednesday, October 18, 2017
Thursday, October 19, 2017

Issue No. 26

First and second meetings:

Study and report on issues and concerns pertaining to cyber security and cyber fraud

WITNESSES:
(*See back cover*)

Première session de la
quarante-deuxième législature, 2015-2016-2017

Délibérations du Comité sénatorial permanent des

BANQUES ET DU COMMERCE

Président :
L'honorable DAVID TKACHUK

Le mercredi 18 octobre 2017
Le jeudi 19 octobre 2017

Fascicule nº 26

Première et deuxième réunions :

Étudier, pour en faire rapport, les questions et préoccupations relatives à la cybersécurité et à la cyberfraude

TÉMOINS :
(*Voir à l'endos*)

53550-53560

STANDING SENATE COMMITTEE ON
BANKING, TRADE AND COMMERCE

The Honourable David Tkachuk, *Chair*

The Honourable Joseph A. Day, *Deputy Chair*

and

The Honourable Senators:

Black
Campbell
Carignan, P.C.
Enverga
* Harder, P.C.
(or Bellemare)
Maltais
Massicotte
Moncion
Ringuette
* Smith
(or Martin)
Tannas
Unger
Wallin
Wetston

*Ex officio members

(Quorum 4)

COMITÉ SÉNATORIAL PERMANENT
DES BANQUES ET DU COMMERCE

Président : L'honorable David Tkachuk

Vice-président : L'honorable Joseph A. Day

et

Les honorables sénateurs :

Black
Campbell
Carignan, C.P.
Enverga
* Harder, C.P.
(ou Bellemare)
Maltais
Massicotte
Moncion
Ringuette
* Smith
(ou Martin)
Tannas
Unger
Wallin
Wetston

* Membres d'office

(Quorum 4)

Published by the Senate of Canada
Available on the Internet: http://www.parl.gc.ca

Publié par le Sénat du Canada
Disponible sur internet : http://www.parl.gc.ca

ORDER OF REFERENCE

Extract from the *Journals of the Senate*, Tuesday, October 17, 2017:

The Honourable Senator Day moved, seconded by the Honourable Senator Eggleton, P.C.:

> That the Standing Senate Committee on Banking, Trade and Commerce be authorized to study and report on issues and concerns pertaining to cyber security and cyber fraud, including:
>
> - cyber threats to Canada's financial and commercial sectors;
> - identity theft, privacy breach and other fraudulent activities targeting Canadian consumers and small businesses;
> - the current state of cyber security technologies; and
> - cyber security measures and regulations in Canada and abroad.

That the committee submit its final report no later than Friday, June 29, 2018, and that the committee retain all powers necessary to publicize its findings until 180 days after the tabling of the final report.

The question being put on the motion, it was adopted.

ORDRE DE RENVOI

Extrait des *Journaux du Sénat* du mardi 17 octobre 2017 :

L'honorable sénateur Day propose, appuyé par l'honorable sénateur Eggleton, C.P.,

> Que le Comité sénatorial permanent des banques et du commerce soit autorisé à étudier, pour en faire rapport, les questions et préoccupations relatives à la cybersécurité et à la cyberfraude, y compris :
>
> - les cybermenaces pesant sur le secteur financier et commercial au Canada;
> - le vol d'identité, l'atteinte à la vie privée et les autres activités frauduleuses ciblant les consommateurs canadiens et les petites entreprises;
> - l'état actuel des technologies de cybersécurité;
> - les mesures et les règlements liés à la cybersécurité au Canada et à l'étranger.

Que le comité présente son rapport final au plus tard le vendredi 29 juin 2018 et qu'il conserve tous les pouvoirs nécessaires pour diffuser ses conclusions dans les 180 jours suivant le dépôt du rapport final.

La motion, mise aux voix, est adoptée.

La greffière du Sénat

Nicole Proulx

Clerk of the Senate

MINUTES OF PROCEEDINGS

OTTAWA, Wednesday, October 18, 2017
(72)

[*Translation*]

The Standing Senate Committee on Banking, Trade and Commerce met this day at 4:18 p.m., in room 9, Victoria Building, the deputy chair, the Honourable Joseph A. Day, presiding.

Members of the committee present: The Honourable Senators Black, Campbell, Carignan, P.C., Day, Enverga, Maltais, Massicotte, Moncion, Ringuette, Tannas, Unger, Wallin and Wetston (13).

In attendance: Adriane Yong, Analyst, Parliamentary Information and Research Services, Library of Parliament.

Also present: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Tuesday, October 17, 2017, the committee began its study on issues and concerns pertaining to cyber security and cyber fraud.

WITNESSES:

Public Safety Canada:

Adam Hatfield, Acting Director General, National Cyber Security Directorate.

Royal Canadian Mounted Police:

Chief Superintendent Scott Doran, Director General, Federal Policing Criminal Operations;

Superintendent Mark Flynn, Director, Cybercrime, Federal Policing.

Canadian Security Intelligence Service:

Charles Lowson, Director General, Counter Intelligence and Counter Proliferation.

The chair made a statement.

Mr. Hatfield, Mr. Doran and Mr. Lowson each made a statement and, together with Mr. Flynn, answered questions.

At 6:06 p.m., the committee adjourned to the call of the chair.

ATTEST:

PROCÈS-VERBAL

OTTAWA, le mercredi 18 octobre 2017
(72)

[*Français*]

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 16 h 18, dans la pièce 9 de l'Édifice Victoria sous la présidence de l'honorable Joseph A. Day (vice-président).

Membres du comité présents : Les honorables sénateurs Black, Campbell, Carignan, C.P., Day, Enverga, Maltais, Massicotte, Moncion, Ringuette, Tannas, Unger, Wallin et Wetston (13).

Également présente : Adriane Yong, analyste, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 17 octobre 2017, le comité entreprend son étude sur les questions et préoccupations relatives à la cybersécurité et à la cyberfraude.

TÉMOINS :

Sécurité publique Canada :

Adam Hatfield, directeur général par intérim, Direction de la cybersécurité nationale.

Gendarmerie royale du Canada :

Surintendant principal Scott Doran, directeur général, Opérations criminelles de la Police fédérale;

Surintendant Mark Flynn, directeur, Cybercriminalité, Police fédérale.

Service canadien du renseignement de sécurité :

Charles Lowson, directeur général, Contre-espionnage et Lutte contre la prolifération.

Le président fait une déclaration.

MM. Hatfield, Doran et Lowson font chacun une déclaration et, avec M. Flynn, répondent aux questions.

À 18 h 6, la séance est levée jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

OTTAWA, Thursday, October 19, 2017
(73)

[*Translation*]

The Standing Senate Committee on Banking, Trade and Commerce met this day at 10:33 a.m., in room 9, Victoria Building, the deputy chair, the Honourable Joseph A. Day, presiding.

Members of the committee present: The Honourable Senators Black, Campbell, Carignan, P.C., Day, Enverga, Maltais, Massicotte, Tannas, Unger, Wallin and Wetston (11).

In attendance: Adriane Yong, Analyst, Parliamentary Information and Research Services, Library of Parliament.

Also present: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Tuesday, October 17, 2017, the committee continued its study on issues and concerns pertaining to cyber security and cyber fraud.

WITNESSES:

Smart Cybersecurity Network (SERENE-RISC):

Benoît Dupont, Scientific Director (by video conference).

Communications Security Establishment:

Scott Jones, Deputy Chief, IT Security;

André Boucher, Director General, Cyber Security Partnerships.

The chair made a statement.

Mr. Dupont made a statement and answered questions.

At 11:27 a.m., the committee suspended.

At 11:30 a.m., the committee resumed.

The chair made a statement.

Mr. Jones made a statement and, together with Mr. Boucher, answered questions.

At 12:25 p.m., the committee adjourned to the call of the chair.

ATTEST:

OTTAWA, le jeudi 19 octobre 2017
(73)

[*Français*]

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 10 h 33, dans la pièce 9 de l'Édifice Victoria sous la présidence de l'honorable Joseph A. Day (vice-président).

Membres du comité présents : Les honorables sénateurs Black, Campbell, Carignan, C.P., Day, Enverga, Maltais, Massicotte, Tannas, Unger, Wallin et Wetston (11).

Également présente : Adriane Yong, analyste, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 17 octobre 2017, le comité poursuit son étude sur les questions et préoccupations relatives à la cybersécurité et à la cyberfraude.

TÉMOINS :

Réseau intégré sur la cybersécurité (SERENE-RISC) :

Benoît Dupont, directeur scientifique (par vidéoconférence).

Centre de la sécurité des télécommunications :

Scott Jones, chef adjoint, Sécurité des TI;

André Boucher, directeur général, Partenariats en cybersécurité.

Le président fait une déclaration.

M. Dupont fait une déclaration et répond et répond aux questions.

À 11 h 27, la séance est suspendue.

À 11 h 30, la séance reprend.

Le président fait une déclaration.

M. Jones fait une déclaration et, avec M. Boucher, répond aux questions.

À 12 h 25, la séance est levée jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

La greffière du comité,

Lynn Gordon

Clerk of the Committee

EVIDENCE

OTTAWA, Wednesday, October 18, 2017

The Standing Senate Committee on Banking, Trade and Commerce met this day at 4:18 p.m. to study and report on issues and concerns pertaining to cyber security and cyber fraud.

Senator Joseph A. Day (*Deputy Chair*) in the chair.

[*Translation*]

The Deputy Chair: Honourable Senators, good afternoon and welcome. Dear colleagues, guests and members of the general public who are following today's proceedings of the Standing Senate Committee on Banking, Trade and Commerce, either here in the room or listening via the Web, my name is Joseph Day. I am the deputy chair of this committee. I am replacing the chair, David Tkachuk, who is not available today.

[*English*]

Today is our first meeting on our study on the issues concerning and pertaining to cybersecurity and cyber fraud. The order of reference was approved by the Senate Chamber, and we're proceeding on it.

I'm very pleased that we have a panel this evening to help us get this study under way.

Let me introduce the panel to you, colleagues, and those watching from elsewhere. From Public Safety Canada, Adam Hatfield, Acting Director General, National Cyber Security Directorate.

From the Royal Canadian Mounted Police, Chief Superintendent Scott Doran, Director General, Federal Policing Criminal Operations; and Superintendent Mark Flynn, Director, Cybercrime, Federal Policing, both from the RCMP. From the Canadian Security Intelligence Service, Charles Lowson, Director General, Counter Intelligence and Counter Proliferation.

Charles Lowson, Director General, Counter Intelligence and Counter Proliferation, Canadian Security Intelligence Service: That's correct.

The Deputy Chair: We are going to call on each of you to make your presentation and then we will go into a question and answer dialogue.

Adam Hatfield, Acting Director General, National Cyber Security Directorate, Public Safety Canada: Thank you for inviting Public Safety Canada to speak to today about cybersecurity as it pertains to Canada's financial and commercial

TÉMOIGNAGES

OTTAWA, le mercredi 18 octobre 2017

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 16 h 18, pour étudier, afin d'en faire rapport, les questions et préoccupations relatives à la cybersécurité et à la cyberfraude.

Le sénateur Joseph A. Day (*vice-président*) occupe le fauteuil.

[*Français*]

Le vice-président : Honorables sénateurs, bonjour et bienvenue. Chers collègues, invités et membres du grand public qui assistent à la réunion aujourd'hui du Comité sénatorial permanent des banques et du commerce, soit ici dans la salle ou sur le Web, je m'appelle Joseph Day. Je suis le vice-président de ce comité. Je remplace le président David Tkachuk, qui n'est pas disponible aujourd'hui.

[*Traduction*]

C'est la première séance que nous consacrons à notre étude sur les questions et préoccupations relatives à la cybersécurité et à la cyberfraude. Nous donnons ainsi suite à l'ordre de renvoi approuvé par le Sénat.

Je suis très heureux que nous puissions accueillir ce soir des témoins qui vont nous aider à entreprendre cette étude sur le bon pied.

Je vais maintenant vous les présenter, chers collègues, en même temps qu'à ceux qui suivent nos délibérations. De Sécurité publique Canada, nous accueillons Adam Hatfield, directeur général par intérim, Direction de la cybersécurité nationale.

Nous recevons aussi deux représentants de la Gendarmerie royale du Canada, soit le surintendant principal Scott Doran, directeur général, Opérations criminelles de la Police fédérale; et le surintendant Mark Flynn, directeur, Cybercriminalité, Police fédérale. Est également des nôtres Charles Lowson, directeur général, Contre-espionnage et Lutte contre la prolifération au Service canadien du renseignement de sécurité.

Charles Lowson, directeur général, Contre-espionnage et Lutte contre la prolifération, Service canadien du renseignement : C'est bien cela.

Le vice-président : Nous allons maintenant inviter chacun de nos témoins à nous présenter un exposé, après quoi il y aura un échange de questions et réponses.

Adam Hatfield, directeur général par intérim, Direction de la cybersécurité nationale, Sécurité publique Canada : Merci d'avoir invité Sécurité publique Canada à témoigner devant vous au sujet de la cybersécurité et de son impact sur les secteurs

sectors. As we all know, Canadians are living in a digital age. There is no aspect of our lives that has not been touched by digital technology on the Internet. The rate of change we are seeing is continuing unabated.

Digital technology presents tremendous benefits and opportunities for Canadians and for Canadian businesses, but like any technology it comes with its share of dangers and risks. Cybersecurity is the enabler that lets us leverage digital technology to the fullest while mitigating those risks and dangers. For that reason, cybersecurity is a government and a national priority and it has been for many years.

Today I would like first to speak about public safety's role as it pertains to cybersecurity and speak to our interactions with the financial sector. I will speak to Public Safety Canada's role on the issue of standard and regulations.

As part of its overall mission to build a safe Canada, Public Safety Canada contributes to the security and resilience of the cyber systems that underpin Canada's national security, public safety and economic prosperity. It does this by providing national leadership and coordination in the area of cybersecurity under the authorities of the Department of Public Safety and Emergency Preparedness Act and the Emergency Management Act.

Within Public Safety's national cybersecurity directorate, there are both strategic policy and operational functions which fulfill the department's mandate. The strategic policy function is responsible for the implementation of Canada's cybersecurity strategy which promotes a coordinated whole-of-government approach to the cybersecurity issue. It is also responsible for the development of national-level policies on cybersecurity and the overall coordination of cybersecurity matters across the federal government.

This policy team, in collaboration with many departments and agencies across the federal government, is also currently developing proposals for the government in response to the cyber review, a public consultation and extensive effort that we are going through now to help guide Canada's way forward for cybersecurity.

Public Safety's operational functions are housed within the Canadian Cyber Incident Response Centre, which serves as a single point of contact for the owners and operators of critical infrastructure to report cyber incidents to the Government of Canada and also to request assistance.

financier et commercial du Canada. Nous le savons tous, les Canadiens vivent dans une ère numérique. Toutes les sphères de notre vie sont influencées par la technologie numérique et Internet, et la technologie ne cesse d'évoluer.

La technologie numérique offre d'énormes avantages et possibilités pour les Canadiens et les entreprises canadiennes. Cependant, comme toute technologie, elle présente son lot de risques et de dangers. La cybersécurité est l'outil qui nous permet de tirer pleinement profit des avantages de l'ère numérique tout en atténuant les risques qui y sont associés. C'est pourquoi la cybersécurité est une priorité à la fois gouvernementale et d'intérêt national depuis de nombreuses années déjà.

Aujourd'hui, je veux d'abord vous entretenir du rôle joué par Sécurité publique Canada en matière de cybersécurité, puis vous parler de la façon dont nous interagissons avec le secteur financier. Je discuterai enfin des normes et de la réglementation qui relèvent du mandat de Sécurité publique Canada.

Dans le contexte de son mandat global qui vise à bâtir un Canada sécuritaire, notre organisation assure la sécurité et la résilience des systèmes cybernétiques vitaux pour la sécurité nationale, la sécurité publique et la prospérité économique du pays. Pour ce faire, Sécurité publique Canada assume un rôle de leadership et de coordination à l'échelle nationale en matière de cybersécurité en vertu de la Loi sur le ministère de la Sécurité publique et de la Protection civile et de la Loi sur la gestion des urgences.

La Direction de la cybersécurité nationale de Sécurité publique Canada appuie le mandat du ministère en contribuant au développement de politiques stratégiques et par le biais de ses activités opérationnelles. La division des politiques stratégiques est responsable de la mise en œuvre de la Stratégie de cybersécurité du Canada qui favorise l'adoption d'une approche pangouvernementale intégrée pour donner suite aux enjeux en matière de cybersécurité. Cela comprend aussi l'élaboration de politiques nationales en matière de cybersécurité ainsi que la coordination des politiques de cybersécurité dans l'ensemble du gouvernement fédéral.

En collaboration avec de nombreux ministères et agences du gouvernement fédéral qui jouent un rôle en matière de cybersécurité, l'équipe en charge des politiques élabore actuellement des propositions qui permettront au gouvernement de réagir aux conclusions de l'examen sur la cybersécurité, un vaste exercice de consultation publique qui devrait contribuer à guider l'évolution de notre stratégie en matière de cybersécurité.

Les activités opérationnelles de Sécurité publique Canda relèvent du Centre canadien de réponse aux incidents cybernétiques qui sert de point de contact central pour les propriétaires et les exploitants d'infrastructures essentielles qui veulent signaler au gouvernement du Canada qu'ils ont été victimes d'un cyberincident et qui souhaitent obtenir de l'aide.

This operational team also has a mandate to coordinate whole of government response to any significant national cyber incident. In all of this work, Public Safety Canada works closely with numerous departments and agencies, all of whom have a role to play in cybersecurity. We work closely with the Royal Canadian Mounted Police and the Canadian Security Intelligence Service who are here today. We also work closely with the communications security establishment, Treasury Board of Canada Secretariat, Shared Services Canada, Innovation and Science Economic Development Canada, Global Affairs Canada and numerous others who are leaders in their respective sectors.

One of industry sectors that Public Safety Canada collaborates with is the financial sector. We have very well-established, trusted and mutually beneficial relationships with financial institutions and associations across Canada dealing with both strategic policy considerations and operational considerations. At the policy level, there have been numerous interactions between Public Safety and the financial sector over many years where the financial community has contributed expertise and also their industry perspective to the development of policies and the priorities that Canada should be facing.

At the level of day-to-day technical operations, a number of Canadian financial institutions are close partners with Public Safety Canada and do share technical information on an ongoing basis. In our experience, the Canadian financial sector has a sophisticated, mature and very well-developed understanding of both the benefits and risks of digital technology. Those risks can range from a simple effort to crack one account holder's account and obtain funds, to an attempt to falsely wire transfer block funds en masse to attempts to compromise financial networks writ large.

Cybersecurity is fundamentally an exercise in business risk management. Financial institutions have an acute understanding of risk management and in our experience are highly motivated and resourced to protect their businesses and the funds of their clients.

With respect to the issue of standards and regulations, Public Safety Canada is not a regulatory or enforcement body in the area of cybersecurity. There is currently no obligation for any individual or any organization to report a cybersecurity incident to Public Safety Canada. Further, Public Safety does not have the ability to compel any individual or organization to report an incident to us, nor does it have the ability to compel anyone to take an action on their network in response to a cyber incident.

Cette équipe opérationnelle a également pour mandat de coordonner les interventions pangouvernementales en cas d'incident cybernétique grave. Dans le cadre de toutes ces activités, Sécurité publique Canada travaille en étroite collaboration avec un grand nombre de ministères et d'agences qui ont un rôle à jouer en matière de cybersécurité. Il s'agit notamment de la Gendarmerie royale du Canada et du Service canadien du renseignement de sécurité dont les représentants sont ici aujourd'hui. Nous travaillons également avec le Centre de la sécurité des télécommunications, le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada, Innovation, Sciences et Développement économique Canada, Affaires mondiales Canada et différentes autres organisations qui sont des chefs de file dans leurs domaines respectifs.

Le secteur financier est l'un de ceux avec lesquels Sécurité publique Canada collabore. Nous avons pu établir au bénéfice des deux parties une solide relation de confiance avec les organisations et les associations du secteur financier qui doivent composer avec des enjeux liés à la cybersécurité autant dans leurs politiques stratégiques que dans leurs activités courantes. Sur le plan stratégique, le secteur financier canadien a, à de nombreuses reprises au fil des ans, contribué à l'élaboration de politiques de cybersécurité et à l'établissement de priorités en la matière en nous faisant profiter de son expertise et de ses points de vue particuliers.

Pour ce qui est des activités courantes, différentes institutions financières canadiennes travaillent en étroite collaboration avec Sécurité publique Canada et nous communiquent régulièrement de l'information de nature technique. Selon notre expérience, le secteur financier canadien a une compréhension approfondie et détaillée des avantages et des risques associés à la technologie numérique. La gamme de ces risques peut aller de simples tentatives d'accéder illégalement au compte personnel d'un client pour y voler des fonds jusqu'à des stratagèmes de fraude à l'égard d'importants transferts de fonds pour compromettre l'intégrité des réseaux financiers.

La cybersécurité se résume fondamentalement à la gestion des risques opérationnels. Selon notre expérience, les institutions financières ont une très bonne compréhension de la gestion des risques, sont très motivées à protéger leur industrie et les fonds de leurs clients, et disposent d'amplement de ressources à cette fin.

En ce qui a trait aux normes et à la réglementation, il est important de savoir que Sécurité publique Canada n'est ni une instance réglementaire ni un organisme d'application de la loi dans le domaine de la cybersécurité. Il n'existe actuellement aucune obligation pour une personne ou une organisation de signaler un incident cybernétique à Sécurité publique Canada. En outre, le ministère n'a pas l'autorité d'exiger qu'une personne ou une organisation lui rapporte un incident. Nous ne pouvons pas non plus obliger qui que ce soit à prendre des mesures

Partners work with us on a voluntary, collaborative basis and we have found that approach is both productive and mutually beneficial over many years of experience.

With some exceptions, cybersecurity is generally not a regulated area in Canada or elsewhere in the world. Those exceptions include the protection of personal information such as might fall under the remit of the Office of the Privacy Commissioner or specific industry regulations as you might find in a regulated industry sector like the health, energy or financial sectors.

Some countries have adopted strategic approaches which place requirements on companies to adhere to specific cybersecurity standards and regulations. Some countries have attempted to mandate information sharing with regard to cybersecurity incidents. Other countries, the bulk, have adopted a voluntary and collaborative approach as we do in Canada.

One of the themes that emerged from the cyber review conducted over the last two years was a call for increased government leadership with respect to standards and regulations. Government is currently working to develop proposals to respond to that review.

In closing, I would emphasize that cyber-threats are constantly evolving and that Canada and Canadians need to work to stay ahead of those threats so we can continue to benefit from digital technology. As a cybersecurity agency, we would stress that digital technology is a wonderful thing, and we should use it, but we should use it safely. That is true for all sectors of our economy, not just the financial sector.

Public Safety enjoys good relationship and frequent interactions with financial institutions across Canada, and we look forward to continuing that collaboration with them as we go forward in dealing with cybersecurity issues.

Thank you for your time.

[*Translation*]

Chief Superintendent Scott Doran, Director General, Federal Policing Criminal Operations, Royal Canadian Mounted Police: Mr. Chair, thank you for the opportunity to speak with you on the issue of cybercrime in Canada.

particulières pour protéger son réseau à la suite d'un incident cybernétique.

Nos partenaires collaborent avec nous de façon volontaire et de nombreuses années d'expérience nous ont permis de constater qu'il s'agit d'une approche productive et mutuellement avantageuse.

À quelques exceptions près, la cybersécurité n'est pas un domaine vraiment réglementé au Canada et à l'étranger. Ces exceptions comprennent la protection des renseignements personnels, via des organisations comme le Commissariat à la protection de la vie privée du Canada, ainsi que d'autres réglementations applicables à des secteurs précis comme la santé, l'énergie ou l'industrie financière.

Certains pays ont adopté des approches stratégiques obligeant les entreprises à se conformer à des normes et à une réglementation détaillées en matière de cybersécurité. D'autres ont essayé de rendre obligatoire la communication de renseignements en cas d'incident cybernétique. La plupart ont opté pour une approche de collaboration volontaire, comme c'est le cas au Canada.

L'examen de la cybersécurité mené au fil des deux dernières années a notamment permis de constater le besoin de renforcer le leadership du gouvernement concernant les normes et la réglementation en matière de cybersécurité. Le gouvernement élabore actuellement différentes propositions en réponse à cet examen.

En conclusion, je tiens à souligner le fait que les cybermenaces sont en constante évolution, et que le Canada et les Canadiens doivent s'efforcer de garder une longueur d'avance sur ces menaces de telle sorte que nous puissions continuer à tirer profit de la technologie numérique. En tant qu'organisation s'occupant de cybersécurité, nous voulons dire à tout le monde que la technologie numérique est un outil merveilleux dont on ne devrait pas se passer, mais qu'il faut l'utiliser de façon sécuritaire. Ceci est vrai pour tous les secteurs de notre économie, et pas seulement pour le secteur financier.

Sécurité publique Canada entretient de bonnes relations avec les institutions financières de tout le pays avec lesquelles nous interagissons fréquemment. Nous espérons bien poursuivre cette collaboration dans les dossiers liés à la cybersécurité.

Je vous remercie du temps que vous m'avez consacré.

[*Français*]

Surintendant principal Scott Doran, directeur général, Opérations criminelles de la Police fédérale, Gendarmerie royale du Canada : Je vous remercie, monsieur le président, de m'avoir donné l'occasion de vous parler aujourd'hui de la question de la cybercriminalité au Canada.

[*English*]

Today I will provide a brief overview of the RCMP's mandate, rules, responsibilities and law enforcement initiatives with respect to addressing cybercrime in Canada and the financial sector.

Cybercrime captures crimes where technology is the primary target and where technology is a significant enabler or instrument for other types of criminality; whether it is financial crime, including fraud and money laundering, illicit drugs or national security offences.

The RCMP plays a central role in the Government of Canada's overarching priority to provide for the safety and security of Canadians, and as such, has the federal mandate and authority to investigate criminal offences related to cybercrime.

The investigations of cybercrime involve those targeting government systems, networks and other critical infrastructure sectors. Our criminal investigations could result in the apprehension of criminals or the disruption of their cybercrime activity.

Policing efforts in the cyber realm are facing unprecedented challenges. This is largely due to the crosscutting nature of cybercrime. It applies to all types of crime, all levels of policing and it is borderless. The borderless nature makes it possible for cybercriminals to commit their crimes across multiple jurisdictions.

In addition, due to the scalable nature of cybercrime, one cybercriminal can victimize numerous individuals on a massive scale in a way that is not possible in the physical world.

Hence, cybercrime is a global problem that significantly impacts the safety and economic well-being of Canadians and Canadian businesses, particularly vulnerable members of our society such as the elderly and young people. Canadian businesses and individuals are a key target for cybercriminals because of our relative wealth and Internet-dependent economy.

Recognizing the threats and challenges being faced, in December 2015, the RCMP published its Cybercrime Strategy. The vision is to reduce the threat, victimization and impact of cybercrime in Canada and is built on three pillars: First, identifying and prioritizing cybercrime threats through intelligence collection and analysis; second, pursuing cybercrime through targeted enforcement and investigative action; and third,

[*Traduction*]

Aujourd'hui, je ferai le survol du mandat, des rôles et des responsabilités de la GRC ainsi que des initiatives d'application de la loi en ce qui concerne la lutte contre la cybercriminalité au Canada et dans le secteur financier.

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

La GRC joue un rôle de premier plan en travaillant dans le sens des priorités générales du gouvernement du Canada qui consistent à assurer la sécurité des Canadiens. À ce titre, elle a reçu des autorités fédérales le mandat et le pouvoir d'enquêter sur les infractions criminelles ayant trait à la cybercriminalité.

Ces enquêtes portent notamment sur les incidents visant les systèmes, les réseaux et les autres infrastructures essentielles du gouvernement. Nos enquêtent peuvent permettre d'appréhender des criminels ou de mettre fin à leurs activités dans le cyberespace.

Les efforts d'application de la loi déployés dans le cyberespace se butent à des défis sans précédent. Cette situation découle en grande partie de la nature transversale de la cybercriminalité. Celle-ci s'applique en effet à tous les types de crimes et à tous les niveaux des services de police, en plus de ne pas connaître de frontières. Cette dernière caractéristique fait en sorte que les criminels peuvent sévir dans de nombreux pays simultanément.

En outre, la nature extensible de la cybercriminalité est telle qu'un seul individu peut faire un très grand nombre de victimes à très grande échelle, ce qui n'est pas possible dans le monde physique.

Par conséquent, la cybercriminalité est un problème mondial qui a d'importantes répercussions sur la sécurité et le bien-être économique des Canadiens et des entreprises canadiennes, et ce, surtout pour les membres les plus vulnérables de la société comme les personnes âgées et les jeunes. Les entreprises canadiennes et les Canadiens eux-mêmes sont des cibles de choix pour les cybercriminels en raison de la richesse relative de notre pays et de notre économie fondée sur Internet.

Bien consciente des menaces et des défis qui existent, la GRC a rendu publique, en décembre 2015, sa Stratégie de lutte contre la cybercriminalité. Cette stratégie vise à réduire la menace que représente la cybercriminalité au Canada, le nombre de victimes qui en souffrent et les répercussions de ce phénomène. Elle s'articule autour de trois piliers. Premièrement, il faut déterminer les menaces liées à la cybercriminalité et en établir l'ordre de priorité via la cueillette et l'analyse de renseignements.

support cybercrime investigations with specialized skills, tools and training.

The Cybercrime Strategy includes an operational framework that was developed to guide the RCMP's actions against cybercrime. One outcome of this is the development and enhancement of a number of teams. The RCMP's federal investigations are undertaken primarily by the National Division Cybercrime Investigative Team located in Ottawa. Divisional Serious and Organized Crime sections, as well as RCMP technical crime units, also provide support and lead cybercrime investigations when the National Division team requires assistance.

The National Division Cybercrime Investigative Team, along with our technical investigative services, also works to improve digital forensic evidence capabilities for all types of investigations.

The National Intelligence Coordination Centre cyberteam is a dedicated federal policing intelligence unit focused on identifying new and emerging cybercrime threats.

With respect to cybercrime matters related to critical infrastructure, the National Critical Infrastructure Team examines physical and cyber threats to critical infrastructure. The team works closely with a range of domestic partners, including banks and other law enforcement agencies, to identify vulnerabilities or trends in order to prevent or mitigate the impact of attacks on our critical infrastructure.

Overall, the RCMP coordinates and collaborates with domestic, private sector and international partners to target cybercrime threat actors or to identify new and emerging cybercrime threats and methodologies. Specifically, the RCMP works closely with federal departments that play an active role in cybersecurity, including CCIRC, as noted by my colleague Mr. Hatfield; the Canadian Security Intelligence Service; and the Communications Security Establishment Canada.

Coordinated and collaborative efforts are conducted on many fronts and are in line with the vision outlined in the Cybercrime Strategy.

Deuxièmement, il faut contrer la cybercriminalité en menant des activités ciblées d'enquête et d'application de la loi. Troisièmement, on doit soutenir les enquêtes liées à la cybercriminalité en misant sur la spécialisation des compétences, des outils et de la formation.

La Stratégie de lutte contre la cybercriminalité comprend un cadre opérationnel élaboré dans le but d'orienter les mesures prises par la GRC dans ce contexte. L'un des résultats a été la mise sur pied et le renforcement d'un certain nombre d'équipes. Les enquêtes de la GRC à l'échelon fédéral sont principalement menées par l'Équipe d'enquête sur la cybercriminalité de la Division nationale dont les bureaux sont situés à Ottawa. Les groupes divisionnaires en charge des crimes graves et du crime organisé de même que les groupes s'occupant de criminalité technologique peuvent aussi apporter leur appui ou mener des enquêtes en matière de cybercriminalité lorsque l'équipe de la Division nationale a besoin d'aide.

L'Équipe d'enquête sur la cybercriminalité de la Division nationale travaille aussi avec nos services d'enquêtes techniques en vue d'améliorer les capacités en matière de collecte de preuves informatiques judiciaires pour tous les types d'enquêtes.

L'Équipe d'enquête sur la cybercriminalité du Centre national de coordination du renseignement est un groupe de la Police fédérale voué au renseignement dont les efforts portent sur le repérage des menaces, nouvelles et émergentes, en matière de cybercriminalité.

En ce qui a trait à la cybercriminalité visant les infrastructures essentielles, l'Équipe nationale des infrastructures essentielles examine les menaces réelles et virtuelles à cet égard. Cette équipe travaille en étroite collaboration avec une diversité de partenaires au pays, comme les banques et les autres organismes d'application de la loi, pour cerner les tendances et les vulnérabilités dans le but de prévenir ou d'atténuer les répercussions d'attaques menées contre les infrastructures essentielles.

Dans l'ensemble, la GRC coordonne les efforts déployés en collaboration avec ses partenaires nationaux, internationaux et du secteur privé pour cibler les auteurs des menaces liées à la cybercriminalité et pour cerner les menaces nouvelles et émergentes en la matière ainsi que les méthodes utilisées par les cybercriminels. Plus précisément, la GRC travaille en collaboration étroite avec les ministères et organismes fédéraux qui jouent un rôle actif dans le domaine de la cybersécurité, y compris le Centre canadien de réponse aux incidents cybernétiques, dont parlait mon collègue M. Hatfield, le Service canadien du renseignement de sécurité et le Centre de la sécurité des télécommunications du Canada.

Des efforts de collaboration et de coordination sont consentis sur plusieurs fronts conformément à la vision définie dans notre Stratégie de lutte contre la cybercriminalité.

Law enforcement activities range from identifying and prioritizing cybercrime threats based on criminal intelligence; coordinating, investigating and disrupting cybercrime activities; and handling digital evidence to support cybercrime investigations.

Operationally, the focus for our investigations include malware developers and distributors; cybercrime infrastructure developers and operators that facilitate cybercrime, for instance, botnets, forums and digital marketplaces; financial network operators that facilitate the laundering and monetization of proceeds from cybercrime; and investigations into traditional crimes under the federal mandate, such as fraud, where the perpetrators are able to use cyber systems to increase victimization.

When it comes to Canada's financial and commercial sectors, the volume and severity of cybercrime affecting Canadians and businesses has been increasing significantly.

The advancements in technology that can be used to assist traditional crimes such as money laundering has led to a shift in the way that law enforcement must respond to large-scale financial crime. No longer are organized crime groups, professional money launderers or international money controllers bound by traditional methods of laundering and moving their proceeds of crime. Dark web marketplaces, the growth of virtual currencies and complex trade-based money laundering schemes are examples of technological advancements that have effectively eroded borders and allowed criminal organizations to set up a truly global footprint.

Cybercrimes that are reported to the RCMP reveal that many are linked to significant financial crimes, both domestically and internationally. That includes the deployment of malware such as banking Trojans, a multiplicity of online fraud scams, email compromise or through extortion events including ransomware or distributed denial of service attacks.

That said, cybercrimes are also under-reported, and one of the reasons stems from the myriad of reporting mechanisms in Canada that are confusing for the public and reduce the likelihood of reporting.

The under-reporting prevents law enforcement from connecting the dots because of a lack of appropriate data to comprehensively understand and analyze the issues. This hinders

Nos activités d'application de la loi vont de la détermination des menaces liées à la cybercriminalité et l'établissement de leur ordre de priorité au moyen du renseignement criminel jusqu'à la coordination des activités d'enquête et de perturbation des activités cybercriminelles, en passant par le traitement des preuves numériques à l'appui de ces enquêtes.

Sur le plan opérationnel, nos enquêtes visent surtout les concepteurs et distributeurs de logiciels malveillants, les créateurs de l'infrastructure utilisée pour la cybercriminalité, les exploitants qui facilitent la cybercriminalité (p. ex., les réseaux de zombis, les forums et les marchés numériques), et les exploitants de réseaux financiers qui facilitent le blanchiment d'argent et la monétisation des produits de la cybercriminalité. De plus, en vertu de notre mandat fédéral, nous menons des enquêtes sur des crimes plus « traditionnels », comme la fraude, lorsque leurs auteurs utilisent des systèmes cybernétiques pour accroître le nombre de leurs victimes.

Pour ce qui est du secteur financier et du secteur commercial au Canada, le volume et la gravité des cybercrimes dont sont victimes des Canadiens et des entreprises du pays ont augmenté considérablement.

En raison des progrès technologiques qui peuvent faciliter les crimes « traditionnels » comme le blanchiment d'argent, les organismes d'application de la loi ont dû modifier la manière dont ils réagissent à la criminalité financière de grande envergure. Les groupes du crime organisé, les blanchisseurs d'argent professionnels et les contrôleurs d'argent internationaux ne sont plus cantonnés à l'emploi de méthodes traditionnelles pour blanchir l'argent et transférer les produits de la criminalité. Les marchés du Web invisible, la multiplication des monnaies virtuelles et les stratagèmes complexes de blanchiment d'argent au moyen d'activités commerciales sont des exemples des progrès technologiques qui ont carrément effacé les frontières et permis aux organisations criminelles de vraiment s'implanter partout dans le monde.

Un grand nombre des cas signalés à la GRC sont des cybercrimes financiers importants commis au Canada ou à l'échelle internationale. Il s'agit notamment de la diffusion de logiciels malveillants, comme les chevaux de Troie bancaires, les multiples escroqueries en ligne, la compromission des courriels et la multiplication des moyens d'extorsion comme les rançongiciels et les attaques par déni de service coordonné.

Cela dit, de nombreux cybercrimes ne sont pas signalés, notamment en raison du trop grand nombre de moyens permettant de le faire au Canada. Cette abondance de mécanismes est une source de confusion pour les gens et réduit, de ce fait, la probabilité qu'un cybercrime soit signalé.

Pour cette raison, les organismes d'application de la loi ne peuvent pas établir de liens entre les crimes, car ils n'ont pas les données voulues pour bien comprendre et analyser les problèmes. Cela les empêche de s'attaquer stratégiquement à la

law enforcement from strategically responding to cybercrime on a larger, coordinated and more targeted scale.

While we continue with efforts to combat cybercrime, gaps and challenges remain. First, most cybercrimes are multi-jurisdictional in nature but are often addressed by domestic police services in isolation, leading to uncoordinated law enforcement efforts.

The demand in this area of criminality has surpassed the RCMP's capacity. We are unable to realistically commence more cybercrime investigations against major threats. It's also a challenge to coordinate joint investigations with international law enforcement partners whose capacity and capabilities differ from ours, making it difficult to ensure Canadian elements are prioritized.

Addressing cybercrime requires both international and domestic cooperation.

Lastly, there is a need for more resources possessing the knowledge and expertise to effectively combat cybercrime. This is an area that affects virtually all law enforcement cybercrime efforts.

[*Translation*]

Bearing this in mind, the RCMP still continues to actively take action to advance the level of readiness to respond to cybercrime and engage in effective collaboration with international partners. On the international front for example, the RCMP works with international law enforcement partners to disrupt networks such as major international criminal infrastructure platforms, used to launch and manage mass global malware attacks. The monetary losses associated with malware attacks are estimated to be in the hundreds of millions worldwide.

The RCMP participates in concerted global efforts with international law enforcement partners to take down such networks and to identify key cybercrime threat actors.

[*English*]

The RCMP is working with government and other stakeholders to examine a variety of reform measures that would help strengthen our ability to keep pace with cybercrime writ large. Some of the specific actions include greater law enforcement collaboration with industry partners, developing new in-house technical solutions, more domestic and international cooperation, and expansion of public awareness.

cybercriminalité à plus grande échelle et de manière coordonnée et mieux ciblée.

Nous poursuivons nos efforts pour combattre la cybercriminalité, mais il y a toujours des lacunes et des difficultés. Premièrement, bien que la plupart des cybercrimes concernent plusieurs administrations à la fois, ils sont souvent abordés isolément par les services de police locaux, ce qui nuit à la coordination des efforts d'application de la loi.

La demande dans ce domaine de la criminalité a surpassé la capacité de la GRC. En fait, nous ne pouvons plus entreprendre de nouvelles enquêtes à l'égard de cybermenaces majeures. Nous avons aussi de la difficulté à coordonner les enquêtes menées conjointement avec nos partenaires étrangers dont les capacités de lutte contre les cybermenaces diffèrent des nôtres. Par conséquent, nous ne pouvons pas nous assurer que les éléments canadiens de ces enquêtes conjointes ont la priorité.

Pour lutter contre la cybercriminalité, il faut de la coopération, tant au Canada qu'à l'échelle internationale.

Enfin, il nous faut plus de ressources pouvant nous faire bénéficier des connaissances et de l'expertise nécessaires pour combattre efficacement la cybercriminalité. C'est vrai pour la quasi-totalité des efforts déployés pour contrer ce phénomène.

[*Français*]

Il ne faut pas oublier que la GRC continue de prendre des mesures concrètes pour améliorer le degré de préparation requis pour réagir aux cybercrimes et établir une collaboration efficace avec ses partenaires étrangers. Par exemple, sur la scène internationale, la GRC travaille de concert avec les responsables de l'application de la loi d'autres pays afin de perturber les réseaux, comme les plateformes majeures de l'infrastructure criminelle internationale, qui sont utilisés pour lancer et gérer des attaques intensives et mondiales de logiciels malveillants. Les pertes monétaires associées aux attaques de logiciels malveillants sont estimées, à l'échelle internationale, à des centaines de millions de dollars.

La GRC participe à des initiatives mondiales concertées avec ses partenaires de l'application de la loi à l'étranger afin de détruire les réseaux et identifier les principaux acteurs de la cybermenace.

[*Traduction*]

La GRC travaille avec le gouvernement et d'autres intervenants dans le but d'explorer diverses réformes qui pourraient aider à renforcer notre capacité à suivre le courant du milieu de la cybercriminalité dans son ensemble. Parmi les mesures envisagées, on pourrait élargir la collaboration avec les partenaires du secteur de l'application de la loi, élaborer à l'interne de nouvelles solutions techniques, augmenter la

Specific to financial crime, the RCMP continues to work with its partners both domestically and internationally to understand better and to address the technological advances. This includes improving information sharing, identifying and taking joint action to address the rise of international money controllers, and sharing methods for training front-line officers on the complexities associated with modern financial crime.

Domestically, we are working with our Government of Canada partners to modernize our financial crime regime to ensure that law enforcement has the tools they need to meet today's challenges effectively as well as those we know that are coming in the future.

I thank you for inviting the RCMP here today and welcome your questions.

The Deputy Chair: Chief Superintendent Doran, thank you very much for your presentation.

We will go to the Canadian Security Intelligence Service, Charles Lowson.

[*Translation*]

Charles Lowson, Director General, Counterintelligence and Counter Proliferation, Canadian Security Intelligence Service: Good afternoon, Mr. Chair and members of the committee. My name is Charles Lowson and I am the Director General of the Counterintelligence and Counter Proliferation Division at the Canadian Security Intelligence Service, or CSIS. My division is responsible for the service's investigations of espionage, foreign influence, proliferation of weapons of mass destruction and certain threats. It also houses CSIS' Cyber Centre, which conducts national security cyber investigations.

[*English*]

Mr. Chairman, the men and women of CSIS work diligently every day to keep Canada and Canadians safe, and I'm proud to represent them here today.

[*Translation*]

I would like to thank you for your invitation to participate in this study on cyber security as it relates to Canada's financial and commercial sectors. I will keep my remarks brief, but I

coopération au Canada et à l'échelle internationale, et sensibiliser davantage la population.

En ce qui concerne la criminalité financière, la GRC continue de travailler en collaboration avec ses partenaires, au Canada et à l'étranger, afin de mieux comprendre les avancées technologies pour pouvoir agir en conséquence. Cela consiste notamment à améliorer les échanges d'information, à cerner et mettre en œuvre les mesures nécessaires devant être prises conjointement pour réagir à l'émergence des contrôleurs d'argent internationaux, et à mettre en commun les méthodes utilisées pour la formation des agents de première ligne à l'égard de la complexité de la criminalité financière moderne.

Au Canada, nous collaborons avec nos partenaires du gouvernement fédéral pour moderniser notre régime de lutte contre la criminalité financière afin que les responsables de l'application de la loi disposent des outils dont ils ont besoin pour surmonter les obstacles déjà existants et ceux que nous prévoyons devoir affronter un jour.

Je tiens à vous remercier d'avoir invité la GRC à comparaître aujourd'hui et je serai ravi de répondre à toutes vos questions.

Le vice-président : Monsieur le surintendant principal, merci beaucoup pour cet exposé.

Nous allons maintenant entendre Charles Lowson du Service canadien du renseignement de sécurité.

[*Français*]

Charles Lowson, directeur général, Contre-espionnage et Lutte contre la prolifération, Service canadien du renseignement de sécurité : Monsieur le président, mesdames et messieurs les membres du comité, bonjour. Je m'appelle Charles Lowson, je suis le directeur général de la division du contre-espionnage et de la lutte contre la prolifération au Service canadien du renseignement de sécurité, ou SCRS. Ma division est chargée des enquêtes du service sur l'espionnage, l'ingérence étrangère, la prolifération des armes de destruction massive et certaines menaces. Elle comprend également le Cybercentre du SCRS, qui mène des enquêtes sur les cybermenaces qui pèsent sur la sécurité nationale.

[*Traduction*]

Monsieur le président, les hommes et les femmes qui travaillent au SCRS mettent tout en œuvre jour après jour pour assurer la sécurité de notre pays et de nos concitoyens canadiens. Je suis fier de les représenter ici aujourd'hui.

[*Français*]

Je vous remercie de m'avoir invité à participer à cette étude sur la cybersécurité ayant trait au secteur financier et commercial du Canada. Je serai bref, mais je tiens à vous éclairer sur le

would like to provide some insight into the service's mandate and role within the broader cyber security community in Canada.

[*English*]

The CSIS Act mandates the service to investigate activities suspected of constituting "threats to the security of Canada" and to advise the government on these threats. These threats are defined in section 2 of the CSIS Act as espionage and sabotage, foreign-influenced activity, terrorism and the subversion of government through violence. CSIS may also undertake measures to reduce the threats to the security of Canada in accordance with well-defined legal requirements and ministerial direction.

Our digital and interconnected world provides a powerful channel by which hostile entities can conduct espionage, foreign influence and even terrorist activity targeting the institutions, businesses and citizens of Canada. Offensive cyber operations have become a tool by which foreign hostile states conduct espionage, sabotage and foreign interference.

While, by virtue of the sensitivity of CSIS's work, I cannot speak to specific threats or active ongoing operations, I can speak to the nature of national security cyber investigations, the current threat environment and channels through which CSIS advises government partners on cyber threats to the security of Canada.

During the course of a cyber investigation, the service leverages the expertise of both technical resources, such as computer scientists, and non-technical resources, such as intelligence officers who are knowledgeable in traditional intelligence operations. It employs a range of collection techniques, which may include human sources, to better understand the trade craft and motivations of cyber threat actors as well as to determine the attribution of cyber incidents. This body of knowledge is crucial in terms of supporting the Government of Canada to assess fully and respond to cyberattacks as well as more broadly to help the Government of Canada respond to the challenges of espionage, sabotage, foreign influence and terrorism.

As an open and developed economy, as well as a leader in innovation and research and development, Canada is a prominent target for malicious cyberattacks, be they perpetrated by state or state-sponsored actors, terrorists or organizations. CSIS investigates threats Canada's national security and provides advice to government. As such, our focus is on states and state-sponsored actors who operate clandestinely, including with cyber operations, to achieve their objectives to the detriment of Canada's national interest.

mandat et le rôle du SCRS au sein de la communauté de la cybersécurité au Canada.

[*Traduction*]

La Loi sur le SCRS confie au Service le mandat d'enquêter sur les activités pouvant constituer une menace pour la sécurité du Canada et de conseiller le gouvernement fédéral à cet égard. Ces menaces, qui sont définies à l'article 2 de la Loi sur la SCRS, sont l'espionnage, le sabotage, l'ingérence étrangère, le terrorisme et la subversion du gouvernement par la violence. Le service peut aussi prendre des mesures pour réduire les menaces pesant sur la sécurité du Canada dans le respect des règles de droit applicables et en conformité avec les instructions du ministre.

Le monde numérique et interconnecté dans lequel nous vivons offre à des organisations et à des personnes malintentionnées un moyen puissant de mener des activités d'espionnage, d'ingérence étrangère, voire de terrorisme, contre les institutions, les entreprises et les citoyens du Canada. Pour des États hostiles, les cyberopérations offensives sont devenues un outil d'espionnage, de sabotage et d'ingérence.

Même si le caractère confidentiel du travail effectué par le SCRS m'empêche de traiter de menaces précises ou d'opérations en cours, je peux vous parler de la nature des enquêtes visant les cybermenaces qui pèsent sur la sécurité nationale, du contexte actuel de ces menaces et des moyens qu'utilise le SCRS pour conseiller ses partenaires gouvernementaux à cet égard.

Pendant une cyberenquête, le service tire parti de l'expertise de ressources techniques, comme les informaticiens, et de ressources non techniques, comme les agents de renseignement qui connaissent le fonctionnement des opérations de renseignement traditionnelles. Le SCRS utilise une vaste gamme de techniques d'enquête, notamment le recours à des sources humaines, pour mieux comprendre les méthodes et les motivations des auteurs de cybermenaces et pour attribuer les cyberincidents. Ces connaissances sont essentielles pour soutenir le gouvernement du Canada de manière à lui permettre de bien évaluer les cyberattaques afin d'y réagir adéquatement, et pour l'aider, dans une perspective plus générale, à relever les défis que posent l'espionnage, le sabotage, l'ingérence étrangère et le terrorisme.

En raison de son économie ouverte et développée et de son statut de chef de file en matière d'innovation, le Canada est une cible de choix pour les cyberattaques malveillantes, qu'elles proviennent d'auteurs étatiques ou parrainés par un État, de terroristes ou d'organisations criminelles. Le SCRS enquête sur les menaces envers la sécurité du Canada et conseille le gouvernement à cet égard. Il se concentre ainsi sur les États et sur les intervenants parrainés par un État qui mènent des activités clandestines, y compris des cyberopérations, pour atteindre leurs objectifs au détriment de l'intérêt national du Canada.

[*Translation*]

In addition to stealing intellectual property, one of the objectives of state- sponsored cyber-activity is to obtain information which will give foreign companies a competitive edge over Canadian firms. This can have a negative impact on investment or acquisition negotiations involving Canadian companies and the Government of Canada, and, in turn, lead to lost jobs, revenue, and market share. Ultimately, cyber-espionage negatively impacts Canada's economy as a whole.

[*English*]

With respect to specific cyber threats to Canada's financial and commercial sectors, the topic of this study, I will defer to my colleagues at the Canadian Cyber Incident Response Centre and the Communications Security Establishment Canada, who specialize in cybersecurity. CSIS has no role in the development of cybersecurity mitigation measures or the provision of advice to the public or industry. It does, however, support its Government of Canada partners when there is a clear threat to national security or a state-sponsored actor involved.

The service does not have the mandate to investigate cybercrime, either, which is rightly a law enforcement role. Of course, the service de-conflicts regularly with the RCMP on a broad range of concerns, including cyberattacks, when the nexus to cybersecurity is unclear, a relatively common situation in the nebulous world of cyber investigations.

In the event of a cyber compromise that represents a threat to national security, the service works closely with other government departments such as the Royal Canadian Mounted Police, the Communications Security Establishment Canada and the Canadian Cyber Incident Response Centre to respond to the cyber compromise, including investigating the compromise, identifying the actor and trade craft, and informing government.

Responses may require immediate technical solutions, but they may also require a broader response. Cyberattacks perpetrated by state actors do not necessarily call for a response in kind. Instead, a variety of different Government of Canada responses may be considered, depending on the state and the gravity of the situation. Informing the development of such responses with intelligence is a key role for CSIS.

[*Français*]

Outre le vol de propriété intellectuelle, les cyberactivités parrainées par un État visent notamment à obtenir des informations qui permettraient à des sociétés étrangères de jouir d'un avantage concurrentiel sur les entreprises canadiennes. Cela peut nuire aux négociations liées à des projets d'investissement ou d'achat avec des entreprises canadiennes et le gouvernement du Canada, puis entraîner la perte d'emplois, de revenus et de parts du marché. En définitive, le cyberespionnage a une incidence négative sur l'économie du Canada dans son ensemble.

[*Traduction*]

En ce qui a trait au sujet de la présente étude, c'est-à-dire les cybermenaces qui visent précisément les secteurs financier et commercial du Canada, je m'en remets aux connaissances de mes collègues du Centre canadien de réponse aux incidents cybernétiques et du Centre de la sécurité des télécommunications, qui sont des spécialistes de la cybersécurité. Le SCRS ne joue aucun rôle dans l'élaboration de mesures d'atténuation des cyberincidents ni dans la prestation de conseils au public ou à l'industrie. Par contre, il soutient ses partenaires du gouvernement du Canada lorsqu'il est manifeste qu'une menace pèse sur la sécurité nationale ou qu'il y a implication d'un intervenant parrainé par un État.

En outre, le SCRS n'a pas le mandat d'enquêter sur la cybercriminalité, qui relève à juste titre des forces de l'ordre. Bien sûr, le SCRS et la GRC harmonisent souvent leurs activités liées à un large éventail de préoccupations, dont les cyberattaques, lorsque le lien avec la sécurité nationale est flou. Il s'agit d'une situation relativement courante dans l'univers nébuleux des cyberenquêtes.

Lorsque la compromission de systèmes informatiques constitue une menace pour la sécurité nationale, le SCRS collabore étroitement avec des partenaires du gouvernement fédéral, y compris la GRC, le Centre de la sécurité des télécommunications du Canada et le Centre canadien de réponse aux incidents cybernétiques, pour réagir à l'incident. Entre autres, il enquête sur la compromission, détermine qui en est l'auteur et quelle est la méthode utilisée, et en informe le gouvernement.

La situation peut exiger l'application immédiate de solutions techniques, mais elle peut aussi requérir une réaction plus vaste. Il n'est pas nécessairement adéquat de rendre la pareille aux auteurs étatiques de cyberattaques. Plutôt, le gouvernement du Canada peut réagir de différentes manières, en fonction du contexte et de la gravité de la situation. Fournir des renseignements au gouvernement pour l'aider à donner un fondement adéquat à ses réactions est l'un des rôles essentiels du SCRS.

The service also works closely with Five Eyes partners and like-minded foreign security and intelligence agencies for the purpose of intelligence exchange. This supports the Government of Canada's awareness of broader cyber threats affecting allies and partners around the world, and supports the development of well-informed Canada-only or joint responses.

For CSIS, foreign influence activity using cyber means is also an investigative priority. States can and do use cyber-facilitated activities to interfere in the lives of members of diasporas across this country and to intimidate or quell political dissent. Recent events around the world have shown the impact that foreign interference in fundamental institutions, including the media, can have, with significant consequences on political systems and outcomes. Cyberattacks are a powerful tool that can be used to release damaging information and spread misinformation that undermines public discourse.

[*Translation*]

As Canada and the world continue to embrace connected digital technologies to progress, cyber-attacks will remain an effective tool of choice for a range of hostile actors: cyber-attacks are efficient, cost effective and deniable. State-sponsored cyber-attacks benefit from significant, dedicated resources, and increased sophistication. This is a threat that is ever-evolving, and a threat that hangs over all sectors of Canadian society.

With that, Mr. Chair, I will conclude my remarks and welcome any questions.

The Deputy Chair: Thank you very much, Mr. Lowson.

[*English*]

Senator Wallin: I have two related questions, first to Mr. Hatfield. As we begin our study here and as Canadians look at this information, everybody will be a bit taken aback to discover that you can't enforce or regulate cybercrime, that no individual has an obligation to tell you if something happens and you can't compel somebody to do that. Do you think those rules should change? I ask that because of Superintendent Doran's remarks that, because cybercrimes are under-reported, that such under-reporting prevents law enforcement from connecting the dots — which was his phrase — and at the same time demand in this area has surpassed your capacity. Chief Superintendent, is this a cry for budgets or a policy change, or both?

Par ailleurs, le service collabore étroitement avec ses partenaires du Groupe des cinq ainsi qu'avec des services de sécurité et de renseignement étrangers de même tendance en vue d'échanger des renseignements. Cela permet au gouvernement du Canada d'être au courant des cybermenaces générales qui touchent ses alliés et ses partenaires du monde entier et de bien fonder ses réactions individuelles ou communes.

Les activités influencées par l'étranger à l'aide de moyens informatiques sont également une priorité d'enquête du SCRS. Des États sont en mesure de mener de telles activités pour s'ingérer dans la vie de membres de communautés d'expatriés au Canada et pour intimider ou faire taire des dissidents politiques, et ils ne s'en privent pas. Des événements survenus récemment dans le monde ont révélé les répercussions que peut avoir l'ingérence étrangère dans des institutions fondamentales, comme les médias, ainsi que ses conséquences importantes sur les systèmes politiques et ses résultats. Les cyberattaques constituent un outil puissant pouvant servir à répandre des informations nuisibles ou mensongères qui minent le discours public.

[*Français*]

Puisque le Canada et le monde ne cesseront pas d'adopter les technologies numériques et connectées dans leur marche vers l'avant, les cyberattaques demeureront un outil efficace et prisé par de nombreux cyberintervenants. Elles fonctionnent, elles sont peu coûteuses, et il est possible de nier en être l'auteur. Les cyberattaques parrainées par un État qui gagne en complexité bénéficient de ressources importantes et exclusives. Il s'agit d'une menace en constante évolution qui pèse sur tous les secteurs de la société canadienne.

Sur ce, monsieur le président, je termine mon allocution et je suis prêt à répondre à toutes vos questions.

Le vice-président : Merci beaucoup, monsieur Lowson.

[*Traduction*]

La sénatrice Wallin : J'ai deux questions connexes. La première s'adresse à M. Hatfield. Au moment où nous commençons notre étude et où les Canadiens examinent cette information, tout le monde sera un peu étonné de constater qu'en matière de cybercriminalité, Sécurité publique n'est ni un organisme de réglementation, ni un organisme d'application de la loi; qu'aucun individu n'a l'obligation de lui dire que quelque chose s'est produit; et qu'on ne peut pas forcer quelqu'un à le faire. Croyez-vous que ces règles devraient changer? Si je pose la question, c'est que le M. Doran a dit que parce que les cybercrimes ne sont pas signalés, les organismes d'application de la loi ne peuvent pas établir de liens entre les crimes — ce sont ses mots — et parallèlement, la demande dans ce domaine a surpassé la capacité. Monsieur le surintendant, demandez-vous des fonds ou un changement de politiques, ou encore les deux?

Mr. Hatfield: Thank you for the question.

First, I would say that there's a distinction between a cybercrime and a technical incident that occurs on a computer network. When a partner contacts Public Safety Canada saying, "I think I see something odd on my network," that doesn't necessarily mean a crime has been committed, and it doesn't necessarily mean that information has been breached. There is a distinction there. The focus of Public Safety Canada is technical network security information to assist our partners in securing their networks and passing on anything we can learn to other partners.

With respect to what should be done, based on the cyber review that has occurred over the past few years, which included a public consultation, there was a significant demand for government leadership in this area. Regulations, standards and all of that were prominently featured in all of the commentary that we received. All of that input is currently being used to determine a new way forward for government.

Senator Wallin: Is there a time frame on that?

Mr. Hatfield: I'm afraid I don't have a date for you, senator.

Mr. Doran: My comments were neither a request for funding nor a request for policy change. We are well engaged with our other government partners to try to figure this issue out.

On the issue of our ability, our capacity has been surpassed. The reality is, it would be no surprise to anybody here that we could have all the resources in the world and there would still be files we couldn't get to. That's just the nature of cybercrime.

For us, it's a combination of the advances in technology that are moving the cybercrime yardsticks very quickly with our inability to staff up properly and efficiently to be able to get to them. That said, our model is one that prioritizes our files based on the greatest threats, so those are the files we're working on. I'm satisfied that we're working on the ones that would be most concerning to Canadians.

Senator Wallin: Would mandatory reporting help or just increase your workload?

Mr. Doran: I don't know that mandatory reporting would help necessarily. What it might do, however, is if we were able to consolidate those reports and analyze them properly, we may develop links that shore up one file in Vancouver, another in Calgary, another in Toronto, that are actually all the same

M. Hatfield : Je vous remercie de la question.

Je dirais tout d'abord qu'il y a une différence entre un cybercrime et un incident technique sur un réseau informatique. Lorsqu'un partenaire communique avec Sécurité publique Canada et lui dit qu'il croit voir quelque chose d'étrange sur son réseau, cela ne veut pas nécessairement dire qu'un crime a été commis et qu'il y a eu violation de renseignements. Il y a une distinction à faire. Sécurité publique Canada se concentre sur l'information technique sur la sécurité des réseaux et aide ses partenaires à sécuriser leurs réseaux et il s'agit de transmettre tout ce que nous apprenons à d'autres partenaires.

Pour ce qui est des mesures à prendre, selon l'examen de la cybersécurité qui a été mené ces dernières années, qui incluait une consultation publique, on a fortement demandé à ce que le gouvernement fasse preuve de leadership à cet égard. Tous les commentaires que nous avons reçus portaient grandement sur la réglementation, les normes et d'autres sujets de ce genre. Toutes les idées reçues sont présentement utilisées pour déterminer une nouvelle avenue pour le gouvernement.

La sénatrice Wallin : Est-ce qu'une date a été fixée à cet égard?

M. Hatfield : Je crains de ne pas avoir de date à vous fournir, sénatrice.

M. Doran : Il ne s'agissait pas ici de demander des fonds ou un changement de politique. Nous collaborons avec nos partenaires du gouvernement pour essayer de trouver une solution.

En ce qui concerne notre capacité, elle a été surpassée. Le fait est, et cela n'étonnera personne, que même si nous avions toutes les ressources au monde, il y aurait toujours des dossiers que nous ne pourrions pas régler. Telle est simplement la nature de la cybercriminalité.

Pour nous, il s'agit à la fois des progrès technologiques qui changent très rapidement les choses sur le plan de la cybercriminalité et de notre incapacité d'avoir les effectifs nous permettant d'aller au fond des choses. Cela dit, nous suivons un modèle selon lequel la priorité est accordée aux plus grandes menaces, et ce sont les dossiers auxquels nous travaillons. J'estime que nous travaillons à ceux qui préoccupent davantage les Canadiens.

La sénatrice Wallin : Le signalement obligatoire serait-il utile ou ne ferait-il qu'accroître votre charge de travail?

M. Doran : J'ignore si le signalement obligatoire serait nécessairement utile. Toutefois, si nous étions en mesure de regrouper les rapports et de bien les analyser, nous pourrions établir des liens entrent un dossier de Vancouver et d'autres dossiers, de Calgary et de Toronto, et nous rendre compte qu'il s'agit des mêmes responsables, ce qui ne se fait pas

perpetrators, which is something that's not happening now. It is happening a little bit, but not on the scale we'd like to see it.

Senator Wetston: Thank you for coming today. I wanted to explore a general area with you. All can answer if you wish. It's not specific to any particular person. From my own experience — and you would probably agree with me — the Internet is clearly the 21st century crime scene. I describe it that way in lay terms.

I read a report from the World Economic Forum, the Davos forum, the Global Risks Report. They recognize that cybersecurity is one of the top commercial risks today. I suspect none of you would disagree with that, but I just pose it as part of my question.

I'd like you to comment on whether this is just an IT issue or is it something more? If you permit me, I'll combine the questions.

I want to pose my question this way because it's more than an IT issue and obviously your expertise is important in this issue. The technology we have is advancing the risks to the marketplace associated with this technology. So the same technology that's creating the benefits is also the same technology that's creating the opportunities for cybercrime and disruption. What is the state of readiness within Canada to deal with cybercrime and cyberattacks in general terms?

Mr. Hatfield: Thank you, senator. You said that cyberspace is the 21st century crime scene and that cybersecurity is one of the top commercial risks. I would also say that cyberspace is the 21st century playground, marketplace and school.

Towards your second question, any kind of technology we've ever developed, be it a sail for a sailboat, a steam engine, electricity, it does bring dangers with it. What we as a society have done largely is learned how to manage and mitigate those risks while leveraging the benefits.

I notice a number of you tonight have tablets in front of you. The tablet as a market segment did not exist eight years ago. When Steve Jobs in 2010 held it up, most people thought he was crazy. That is the rate of change we're seeing with technology.

What is the state of readiness in Canada? Canada has a tremendous amount of capability in this field. We are world leaders in many areas related to cybersecurity. What Canada is doing in quantum research is second to none in the world. Our information communications technology sector is deep, broad and mature. Our impression from where we stand and how we

actuellement. Cela se fait un peu, mais pas autant que nous le souhaiterions.

Le sénateur Wetston : Je vous remercie de votre présence. Je voulais explorer un thème général avec vous. Vous pouvez tous répondre si vous le voulez. Ma question ne s'adresse pas à un témoin en particulier. D'après mon expérience — et vous serez probablement d'accord avec moi —, de toute évidence, Internet est la scène de crime du XXIe siècle. Je le décris ainsi, en termes simples.

J'ai lu un rapport du Forum économique mondial, du forum de Davos, soit le rapport sur les risques. On y constate que la cybersécurité représente l'un des grands risques commerciaux de nos jours. Je suppose que c'est l'avis de tous les gens ici présents, mais je le dis dans le contexte de ma question.

J'aimerais savoir si vous êtes d'avis qu'il ne s'agit que d'une question de TI ou s'il y a autre chose. Si vous me le permettez, je vais poser toutes mes questions maintenant.

Je veux poser ma question de cette façon parce qu'il ne s'agit pas seulement d'une question de TI et, évidemment, votre expertise est importante à cet égard. Les technologies que nous avons augmentent les risques pour le marché. Ainsi, une technologie qui crée les avantages crée également les occasions de commettre des cybercrimes et de causer des perturbations. Comment décririez-vous la situation du Canada en ce qui concerne l'état de préparation pour lutter contre la cybercriminalité et les cyberattaques en général?

M. Hatfield : Je vous remercie, sénateur. Vous avez dit que le cyberespace est la scène de crime du XXIe siècle et que la cybersécurité représente l'un des principaux risques commerciaux. J'ajouterais que le cyberespace est le terrain de jeu, le marché et l'école du XXIe siècle.

Concernant votre deuxième question, quelle que soit la technologie que nous avons créée, qu'il s'agisse d'un voilier pour un bateau à voile, d'une machine à vapeur ou de l'électricité, des dangers y sont associés. Essentiellement, en tant que société, nous avons appris à gérer et à atténuer les risques tout en tirant parti des avantages.

Je remarque qu'un certain nombre d'entre vous ont une tablette. La tablette, en tant que segment de marché, n'existait pas il y a huit ans. Lorsque Steve Jobs l'a présentée, en 2010, la plupart des gens croyaient qu'il était fou. Voilà la vitesse à laquelle les changements technologiques s'effectuent.

Quel est l'état de préparation du Canada? Le Canada a d'énormes capacités en la matière. C'est un chef de file dans bien des secteurs liés à la cybersécurité. Ce que fait le Canada dans le domaine de la recherche quantique est inégalé dans le monde. Son secteur des technologies de l'information et des communications est vaste et bien établi. D'après notre position et

have engaged with partners is we are very well positioned in this space.

So is this just an IT issue? Absolutely it is not. Cybersecurity is about people, processes and technology, of course. But no technological issue or risk is ever solved just with technology. It's solved by the people who work together to address these issues.

Superintendent Mark Flynn, Director, Cybercrime, Federal Policing, Royal Canadian Mounted Police: I can add to the comments that Mr. Hatfield just gave. It is certainly more than IT. IT is a very large component of it. But as people adopt the new technology in their day-to-day lives and the rate at which they've done so, we're in that spot where they need to balance their use with it, their understanding of it, with the access it provides and the implications it has for their privacy.

The Internet and other online systems have allowed criminals and other actors to remove the personal interaction elements, and some of those personal communication skills that we see that people use to identify when a threat is present and when a threat is not present. The proliferation of all these online systems and communications and the depersonalization of interaction with people for banking and other things make people vulnerable to that impersonal interaction and that trickery that cybercriminals are using to exploit them.

So we're in a place where everyone is learning the advantages of the access, ensuring the privacy and access that they want to have in that space versus implementation of protections to keep them safe while they're there. That's an ongoing effort.

Mr. Lowson: I will largely defer to what my colleagues have said because your questions focused principally on cybercrime. As I mentioned in my opening statements, that's the responsibility of law enforcement, not the Canadian Security Intelligence Service.

However, you did speak about your belief that cybercrime and cyberattacks are more than an IT issue. My colleagues have reinforced that notion. I would agree with that. When we speak specifically about the threats to the security of Canada with which the service is concerned — and again, those would be espionage, sabotage, foreign-influenced activities and terrorism — we've used cyber as an enabler. It's a tool that allows actors to be better at what they do. It's from that perspective that we look at it. So it's connected to the traditional threats that we've always looked at, but it's allowing those threats to be carried out in a new space and with a new velocity. Those are some of the challenges we face as we look at this evolution of the threat.

notre travail de collaboration avec nos partenaires, nous avons le sentiment que nous occupons une place de choix dans ce secteur.

S'agit-il donc seulement d'une question de TI? Non, absolument pas. La cybersécurité concerne les gens, les processus et la technologie, bien sûr. Or, les problèmes ou les risques technologiques ne peuvent pas être éliminés qu'à l'aide de la technologie; ils sont éliminés par les gens qui unissent leurs efforts pour trouver des solutions.

Surintendant Mark Flynn, directeur, Cybercriminalité, Police fédérale, Gendarmerie royale du Canada : Je peux ajouter quelques mots aux observations que vient de faire M. Hatfield. C'est certes plus qu'une question de TI. Les TI constituent un volet très important, mais à mesure que les gens adoptent les nouvelles technologies, quotidiennement, et compte tenu du rythme auquel ils le font, dans l'état actuel des choses, ils doivent trouver un équilibre entre l'utilisation qu'ils en font, la facilité d'accès et les répercussions sur leur vie privée.

Internet et d'autres systèmes en ligne permettent à des criminels et à d'autres acteurs de retirer les composantes d'interactions personnelles, et certaines de ces capacités de communication que, comme nous le voyons, les gens utilisent lorsqu'il y a une menace et lorsqu'il n'y en a pas. La prolifération de tous ces systèmes et communications en ligne et la dépersonnalisation des interactions pour les services bancaires, entre autres, font en sorte que les gens sont vulnérables à cette interaction impersonnelle et à cette ruse que les cybercriminels utilisent pour les exploiter.

Nous sommes donc dans une situation où tout le monde est en train d'en apprendre sur les avantages de l'accès, la protection des renseignements personnels et l'accès qu'on veut avoir dans cet espace par rapport à la mise en place de mesures de protection pour assurer la sécurité. Cela s'inscrit dans un effort constant.

M. Lowson : Je m'en remets grandement à mes collègues, car vos questions portent principalement sur la cybercriminalité. Comme je l'ai mentionné dans ma déclaration préliminaire, elle relève des forces de l'ordre et non du Service canadien du renseignement de sécurité.

Cependant, vous avez dit croire que concernant la cybercriminalité et les cyberattaques, c'est plus qu'une question de TI. Mes collègues ont renforcé cette idée. Je suis d'accord avec eux. Lorsque nous parlons des menaces à la sécurité du Canada, sur lesquelles enquête le service — et encore une fois, ces menaces sont l'espionnage, le sabotage, l'ingérence étrangère et le terrorisme —, nous utilisons le cyberespace comme un outil. Il permet aux acteurs d'être meilleurs dans ce qu'ils font. C'est de ce point de vue que nous examinons les choses. C'est donc lié aux menaces traditionnelles que nous avons toujours examinées, mais ces menaces peuvent être mises à exécution dans un nouvel espace et à un rythme différent. Voilà une partie

[*Translation*]

Senator Moncion: Thank you for your presentation. I have worked in the financial milieu, and I know that it was generally well protected, precisely because large amounts of money are at stake. You spoke a great deal about infrastructures. What type of regulation is in place to help reduce the number of investigations for businesses that operate infrastructures and websites? First of all, is there regulation to fight these famous crimes? Let's take Equifax Canada as an example. It created a major personal information security issue for millions of people. What type of regulation is in place for these businesses, in order to lighten your workload where there are no safeguards?

[*English*]

Mr. Hatfield: I would say when there's a sharp distinction between regulatory requirements that we place on companies and standards and technologies available to them. Cybersecurity is a very well-developed field. The top 20 things you should do to your network to make sure it is secure largely haven't changed in the last 20 years. We are still trying to get people to change their passwords on a regular basis and not having great success any more than we did 20 years ago. But the basics are very well known.The expertise is there. There are extremely skilled companies with great resources available to them that can assist companies across Canada.

Changing that from a standard or best practice or available expertise to a mandated regulation is a separate question. Public Safety Canada is not a regulatory agency. I would encourage you to ask regulators in the financial sector precisely what regulations they impose on companies of this type.

Mr. Doran: In the case of the financial sector, of course, the information that is being stolen was on a paper file 20 or 25 years ago. They're using the cyberworld to enable their business, period.

To put regulations around that — security regulations, perhaps, and it's certainly not our area and I don't want to espouse regulations one way or the other, but I will say that we have, generally speaking, a very good relationship with the Canadian financial institutions, and they cooperate with us and we cooperate with them, and it's in all of our best interests to ensure the integrity of that particular infrastructure.

des difficultés auxquelles nous sommes confrontés lorsqu'il s'agit de l'évolution de la menace.

[*Français*]

La sénatrice Moncion : Je vous remercie de votre présentation. J'ai travaillé dans le milieu financier et je sais qu'il a toujours été assez bien protégé justement parce que des sommes d'argent importantes peuvent être perdues. Vous avez beaucoup parlé d'infrastructures. Quel genre de réglementation est mis en place pour aider à réduire le nombre d'investigations pour les entreprises qui opèrent des infrastructures et des sites? Tout d'abord, une telle réglementation existe-t-elle pour lutter contre ces fameux crimes? Prenons l'exemple d'Equifax Canada. Elle a créé un problème majeur sur le plan de la sécurité de l'information personnelle de millions de personnes. Quel genre de réglementation est instaurée par rapport à ces entreprises pour alléger votre charge de travail là où il n'y a pas de pare-feu?

[*Traduction*]

M. Hatfield : Je dirais qu'il faut faire une nette distinction entre les exigences réglementaires que doivent respecter les entreprises et les normes et les technologies qui sont à leur disposition. La cybersécurité est un domaine très bien conçu. Les 20 mesures les plus importantes à prendre pour s'assurer que le réseau est sécuritaire n'ont pas changé au cours des deux dernières décennies. Nous essayons toujours d'inciter les gens à changer leurs mots de passe régulièrement et nous n'y arrivons pas davantage qu'il y a 20 ans. Or, les éléments essentiels sont très bien connus. Les compétences ne manquent pas. Des acteurs extrêmement compétents ont accès à de très bonnes ressources et peuvent aider des entreprises partout au pays.

Pour ce qui est du passage d'une norme ou d'une pratique exemplaire à une réglementation, c'est une question distincte. Sécurité publique Canada n'est pas un organisme de réglementation. Je vous encourage à demander aux organismes de réglementation du secteur financier quels règlements ils imposent à ce genre d'entreprises.

M. Doran : Dans le cas du secteur financier, bien entendu, les renseignements qui sont volés figuraient sur un dossier papier il y a 20 ou 25 ans. On se sert du monde virtuel pour mener des activités, un point c'est tout.

Concernant la réglementation à cet égard — des règlements sur la sécurité, peut-être, et puisque ce n'est pas notre secteur, je ne veux pas trancher sur les des règlements à adopter de quelle que façon que ce soit —, je dirais qu'en général, nous avons de très bonnes relations avec les institutions financières canadiennes, qu'elles collaborent avec nous et vice versa, et que nous avons tous intérêt à veiller à l'intégrité de cette infrastructure.

Senator Moncion: I agree with you, but there is now a concern about open banking, and the federal government is looking at opening the networks between banks. How are we going to work around that?

Mr. Doran: I'm not that familiar with the open banking concept. I will say, from a police investigative pursuit point of view, of course, that will make things more complicated, as are the virtual currencies that currently exist, and the emerging new cryptocurrencies that seem to be popping up on a regular basis.

It's all more complicated. To the earlier point, is it IT? We all said, no, it's not IT, but I don't want to diminish the importance that exists with the advances in IT. You can imagine how difficult it is to keep up. For every tablet in this room, we need to figure out a way to get into it, or try to, and that's just one facet of one technology.

It is an enormous task from an investigative perspective. As far as the open banking goes, absolutely, it will bring challenges, and hopefully challenges that we can deal with collectively.

[*Translation*]

Senator Carignan: I listened to you, and you said that cybercrime costs several hundred million dollars. It may in fact be several hundred billion dollars a year, according to the figures. I have the sense that the problem is so huge that we have lost control of it. This is a situation where individuals and businesses have to take their own security in hand by installing security software on their equipment or their own systems, because security services don't have the means to stop the crime or to punish the perpetrators. Am I mistaken? I would like to hear your comments, because I get the impression that we are in the virtual Far West, and that no one is safe anywhere. Law enforcement cannot ensure our security. We have to take charge of it ourselves by installing security on our equipment and our systems.

[*English*]

Mr. Doran: Adam, maybe you can speak to cybersecurity writ large, but it is obviously on a large scale, but I don't see this much different from putting door locks on your house. We have always had door locks. We have always had to protect ourselves unless you lived in the country and had the luxury of knowing all your neighbours and felt more secure. People will feel more or less secure depending on their personal experiences, and they will make the judgment whether they need more or less security.

La sénatrice Moncion : Je suis d'accord avec vous, mais le concept de « système bancaire ouvert » soulève des préoccupations, et le gouvernement fédéral envisage d'ouvrir les réseaux entre les banques. Comment allons-nous résoudre cela?

M. Doran : Je ne connais pas bien ce concept. Du point de vue des enquêtes policières, bien entendu, cela compliquerait les choses, tout comme c'est le cas actuellement pour les devises virtuelles et pour les nouvelles cryptomonnaies qui semblent apparaître de façon régulière.

Tout est plus complexe. Pour revenir à une question précédente, s'agit-il des TI? Nous avons tous dit que ce n'était pas le cas, mais je ne veux pas réduire l'importance des avancées en TI. Vous pouvez vous imaginer à quel point il est difficile de suivre le rythme. Pour chaque tablette dans cette pièce, nous devons trouver une façon de procéder, ou essayer de le faire, et ce n'est qu'un aspect d'une technologie.

Sur le plan des enquêtes, il s'agit d'une tâche énorme. En ce qui concerne le concept de système bancaire ouvert, oui, il y aura des difficultés, et il est à espérer que nous pourrons les surmonter collectivement.

[*Français*]

Le sénateur Carignan : Je vous écoute et vous dites que la cybercriminalité coûte plusieurs centaines de millions de dollars. Selon les chiffres, c'est peut-être même plusieurs centaines de milliards de dollars par année. J'ai l'impression que le problème est tellement immense qu'on a perdu le contrôle. On est dans une situation où les particuliers et les entreprises doivent prendre en main leur propre sécurité en prévoyant l'installation de dispositifs de sécurité sur leur équipement, sur leur propre système, parce que les services de sécurité n'ont plus les moyens de réprimer les infractions ni de punir les fraudeurs. Est-ce que je me trompe? J'aimerais entendre vos commentaires parce que j'ai l'impression qu'on est dans le *Far West* virtuel où on n'est pas en sécurité nulle part. Les forces de l'ordre ne sont pas en mesure d'assurer notre sécurité. On doit s'en charger nous-mêmes en prévoyant l'installation de dispositifs de sécurité sur nos équipements et nos systèmes.

[*Traduction*]

M. Doran : Adam, vous pourrez peut-être parler de la cybersécurité en général, mais c'est évidemment à une échelle très vaste. Or, je ne vois pas une très grande différence entre cette situation et le fait d'installer des serrures sur la porte de son domicile. Nous avons toujours verrouillé nos portes. Nous avons toujours dû nous protéger à moins de vivre en campagne et d'avoir le luxe de connaître tous nos voisins et de nous sentir en sécurité. Selon leurs expériences personnelles, les gens se sentiront plus en sécurité ou moins en sécurité et détermineront le niveau de protection dont ils ont besoin.

I don't think the concept of securing yourself is anything new, and I think people do have a responsibility to protect themselves online, as they would in their house and on the street, and be cautious in moving forward.

We are having an impact. To say the problem is out of control is — well, to be honest, I can't comment whether it's out of control. I feel the investigations we have are well in hand and we are controlling them and making advances, and we are putting people in jail. We are not, but the courts are, based on the evidence we've collected. I feel quite comfortable in that regard. Again, it's a scalable issue. Could we do more? Yes. Could people do more for their own security? Absolutely.

[*Translation*]

Senator Carignan: How many offences were reported, and how many people were convicted of cybercrime?

Mr. Doran: I can't give you an answer, because cybersecurity is the responsibility of all police forces in Canada, and so the statistics come from Toronto. I could not answer you.

Senator Carignan: And what of your own?

Mr. Doran: I can note the question and send you an answer later.

Senator Carignan: Do you see the dilemma? Where are we going to deploy our resources? Are we going to put more resources into police services that seem to have trouble flushing out the criminals, or should we give more resources to businesses, to financial services and to individuals, so that they may invest in their own independent protective devices?

Mr. Doran: Is that a question?

Senator Carignan: Yes.

[*English*]

Mr. Doran: It has to be a comprehensive approach. I don't think you can invest in one area alone and expect the problem to go away. There has to be a balanced approach. We do a lot of prevention work. We try and teach people to protect themselves, and we do investigations, and our colleagues do the same thing, except for the investigation parts, in government.

There has to be a comprehensive, multi-faceted approach to dealing with this issue.

L'idée d'assurer sa propre sécurité n'a rien de nouveau, et je pense que les gens ont la responsabilité de se protéger en ligne, comme ils le feraient à leur domicile et dans la rue, et d'agir avec prudence.

Nous avons un effet. Dire que l'on a perdu le contrôle… eh bien, pour être franc, je ne peux pas dire si c'est le cas. J'estime que pour ce qui est des enquêtes, nous avons les choses bien en main, que nous menons les enquêtes et que nous réalisons des progrès, et nous mettons des gens en prison. Ce n'est pas nous qui le faisons, mais bien les tribunaux, sur la base des éléments de preuve que nous recueillons. Je me sens très à l'aise à cet égard. Encore une fois, la cybercriminalité est de nature extensible. Pourrions-nous en faire davantage? Oui. Les gens pourraient-ils en faire plus pour assurer leur propre sécurité? Absolument.

[*Français*]

Le sénateur Carignan : Combien d'infractions ont été rapportées et combien de personnes ont été condamnées en cybercriminalité?

M. Doran : Je ne peux pas vous donner de réponse, parce que la cybersécurité est la responsabilité de tous les corps policiers au Canada. Donc, les statistiques proviennent de Toronto. Je ne saurais vous répondre.

Le sénateur Carignan : Les vôtres?

M. Doran : Je peux noter la question et vous donner une réponse plus tard.

Le sénateur Carignan : Voyez-vous le dilemme? Où allons-nous déployer nos ressources? Allons-nous mobiliser davantage nos ressources dans les services de police qui semblent avoir de la difficulté à débusquer les fraudeurs ou est-ce qu'on confie plus de ressources aux entreprises, aux services financiers, aux particuliers pour qu'ils investissent dans des systèmes de protection autonomes?

M. Doran : Est-ce une question?

Le sénateur Carignan : Oui.

[*Traduction*]

M. Doran : Il doit s'agir d'une démarche exhaustive. Je ne crois pas qu'on puisse investir dans un seul secteur et s'attendre à ce que le problème disparaisse. Il faut qu'une démarche équilibrée soit adoptée. Nous faisons beaucoup de travaux de prévention. Nous essayons de montrer aux gens comment se protéger, et nous menons des enquêtes, et nos collègues font la même chose, sauf pour ce qui est des enquêtes, au gouvernement.

Il faut qu'une démarche exhaustive et multidimensionnelle soit adoptée pour régler la question.

Mr. Flynn: We are being called upon by many of the technical resources in very capable cybersecurity units within the private sector to add the elements that police uniquely have with respect to judicial authorities, to go and attempt to remove the people who are committing these crimes from the system.

As Chief Superintendent Doran said, it is a balance of what they are able to do with the skills and authorities they have within the private sector, married with the authorities that are limited to police and other organizations to take action to augment that phenomenal capacity that exists today in the private sector.

Senator Ringuette: Thank you, gentlemen. I have to question what, from my perspective, is practical. The first is the case of Equifax where the personal data of 100,000 Canadians was gathered through cyber intrusion, and so we have a situation where there is a possible identity and financial theft for 100,000 Canadians. Who manages that file? Who investigates that file? Equifax says they are talking with those Canadians, informing them that their personal information was gathered, but there is an entire follow-up to that, more than an Equifax letter.What is the process that you do in such a situation?

Mr. Flynn: From the RCMP's perspective — and I'll speak in a general sense around a situation like that, just so I'm not going too deeply into an individual incident — when something like that occurs, particularly in a global fashion as did occur with Equifax, we collaborate closely with the other international law enforcement agencies that are responding. We are looking at where infrastructure is, where victims are and where potential actors are, and we work collaboratively with the law enforcement community around the world to try and target those individuals, determine who they are and prosecute them within the authority of the laws in whichever country they are acting or within Canada, if appropriate.

With respect to the victims and the long list of people whose identities were potentially compromised, we monitor what is occurring within that effort to make sure they are informed. However, our primary goal is to investigate it and ensure their privacy is protected as much as we can going forward.

The ability of the RCMP to take the list of hundreds of thousands or millions of individuals whose identity was potentially compromised is a very challenging feat for us, so we are very pleased when the private sector takes appropriate action and notifies people so that they are aware of what has occurred with their private information and can take appropriate action.

Senator Ringuette: There is more to this than the immediate follow-up. Within this case, Equifax shared with you the personal data that was stolen so that you know and you can work

M. Flynn : Bon nombre de ressources techniques dans les unités de cybersécurité du secteur privé très compétentes nous interpellent pour ce qui est de l'ajout des éléments que la police a concernant les autorités judiciaires, pour essayer de retirer du système les gens qui commettent ces crimes.

Comme l'a dit le surintendant principal, c'est un équilibre entre ce qu'ils sont capables de faire avec les compétences et les autorités du secteur privé, combiné aux pouvoirs qui sont limités à la police et à d'autres organismes pour prendre des mesures afin d'augmenter la capacité phénoménale qui existe aujourd'hui dans le secteur privé.

La sénatrice Ringuette : Merci, messieurs. Je me dois de poser des questions qui, de mon point de vue, sont d'ordre pratique. La première porte sur l'affaire Equifax; les données personnelles de 100 000 Canadiens ont été obtenues lors d'une cyberintrusion, de sorte que ces 100 000 Canadiens risquent maintenant d'être victimes de vol d'identité et d'argent. Qui gère ce dossier? Qui est chargé de l'enquête dans ce dossier? Equifax indique avoir communiqué avec ces Canadiens pour les informer que leurs renseignements personnels ont été divulgués, mais cela nécessite un suivi. Une lettre d'Equifax ne suffit pas. Comment procédez-vous dans de tels cas?

M. Flynn : Dans une telle situation, en particulier dans le cas d'un incident qui a une ampleur mondiale comme l'affaire Equifax, la GRC a l'habitude — de façon générale, afin de ne pas aller dans les détails d'un incident précis — de collaborer étroitement avec les autres organismes d'application de la loi internationaux qui interviennent dans le dossier. Nous cherchons à savoir où sont les infrastructures, les victimes et les auteurs potentiels. Nous collaborons avec les forces policières de partout dans le monde pour cibler ces individus, découvrir leur identité et les traduire en justice en vertu des lois du pays où ils ont mené leurs actions, ou des lois canadiennes, le cas échéant.

Quant aux victimes et aux nombreuses personnes dont l'identité est potentiellement compromise, nous surveillons les mesures qui sont prises pour veiller à ce qu'elles soient informées. Toutefois, notre objectif premier est d'enquêter sur l'incident et de nous assurer que leurs renseignements personnels seront protégés le mieux possible, à l'avenir.

Il est extrêmement difficile pour la GRC d'obtenir la liste des centaines de milliers ou même des millions de personnes dont l'identité a été potentiellement compromise. Nous sommes donc très heureux lorsque le secteur privé prend des mesures adéquates pour informer les gens d'un incident lié à leurs renseignements personnels pour qu'ils puissent prendre les mesures appropriées.

La sénatrice Ringuette : Ce n'est pas uniquement une question de suivi immédiat. Dans cette affaire, Equifax vous a communiqué les données personnelles qui ont été volées pour que vous soyez au courant et que vous puissiez travailler avec les

with the Canadians involved in this to help them protect themselves in regard to financial and identity theft.

When you talk about victims, there is also a proactive process that needs to be followed. Are you doing that?

Mr. Flynn: In many situations where private information was stolen by a cyber actor, individuals' information is not necessarily shared with police or other entities. That is still private information, and I would assume many would not want that information shared directly with police.

The information that police are given or to which police gain access through different judicial authority is the information necessary to gather evidence to hold to account the people who perpetrated the offence.

Senator Ringuette: So in other words, you have no knowledge of the victims.

Mr. Flynn: In many situations, we do not know the private information of all of the victims, that is correct.

Senator Ringuette: Wow.

Mr. Doran: You must understand that from an investigative perspective, not a policing perspective writ large, we don't necessarily need to know it to conduct our investigation. We are looking for the administrator, the infrastructure and the money. Those are our responsibilities.

However, to your other point about public awareness and letting potential victims become aware of the threats potentially related to them, we do that predominantly through the Canadian Anti-Fraud Centre, which is located in North Bay. They are responsible for receiving calls on fraud, scams and things of that nature and collecting the information and trying to develop an intelligence picture. They actually have a seniors' program where they will call seniors who have been victimized, give them information packages and tell them of the most recent frauds are so they are aware. They will do that coast to coast.

As far as there being a public awareness and prevention campaign, we do that as well, but Mr. Flynn is talking specifically about the investigative process. We are after the people behind the machines. With the victims, it's unfortunate, but Equifax is the primary victim. They're the ones we need to deal with, because they have the information we need on their systems to backtrack to where we need to get to.

Senator Ringuette: There is a loophole into this cycle, and the loophole is the victims that I find.

Canadiens touchés pour les aider à se protéger contre le vol d'identité et d'argent.

En ce qui a trait aux victimes, vous devez également mettre en place un processus proactif. Le faites-vous?

M. Flynn : Dans bien des cas, les informations personnelles sur les personnes touchées par un vol de renseignements personnels par un cybercriminel quelconque ne sont pas nécessairement communiquées aux services policiers ou à d'autres entités. Ces renseignements sont toujours confidentiels, et je vous assure que beaucoup de gens ne voudraient pas qu'ils soient communiqués directement aux services policiers.

Les informations qui sont fournies aux services policiers ou auxquelles ils ont accès par l'intermédiaire de diverses autorités judiciaires sont celles dont ils ont besoin pour recueillir les preuves nécessaires pour traduire les auteurs en justice.

La sénatrice Ringuette : Donc, autrement dit, vous ne connaissez pas l'identité des victimes.

M. Flynn : En effet, dans bien des cas, nous n'avons pas les informations personnelles sur toutes les victimes.

La sénatrice Ringuette : Wow.

M. Doran : Vous devez comprendre que du point de vue des enquêtes, et non du point de vue de l'application de la loi en général, nous n'avons pas nécessairement besoin de ces renseignements pour mener notre enquête, qui porte sur l'administrateur, l'infrastructure et l'argent. Voilà notre mandat.

Toutefois, concernant l'autre point que vous avez soulevé, la sensibilisation du public et des victimes potentielles sur les menaces qui pourraient les toucher, nos activités en ce sens se font principalement par l'intermédiaire du Centre antifraude du Canada, qui est situé à North Bay. Le centre reçoit les appels de signalement des fraudes, des escroqueries et des choses de ce genre; il recueille ces informations et tente d'établir un tableau d'ensemble de la situation. Le centre a un programme destiné aux aînés qui sert à communiquer avec les aînés qui ont été victimes afin de leur fournir des trousses d'information et de les renseigner sur les nouvelles tendances en matière de fraude. Ces activités se font à l'échelle nationale.

Nous menons également une campagne de sensibilisation et de prévention, mais M. Flynn parle plus précisément du processus d'enquête. Nous recherchons les auteurs, ceux qui sont derrière les ordinateurs. En ce qui concerne les victimes, c'est malheureux, mais la victime principale, c'est Equifax. C'est sur cette société que nous devons nous concentrer, car c'est elle qui détient, dans ses systèmes, les informations dont nous avons besoin pour remonter à la source du problème.

La sénatrice Ringuette : Il y a une faille dans ce cycle: les victimes.

Chair, may I go with my other practical question?

The Deputy Chair: We will put you down for your other question for round two. Have you finished your first question?

Senator Ringuette: We need to acknowledge that in the current spectrum of protection from cyberattacks, there is no real mechanism in place for the victims of cyberattack.

The Deputy Chair: We can get into that more on round two. It will give them a chance to think about it.

[*Translation*]

Senator Massicotte: Thank you for appearing before our committee. First, I am trying to understand the scope of the problem. You say, Mr. Doran, that we lack resources to react. I feel like I am on the telephone with a representative from HP or Microsoft who is trying to explain to me how to operate my computer, and I have trouble understanding the gist of what he is saying to me.

I'd like to do a little exercise with you. Suppose you had two minutes with the Prime Minister of Canada and the provincial premiers to explain the importance and seriousness of the problem, and to talk about your budgets and the regulations you need in order to do very good work. I feel we are facing a very big problem and that we are in a race with criminals, and at this point, I wonder if they are not winning the race. I'd like you to give us an overview of what you need. Is this a major, significant issue? I think it is very important.

[*English*]

Mr. Doran: The problem is important. I would have to get back to you on the scale of the cybercrime-enabled losses versus what the losses were before cybercrime existed. Clearly, they would have increased, but I'm not comfortable saying they have increased exponentially to the point where the problem is out of control, as your colleague mentioned earlier.

More public awareness? Absolutely. Having people secure themselves? Absolutely. Having people be aware of the various scams and attacks that happen is very important. It is being done. Can we do it more? Probably.

Investigations, per se — at the end of day, that may become a policy decision on what is reasonable to go after and what is too much as far as — we're never going to eliminate it entirely.

Monsieur le président, puis-je poser mon autre question d'ordre pratique?

Le vice-président : Nous allons inscrire votre nom pour le deuxième tour pour que vous puissiez poser votre autre question. En avez-vous terminé avec la première?

La sénatrice Ringuette : Nous devons reconnaître que l'actuel éventail de mesures de protection contre les cyberattaques ne comprend aucun mécanisme réel pour les victimes.

Le vice-président : Nous pourrons aborder cet aspect de façon plus approfondie pendant le deuxième tour. Cela leur donnera l'occasion d'y réfléchir.

[*Français*]

Le sénateur Massicotte : Merci de comparaître devant notre comité. J'essaie de comprendre, au départ, l'envergure du problème. Vous dites, monsieur Doran, qu'on manque de ressources pour réagir. J'ai l'impression d'être au téléphone avec un représentant de HP ou de Microsoft qui tente de m'expliquer comment opérer mon ordinateur et j'ai de la difficulté à comprendre l'essence de ce qu'il me dit.

J'aimerais faire un petit exercice avec vous. Disons que vous disposiez de deux minutes avec le premier ministre du Canada et les premiers ministres des provinces pour leur expliquer l'importance et la sévérité du problème, et pour leur faire part du budget et des règlements dont vous avez besoin pour faire un très bon travail. J'ai l'impression que nous sommes devant un gros problème, que nous sommes engagés dans une course avec des bandits, et, à ce point-ci, je me demande si ce n'est pas eux qui la gagnent. J'aimerais que vous nous donniez un aperçu de ce dont vous avez besoin. Le problème est-il majeur, est-il important? Je pense qu'il est très important.

[*Traduction*]

M. Doran : Le problème est important. Pour ce qui est de l'ampleur des pertes liées à la cybercriminalité comparativement aux pertes qu'on observait avant que cela n'existe, je devrai vous revenir là-dessus. De toute évidence, cela a augmenté, mais je ne suis pas prêt à dire que cela a augmenté exponentiellement au point de devenir incontrôlable, comme votre collègue l'a mentionné plus tôt.

Faut-il sensibiliser davantage le public? Absolument. Faut-il inciter les gens à prendre des précautions? Absolument. Il est extrêmement important d'informer les gens sur les diverses escroqueries et attaques qui se produisent. Nous le faisons. Pouvons-nous en faire davantage? Probablement.

Quant aux enquêtes comme telles... En fin de compte, cela pourrait devenir une décision de politique sur le caractère raisonnable d'une enquête et sur ce qui va trop loin. Nous ne parviendrons jamais à éliminer cela totalement.

Senator Massicotte: I'm hearing it's another problem among many others you have, it doesn't deserve any particular attention or additional monies, and it is run of the mill. Is that the right impression?

Mr. Doran: No, it's a problem we're extremely concerned about. It's an evolving issue that evolves as quickly as the technology is evolving and as quickly as people can get their hands on and become bad with the technology.

It's not a small problem; it's a significant problem. I just can't tell you compared to organized crime and other criminality how much bigger it is, but I would say it is definitely bigger than it was.

Senator Massicotte: I have a fear — and you can respond — that you don't know what you don't know. So you are talking about things you have seen. I am concerned that this thing is huge, and I bet you a lot of old people respond to those emails, lose a lot of money, and never report to their kids, to you or local police. They are so good at it. How do you know what you don't know? I suspect what you don't know might be a lot.

Mr. Doran: We think there is a significant under-reporting problem. I completely support that proposal. I also think under-reporting is an issue that has existed for every type of crime we've known about, whether it's break and enters or others. We know sexual assaults are under-reported and so on. That's a pervasive issue when you are investigating crime.

That said, are reporting efforts getting people to report more? Yes. Our cybersecurity strategy involves that. The government writ large is trying to get people to report more, to get a better picture of what is going on. You are right that we don't have an absolutely clear picture, but we have a picture of what we know and we don't have a picture of what we don't know. We can estimate. I think the Canadian Anti-Fraud Centre estimates that the under-reporting is well over 50 per cent.

Senator Massicotte: As a Canadian citizen, given that it's like a competition, the bandits have a lot of money and they can hire the best computer hacker. Your team has limited funds. I hope you win. It's important stuff.

Mr. Doran: In fairness, we've never solved all crime. We try and solve enough to keep good people good and keep things rolling the way they should be in our communities so that people

Le sénateur Massicotte : Ce que j'entends, c'est qu'il s'agit d'un problème parmi tant d'autres qui ne nécessite pas une attention particulière ou des ressources financières supplémentaires, que c'est un problème ordinaire. Est-ce la bonne impression?

M. Doran : Non; c'est un problème qui nous préoccupe énormément. C'est un problème grandissant qui évolue aussi rapidement que la technologie et l'accès à la technologie par des gens qui souhaitent l'utiliser à mauvais escient.

Le problème n'est pas mineur; il est majeur. Je ne peux tout simplement pas vous donner un ordre de grandeur comparativement au crime organisé ou à d'autres activités criminelles, mais je dirais que cela a certainement pris de l'ampleur.

Le sénateur Massicotte : Ce que je crains — et vous pouvez répondre —, c'est que nul n'est conscient de ce qu'il ignore. Donc, vous parlez de choses dont vous êtes au courant. Ce qui me préoccupe, c'est l'ampleur de ce phénomène, et je suis prêt à parier que beaucoup de personnes âgées répondent à ces courriels, perdent beaucoup d'argent et ne le signalent jamais, que ce soit à leurs enfants, à vous, ou à la police locale. Les criminels sont si habiles. Que savez-vous de ce qui ne vous est pas signalé? Pas grand-chose, je suppose.

M. Doran : Nous considérons que la sous-déclaration est un problème important. Je suis tout à fait d'accord avec vous là-dessus. Je pense aussi que la sous-déclaration est un problème pour toutes les formes de crimes connus, notamment les introductions par effraction. Nous savons d'ailleurs que c'est le cas pour les agressions sexuelles, et cetera. C'est un problème récurrent dans les enquêtes sur les crimes.

Cela dit, la question est de savoir si les efforts que nous menons en ce sens incitent plus de gens à signaler les incidents. La réponse est oui. Cela fait partie de notre stratégie en matière de cybersécurité. Le gouvernement en général tente d'inciter les gens à signaler les cas davantage pour avoir une meilleure vue d'ensemble de la situation. Vous avez raison de dire que nous n'en avons pas une idée absolument précise. Nous avons un portrait général; on ne peut savoir ce qu'on ignore, mais nous pouvons faire des projections. Je crois savoir que le Centre antifraude du Canada estime que le taux de sous-déclaration se situe bien au-delà de 50 p. 100.

Le sénateur Massicotte : Je dirais, en tant que citoyen canadien, étant donné que cela semble être une compétition, que les malfaiteurs ont beaucoup d'argent et qu'ils peuvent embaucher les meilleurs pirates informatiques, tandis que votre équipe a des fonds limités. J'espère que vous gagnerez. C'est un enjeu important.

M. Doran : Soyons francs: nous n'avons jamais réussi à résoudre tous les crimes. Nous faisons notre possible pour résoudre un nombre suffisant de cas, pour protéger les gens bien

can feel safe. I think we are accomplishing that. But we are under no illusion that we are going to stop cybercrime or crime at large.

Senator Unger: Thank you for your presentations. I would like to add another problem, or maybe it's many problems, I'm not sure.

You're probably aware that at a university in Belgium, an announcement was made that hackers have discovered a way to completely defeat the encryption that WPA2 provides on Wi-Fi networks. It is serious, of course. It affects all modern Wi-Fi equipment from mobile phones, tablets, workstations, routers, printers and the usual suspects. Would any of you like to comment about this? How do we even begin to ensure cybersecurity when vulnerabilities like this are possible?

Mr. Hatfield: That particular issue was actually identified by the technology community at least the early part of this year. Many manufacturers have already issued fixes and patches to mitigate the problem with their equipment.

What we see generally when this kind of thing is discovered — and it is discovered, no one can build a perfect system so there are always flaws — is the technological community and the international, global community of cyberexperts tend to respond extremely quickly.

This particular issue within the Government of Canada, when the announcement came out, many questions were asked. Our IT people were well aware and already on it.

I would recommend the technical lead for cybersecurity technology issues of that type is the Communication Security Establishment. They would be able to speak to that question in detail.

Senator Unger: Mr. Hatfield, you said we are world leaders when it comes to cybercrimes and cybersecurity. How do we compare to the U.S.A.? From the cyber review that was done, there was a call for increased government leadership on this. What would that be?

Mr. Hatfield: In terms of how we compare to the United States or other partners, we spend a great deal of time — myself and my organization within the cybersecurity policy domain and I know my counterparts in their respective domains — talking to international counterparts. We ask, "What are you doing? How

et pour assurer le bon fonctionnement de nos collectivités afin que la population se sente en sécurité. Je pense que nous y parvenons. Toutefois, nous n'allons pas jusqu'à croire que nous pourrons complètement éliminer la cybercriminalité ou la criminalité en général.

La sénatrice Unger : Merci de vos exposés. J'aimerais soulever un autre problème, ou peut-être plusieurs; je n'en suis pas certaine.

Vous savez probablement qu'il a récemment été annoncé, dans une université belge, que les pirates informatiques ont découvert comment percer le chiffrement WPA2 utilisé pour les réseaux sans fil. C'est un problème grave, évidemment, puisqu'il touche tous les appareils modernes, notamment les téléphones cellulaires, les tablettes, les postes de travail, les routeurs, les imprimantes, et cetera. L'un d'entre vous aurait-il des commentaires à ce sujet? Comment pouvons-nous commencer à assurer la cybersécurité, alors que de telles vulnérabilités sont possibles?

M. Hatfield : Je précise que ce problème a été découvert par les acteurs du secteur des technologies au début de l'année. De nombreux fabricants ont déjà créé des correctifs et des rustines pour atténuer le problème pour leurs appareils.

En général, lorsque les problèmes de ce genre sont découverts — ils sont bel et bien découverts, puisqu'il existe toujours des failles, étant donné qu'il est impossible de concevoir un système parfait —, les acteurs du milieu des technologies et les spécialistes internationaux de la cybersécurité tendent à réagir extrêmement rapidement.

Lorsque l'annonce sur ce problème précis a été faite, beaucoup de questions ont été soulevées au gouvernement du Canada. Nos spécialistes des technologies de l'information étaient au courant et s'attaquaient déjà au problème.

Je dirais que les gens du Centre de la sécurité des télécommunications seraient les mieux placés pour traiter des aspects techniques des solutions technologiques en matière de cybersécurité. Ils seraient capables de répondre à cette question de façon détaillée.

La sénatrice Unger : Monsieur Hatfield, vous avez indiqué que nous sommes des chefs de file mondiaux de la cybersécurité et de la lutte contre la cybercriminalité. Comment le Canada se compare-t-il aux États-Unis? Dans l'examen de la cybersécurité, on demande au gouvernement de faire preuve d'un leadership accru à cet égard. En quoi cela consistera-t-il?

M. Hatfield : Pour ce qui est d'une comparaison aux États-Unis ou à d'autres partenaires, nous consacrons beaucoup de temps aux discussions avec nos homologues internationaux. Je parle de moi-même et de mon organisation pour ce qui est des politiques en matière de cybersécurité, et de mes homologues, dans leurs domaines de compétence respectifs. Nous leur

are you addressing this problem? ”The answer we usually get is, “That’s a really good question. What are you doing?”

We have found we are very much at par with international allies in terms of understanding the problem and the kind of initiatives we are putting forward to deal with these things. Everyone on the planet is using the same IP protocol on computers. We all have the same Apple iPhone designed in California. We all are dealing with the same technological issues. We are at par if not leading in many areas with respect to cybersecurity. In some niche areas, for example quantum computing, Canada is breaking ground globally.

The cyber review has been running over the past two years and its purpose is to elicit a wide access across Canada and what the next step for government should be. All of that input is being used to find a new way forward for government.

Senator Unger: Lastly, should we be worried about Russia?

The Deputy Chair: Did you expect an answer to that or are you just putting it out there?

Senator Unger: If anyone wants to answer, please do. If you don’t, that’s okay.

The Deputy Chair: We should be worried about everybody.

Senator Unger: I am thinking specifically about the Senate inquiry in the United States. They have some interesting issues to deal with that they are trying to get to the bottom of and I’m wondering if we should have those concerns as well?

Mr. Doran: That question is out of our purview. However, when it comes to cybersecurity and cybercrime, I would worry about a lot of people in a lot of different countries.

Senator Campbell: Thank you for coming today.

When I push the print button, I’m amazed that a machine across the room spits something out. That’s my level of this.

My concern isn’t about Equifax. My concern isn’t about elderly people being ripped off. I’m obviously concerned about it, but that has taken place forever. I was a Mountie at one time and we dealt with it differently.

I’m concerned about the threat where we have the super imposition of organized crime, foreign governments and terrorism all wrapped up in the same ball of wax. When I look

demandons: « Que faites-vous? Comment réglez-vous ce problème? » On nous répond actuellement: « C’est une excellente question. Qu’en est-il de votre côté? »

Nous avons constaté que nous nous comparons très bien avec nos alliés internationaux quant à notre compréhension des enjeux et des mesures que nous mettons en œuvre pour les régler. Tous les ordinateurs de la planète utilisent le même protocole IP, et nous utilisons tous un iPhone d’Apple conçu en Californie. Nous avons tous les mêmes problèmes technologiques. Pour bien des aspects liés à la cybersécurité, nous sommes sur un pied d’égalité, voire en avance. Dans certains créneaux, comme l’informatique quantique, le Canada est un précurseur sur la scène internationale.

L’examen de la cybersécurité, en cours depuis deux ans, vise à favoriser un accès élargi à l’échelle du pays et à déterminer les prochaines étapes pour le gouvernement. Toutes les informations recueillies servent à redéfinir les orientations du gouvernement.

La sénatrice Unger : Enfin, la Russie devrait-elle être une préoccupation?

Le vice-président : Attendez-vous une réponse à cette question, ou faites-vous simplement la lancer, comme cela?

La sénatrice Unger : J’invite toute personne qui souhaite y répondre de le faire. Sinon, cela ne pose pas problème.

Le vice-président : Nous devrions nous préoccuper de tout le monde.

La sénatrice Unger : Je pense en particulier à l’enquête du Sénat aux États-Unis. On tente de trouver des réponses à des enjeux forts intéressants, et je me demandais si nous devrions avoir ces mêmes préoccupations.

M. Doran : Cette question est hors de notre champ de compétence. Toutefois, en ce qui concerne l’aspect sécurité et la cybercriminalité, je serais préoccupé par beaucoup de gens dans de nombreux pays.

Le sénateur Campbell : Merci d’être venus aujourd’hui.

Lorsque j’appuie sur le bouton d’impression, je m’étonne toujours de voir qu’une machine de l’autre côté de la pièce imprime quelque chose. Voilà mon niveau d’expertise à cet égard.

Mes préoccupations ne portent pas sur Equifax. Elles ne portent pas non plus sur les personnes âgées qui se font arnaquer. Cela me préoccupe, évidemment, mais ces problèmes existent depuis toujours. J’ai déjà été membre de la GRC, et nous réglions les problèmes autrement.

Ce qui me préoccupe, ce sont les menaces d’une grande complexité où se superposent, en une sorte d’amalgame, le crime organisé, les gouvernements étrangers et le terrorisme. Lorsque

here and I see three or four or five different agencies, plus the private sector who all have a responsibility in it, I worry about how we've organized that, whether we are in a position for the rapid deployment of it. I would worry about finding out that we have no electricity. For instance, is WikiLeaks criminal? I don't know, but it seems to be. I believe you can get into anything you want. There is not a system built that someone can't get into.

How do you coordinate at our level when all of these come together? We know that they all come together. People sell drugs which gets money that then goes to terrorism or to foreign governments that have no trade with the world. How do we deal with that when we come upon it?

Mr. Hatfield: The coordination question is an excellent one. It's an old saying in cybersecurity that it is everyone's problem and everyone has a role to play. The Government of Canada has looked to Public Safety Canada to coordinate cybersecurity policy writ large across government. We do have mechanisms in place where multiple government departments regularly come together. I could probably name 14 that are regularly engaged in cybersecurity matters, be it law enforcement, national security, intelligence, protection of critical infrastructure, foreign affairs issues, financial issues, et cetera. There is a very deep understanding of the requirement to coordinate and to ensure that the many facets of cybersecurity are being addressed in a holistic way.

It is true that specific agencies have specific mandates, roles and responsibilities. That also applies to the private sector.

Everyone does have a role to play. Your own system, your own information and intellectual property, no one cares about it more than you do. The private sector and citizens do have a responsibility to educate themselves and to use what they buy in a safe way.

The engineer can put the seat belt in a car, but you have to put it on every time you get in the car. We have learned to do that and accepted that as part of using a car safely.

The coordination is absolutely there. As was noted earlier, the need for more government leadership and clear leadership on this issue was a strong theme that came out in the cyber review. Another strong theme was concerns about cybercrime. All of

je regarde ce qui se passe ici et que je vois trois, quatre ou cinq organismes différents, auxquels s'ajoutent des acteurs du secteur privé, qui jouent tous un rôle dans ce domaine, je me préoccupe de la façon dont nous avons organisé tout cela et je me demande si nous avons la capacité d'intervenir rapidement. Je serais préoccupé de constater que nous n'avons plus d'électricité. Par exemple, WikiLeaks est-elle une organisation criminelle? Je ne sais pas, mais il semble que ce soit le cas. Je pense qu'il est possible d'avoir accès à tout ce qu'on veut. Il n'existe aucun système auquel on ne peut avoir accès.

Comment coordonnez-vous les activités à notre niveau lorsque tous ces facteurs entrent en jeu? Nous savons que tout se recoupe. Des gens vendent des drogues, ce qui rapporte de l'argent, puis cet argent sert à financer le terrorisme ou est envoyé à des gouvernements étrangers qui n'entretiennent aucune relation commerciale avec le reste du monde. Comment réagissons-nous, dans de tels cas?

M. Hatfield : Votre question sur la coordination est une excellente question. Dans notre domaine, on dit souvent que la cybersécurité est l'affaire de tout le monde et que tous ont un rôle à jouer. Le gouvernement canadien a chargé Sécurité publique Canada de la coordination des politiques en matière de sécurité à l'échelle gouvernementale. Nous avons mis en place des mécanismes qui favorisent les échanges réguliers entre les responsables de divers ministères. Je pourrais certainement nommer 14 ministères qui jouent un rôle actif pour divers enjeux de cybersécurité, notamment l'application de la loi, la sécurité nationale, le renseignement, la protection des infrastructures essentielles, les affaires étrangères, les enjeux financiers, et cetera. Il existe dans notre milieu une compréhension profonde de la nécessité d'une action concertée et de veiller à la prise en compte des divers aspects de la cybersécurité dans une perspective globale.

Il est vrai que les divers organismes ont chacun des mandats, des responsabilités et des rôles précis. Cela vaut aussi pour le secteur privé.

Tout le monde a un rôle à jouer. Personne ne se préoccupe davantage que vous de vos systèmes, de vos propres informations et de votre propriété actuelle. Il incombe aux acteurs du secteur privé et aux particuliers de s'informer et d'utiliser l'équipement qu'ils achètent de façon sécuritaire.

Un ingénieur peut installer une ceinture de sécurité dans une voiture, mais vous devez tout de même mettre votre ceinture de sécurité lorsque vous montez à bord. Nous avons appris à le faire et nous convenons tous que cela fait partie de l'usage sécuritaire d'un véhicule.

La coordination est bien réelle. Comme cela a été indiqué plus tôt, la nécessité que le gouvernement exerce une direction accrue et claire sur cet enjeu a été un thème récurrent de l'examen de la cybersécurité. Un autre thème important était celui des préoccupations relatives à la cybercriminalité. Tous ces enjeux

those issues are being examined right now; a new way forward is being looked at.

Senator Campbell: How do you do that when things change so quickly? How do you keep out in front of this? I'm not asking about the investigational techniques. Every day we read that somebody's discovered this or been able to do that. There are people who spend their lives trying to break into things just for the hell of it, just to be able to get inside there. How do we deal with that with technology changing so quickly? Do we ever get ahead of it, or are we always on the trailing edge?

Mr. Hatfield: Something that we have observed is exactly what you've described, there's always a news item about there's been another attack, another breach, some other hacker has accomplished something. I feel it is very easy to lose sight of whether there are unfathomable amounts of innovation that have occurred across the globe because of digital technology and the Internet. Every year that has gone by has seen more hacks than the year before, but every year that has gone by has seen more commerce done over the Internet and more users and activity on the Internet. Canada leads the world in per capita usage of computers and Internet time.

The negative headlines are easy to see, and it's easy to look at the numbers that always seem to go up, but all of the positive numbers are also going up. The benefits we receive from the Internet, we don't notice them so much, but this particular presentation is being webcast. That would not have occurred 10 years ago, but today it is, and we don't even think twice about it.

It is easy to see only the negative. As part of our cyber review, the reason we asked those questions was to say to Canadians, "How bad is this problem really, and what is the right next step for Canada?" That is the work being done now to put forward a new strategy.

Senator Black: I would like to build on the excellent questions my colleagues have been asking you, but, first of all, I want to thank you all for being here but more importantly for your service to Canada. You're doing important work. We rely on it, and we know, in large part, it must be successful because we haven't heard a lot of things from you. I'm glad about that.

I liken what we've heard today to a hockey game. You're the good guys, and there's a team of bad guys. I'm sitting in the stands watching the play move back and forth. Are the good guys or the bad guys winning this game? It's a general, high-level way to put what I'm hearing. Who is winning?

sont actuellement étudiés, et une nouvelle politique est en préparation.

Le sénateur Campbell : Comment y parvenez-vous quand les choses évoluent aussi rapidement? Comment réussissez-vous à prendre les devants? Je ne vous interroge pas sur les techniques d'enquête. Chaque jour, on apprend que quelqu'un a fait une découverte ou a réussi à faire quelque chose. Certaines personnes passent leur vie à tenter de percer les mesures de sécurité pour le simple plaisir de la chose. Comment contrer cette menace, compte tenu de l'évolution rapide de la technologie? Réussissez-vous à devancer cette évolution ou tirez-vous toujours de l'arrière?

M. Hatfield : Tout comme vous, nous avons constaté qu'il arrive toujours quelque chose de nouveau, qu'une autre attaque ou une autre violation est survenue, ou qu'un autre pirate a accompli quelque chose. J'ai l'impression qu'on peut aisément perdre de vue le fait qu'une quantité inimaginable d'innovations ont vu le jour dans le monde grâce à la technologie numérique et à Internet. Chaque année, le nombre d'actes de piratage augmente, mais il y a aussi plus de commerce en ligne et d'activités et de gens sur Internet. Le Canada fait figure de chef de file mondial au chapitre de l'utilisation des ordinateurs et du temps passé sur Internet par habitant.

Il est facile de voir les mauvaises nouvelles à la une et de constater que les chiffres semblent croître sans cesse, mais les bons chiffres augmentent aussi. Nous ne remarquons pas tellement les avantages que nous tirons d'Internet, mais je ferais remarquer que la présente séance est diffusée sur le Web. Cela n'aurait pas été possible il y a 10 ans, mais aujourd'hui, on n'y pense même pas deux fois.

Il est facile de ne voir que le négatif. Si nous avons posé certaines questions dans le cadre de notre examen de la cybersécurité, c'est pour demander à la population son avis sur la gravité du problème et sur les mesures qu'il conviendrait de prendre au pays. Voilà ce que nous faisons actuellement en vue de proposer une nouvelle stratégie.

Le sénateur Black : Je voudrais donner suite aux excellentes questions que mes collègues vous ont posées, mais tout d'abord, je tiens à vous remercier de témoigner et, surtout, de servir le Canada. Vous accomplissez un travail important, dont nous sommes tributaires, et nous savons qu'il doit porter fruit en grande partie, car nous n'avons pas beaucoup de nouvelles de votre part. J'en suis ravi.

Je comparerais ce que nous avons entendu aujourd'hui à une partie de hockey. Vous êtes les bons, et les pirates forment l'équipe des méchants. Assis dans les gradins, je suis la partie. Qui, des bons et des méchants, gagne la partie? C'est une manière générale de présenter ce que je comprends. Qui l'emporte?

Mr. Doran: One of your colleagues mentioned earlier we may not know what we don't know. In the game we're playing, we're doing pretty well, I would say, from what I know. But I would also point out that as the game and season evolves, and as the year turns into another year and a different game, we have a new generation of good and bad players coming up.

The bad players are what we're trying to deal with now. We have a bunch of young hockey players who are just as smart and just as switched on as the bad guys. They are keeping pace. The things we don't know, however, that's the ringuette game going on at the next rink, and we're not sure what's going on over there.

Senator Black: I assume, though, from what you have said that we also have pretty good scouts out there trying to understand the game. I would assume that when North Korea hacks Bangladesh's national bank, you figure out what's gone on there and adjust your game plan. That would be a fair assumption, I would imagine.

Mr. Doran: Yes.

Senator Black: Can you tell us what your obstacles are? Give us your three obstacles to continuing to win the game. We're having these hearings because we want to be helpful to this cause.

Mr. Flynn: One of the most significant issues we're having is around having better coordination with all of our other partners. We're undertaking to do that better. We're undertaking to work better with local police.

I will tell you that, as you have four of us sitting here from three different organizations, this is not the first time that we have all sat at the same table. The one distinct element of what we're doing around cyber, the seriousness that we're all applying to it, is that we have a collaborative relationship with all the government departments engaged in cyber. We've moved far beyond any competitive element of whose mandate is this and that and where is the overlap. Whenever we see elements of overlap, we look at that as an opportunity and a very good thing of where we can work together and make things much better.

Anything we can do to improve the coordination and collaboration, better communication with the public in raising the awareness and skills of the individuals that we require to target this crime, we welcome those things.

Senator Black: Obstacle one, coordination, although you say you work well together, but it's still an ongoing challenge. Other obstacles?

M. Doran : Un de vos collègues a indiqué plus tôt qu'on ignore peut-être ce qu'on ne sait pas. Dans le jeu auquel nous jouons, nous faisons, à ce que je sache, assez bonne figure. Sachez toutefois que le jeu et la saison évoluent, et qu'au fil du temps, nous voyons arriver une nouvelle génération de bons et de mauvais joueurs.

À l'heure actuelle, nous tentons de nous attaquer aux mauvais joueurs. Nous disposons d'une équipe de jeunes hockeyeurs qui sont tout aussi doués que les mauvais joueurs, et ils gardent le rythme. Par contre, une partie de ringuette est en cours sur la patinoire voisine, et nous ignorons ce qu'il s'y passe.

Le sénateur Black : D'après ce que vous nous avez dit, cependant, je présume que nous pouvons aussi compter sur de bons éclaireurs qui tentent de comprendre la partie. Je suppose que quand la Corée du Nord pirate les systèmes de la banque nationale du Bangladesh, vous déterminez ce qu'il s'est passé et adaptez votre plan de match en conséquence. J'imagine que ce serait une présomption juste.

M. Doran : Oui.

Le sénateur Black : Pouvez-vous nous indiquer quels sont les obstacles? Nommez-nous-en trois qui vous empêchent de continuer de gagner la partie. Nous tenons ces séances pour aider cette cause.

M. Flynn : Le principal problème, c'est que nous devons assurer une meilleure coordination avec nos autres partenaires. Nous déployons des efforts en ce sens afin de mieux collaborer avec les corps de police locaux.

Quatre d'entre nous, représentant trois organisations différentes, comparaissent devant vous, et sachez que ce n'est pas la première fois que nous sommes réunis à la même table. Ce qui est remarquable dans les activités que nous mettons en œuvre pour assurer la cybersécurité et le sérieux que nous accordons à la question, c'est que nous avons une relation de collaboration avec tous les ministères concernés. Nous faisons fi de tout élément de concurrence quant aux mandats et aux chevauchements des responsabilités. Lorsque nos mandats se chevauchent, nous considérons cela comme une occasion et une excellente chose, car nous pouvons travailler ensemble et grandement améliorer les choses.

Nous voyons d'un œil favorable tout ce qui peut améliorer la coordination, la collaboration et la communication avec la population afin de renforcer la sensibilisation et les compétences dont nous avons besoin pour nous attaquer à ces crimes.

Le sénateur Black : La coordination constitue donc le principal obstacle. Même si vous affirmez que vous travaillez bien ensemble, des difficultés persistent. Y a-t-il d'autres obstacles?

Mr. Flynn: It's always a balance for us of the number of resources versus the problem we have and the ability to tackle it. Looking from my primary role of coordinating governance and oversight of operations, we always want to tackle more. When we look towards the collaboration and identification of the resources, the private sector, we're looking for ways to use as multipliers for the existing things in place. "Coordination" is a word I use. It's more than just a single word that says we need to communicate better. It's applying the resources that exist, and potentially new, if appropriate, to tackle the problem in the most effective way.

Senator Enverga: Thank you for the presentations. We're wide-eyed here. We want to listen to you, of course. I worked with computers for the longest time in my previous life. I know there are multiple points of attack all the time. It could be just your cellphone or your printer or something else in the airwaves. Those are the things we are looking for.

How prepared are we? How protected are we? On a scale of 1 to 10, where are we right now in terms of preparation and protection?

Mr. Hatfield: I would hesitate to put us on a scale. As we've said, we don't know what we don't know. What I will say is that in working with critical infrastructure sectors, for example, across the country — all sectors, not just the financial sector — the importance of digital technology and what it means for automation, for efficiencies, for improving service, many of us now have a smart meter in our house that lets us save power across the province in ways we never imagined. All of those innovations, it is well understood that when you put a piece of digital technology in your smart meter in your home, your fridge or, for some reason, your toaster — you can get an Internet-enabled toaster that burns the weather forecast into your toast. I'm not making this up. Every time you do that, you introduce something that could be exploited by somebody. The critical infrastructure sectors across Canada are acutely aware of that.

What I would say in response to this — and it's somewhat in response to previous questions as well — Canadians are smart people, and we shop online and spend a lot of time on the Internet, and our companies automate and leverage technology, and we're still here. We're enjoying it and benefiting from it, and I don't think Canadians would do that if it was imperilling them. I don't think if they were losing money hand over fist they would continue to do it.

M. Flynn : Pour nous, c'est toujours une question d'équilibre entre les ressources dont nous disposons, le problème et notre capacité à le résoudre. Mon rôle principal consiste à coordonner la gouvernance et à surveiller les activités, et nous voulons toujours en faire davantage. Lorsque nous cherchons à collaborer et à trouver des ressources auprès du secteur privé, nous sommes toujours à la recherche de moyens d'utiliser ces dernières pour multiplier les ressources existantes. J'emploie le mot « coordination », qui est plus qu'un simple terme indiquant que nous devons mieux communiquer. Il s'applique aux ressources existantes et potentiellement aux nouvelles pour que nous puissions nous attaquer au problème avec une efficacité optimale.

Le sénateur Enverga : Je vous remercie de vos exposés. Nous avons les yeux grands ouverts. Nous voulons vous écouter, bien entendu. Dans ma vie antérieure, j'ai travaillé longtemps en informatique, et je sais que les attaques peuvent survenir en tout temps et à une multitude d'endroits, comme sur un téléphone cellulaire, une imprimante ou autre chose sur les ondes. Voilà ce qui nous intéresse.

Dans quelle mesure sommes-nous prêts et protégés? Où nous situons-nous, sur une échelle de 1 à 10, sur le plan de la préparation et de la protection?

M. Hatfield : J'hésiterais à vous donner un chiffre sur une échelle. Comme nous l'avons souligné, nous ignorons ce que nous ne savons pas. Sachez toutefois que nous travaillons en collaboration, avec les secteurs des infrastructures essentielles du pays, par exemple. Nous collaborons avec tous les secteurs, pas seulement celui des finances, en ce qui concerne l'importance de la technologie numérique et son incidence sur l'automatisation et l'amélioration de l'efficacité et du service. Nombre d'entre nous disposent maintenant d'un compteur intelligent à la maison pour économiser l'énergie dans la province de manières que nous n'aurons jamais imaginées. Grâce à toutes ces innovations, nous dotons nos appareils de technologies numériques. Il peut s'agit d'un compteur intelligent, d'un réfrigérateur ou d'un grille-pain, ce dernier pouvant, une fois branché à Internet, griller les rôties en y inscrivant les prévisions météorologiques, et ce n'est pas là une invention de ma part. Cependant, chaque fois qu'on y installe un dispositif numérique, on ajoute quelque chose qui risque d'être exploité par quelqu'un. Les secteurs des infrastructures essentielles du pays en sont parfaitement conscients.

Ce que je pourrais répondre à cette question et, d'une certaine manière, à la précédente, c'est que les Canadiens sont intelligents. Nous magasinons en ligne et passons beaucoup de temps sur Internet, nos entreprises automatisent leurs activités et tirent parti de la technologie, et nous sommes encore là. Nous aimons cette technologie et nous en profitons, et je ne pense pas que les Canadiens le feraient si cela les mettait en danger. Ils ne continueraient pas d'utiliser la technologie s'ils se faisaient allègrement plumer.

There are problems and risks, but looking at the expertise and level of awareness we have and the coordination that my RCMP colleagues have spoken of, I won't put it on a scale, but I think we're doing this the right way, and we're among the best in the world at doing it.

Senator Enverga: Is it 50-50 or in the middle? You are basically unaware or have no clue what's happening in the future. Is that what it means? I know you're ready, but how ready are we? If you can't scale it from 1 to 10 . . .

Mr. Doran: But when you say "how ready are we?" —

Senator Enverga: How protected are we?

Mr. Doran: Maybe it would be helpful to clarify. Are you talking about the Canadian public writ large or my neighbour, who is far less ready than I am?

It's a scalable thing, and it's an individual thing as well. Some people are careless; some people are very careful; some people are paranoid. From a systems perspective, as Adam said, I think we're doing very well, but that doesn't prevent people who are being careless from becoming victimized or becoming victimized because of carelessness.

That's why it's a difficult question to answer on 1 to 10 scale.

Senator Enverga: How about Canadian government infrastructure? Are we 100 per cent protected? Are we 100 per cent ready to defend?

Mr. Hatfield: That is a question you should direct to Shared Services Canada and to the Communications Securities Establishment. Based on our experience, the security of Government of Canada networks is the envy of many of our allies, and we are doing an extremely good job in that respect. They can provide you the details, but we have very much to be proud of in how we protect our own information.

Senator Enverga: One last question about this —

The Deputy Chair: You're challenging your time here. Is this a new idea or a clarification of something? Say "clarification."

Senator Enverga: It's with regard to making it 100 per cent secure.

Do you propose any legislative tools that we can propose?

Il existe des problèmes et des risques, mais au regard de notre expertise, de notre degré de sensibilisation et de la coordination dont mes collègues de la GRC ont parlé, je ne donnerai pas de chiffre sur une échelle; je pense toutefois que nous agissons adéquatement et que nous figurons parmi les meilleurs du monde à ce chapitre.

Le sénateur Enverga : Est-ce 50/50 ou dans le milieu? Vous n'avez essentiellement aucune idée de ce qui vous attend dans l'avenir. Est-ce bien ce que cela veut dire? Je sais que vous êtes prêts, mais dans quelle mesure le sommes-nous? Si vous ne pouvez l'indiquer sur une échelle de 1 à 10…

M. Doran : Quand vous dites « dans quelles mesures sommes-nous prêts? »...

Le sénateur Enverga : Dans quelle mesure sommes-nous protégés?

M. Doran : Il serait peut-être utile de clarifier la question. Parlez-vous de la population canadienne en général ou de mon voisin, qui est bien moins prêt que moi?

La situation varie d'une personne à l'autre, car c'est une question individuelle. Certains sont insouciants, alors que d'autres sont très prudents ou paranoïaques. Au chapitre du système, comme Adam l'a fait remarquer, tout va très bien, mais cela n'empêchera pas les imprudents d'être victimes de leur insouciance.

Voilà pourquoi il m'est difficile d'attribuer une note de 1 à 10.

Le sénateur Enverga : Qu'en est-il de l'infrastructure du gouvernement fédéral? Sommes-nous entièrement protégés et prêts à nous défendre?

M. Hatfield : Vous devriez poser la question à Services partagés Canada et au Centre de la sécurité des télécommunications Canada. D'après notre expérience, la sécurité des réseaux du gouvernement du Canada fait l'envie d'un grand nombre de nos alliés, et nous accomplissons un excellent travail à cet égard. Les organismes que j'ai nommés peuvent vous donner des détails à ce sujet, mais nous avons tout lieu d'être fiers de la manière dont nous protégeons notre information.

Le sénateur Enverga : J'aurais une dernière question à ce sujet.

Le vice-président : Vous dépassez votre temps. S'agit-il d'une nouvelle idée ou d'un éclaircissement? Dites que c'est un éclaircissement.

Le sénateur Enverga : Cela concerne les démarches pour rendre le système entièrement sécuritaire.

Proposez-vous des outils législatifs que nous pourrions recommander?

Mr. Hatfield: Regarding the discussion of what mechanisms and legislation to put forward, the cyber review process going on right now is examining exactly that question. The government does intend to come forward with a new way forward for Canada on that.

[*Translation*]

Senator Maltais: Thank you for being here, gentlemen. My comments are for Mr. Lowson. In your brief, on page 4, in the second and third paragraphs, you refer to state-sponsored intellectual property theft for the purpose of obtaining information that would allow foreign companies to have a competitive advantage. I will quote you: "This can have a negative impact on investment or acquisition negotiations involving Canadian companies and the government of Canada, and in turn lead to lost jobs, revenue, and market share." I agree with you on this 100 per cent. Are these "pirate states" on a list, and is their name given to the executive branch of the Canadian government, that is to say the Prime Minister's Office?

Mr. Lowson: Thank you very much for the question, senator.

[*English*]

As I explained in my opening comments, one of the roles of CSIS is to provide advice to the Government of Canada, which we do on threats to national security. That includes threats that come from foreign state actors. Yes, the people within the government who need to be aware of who those state actors are do have that level of awareness.

I would add that foreign investment in Canada is an important issue. It's vital to our economy that we continue to have investors from abroad who are interested in investing in the Canadian economy. But we have to be cautious. It's for that reason that, under the provisions of the Investment Canada Act, there is a clause for a national security review. It's something the government takes seriously, and when there are actors about whom we have concerns who are proposing to make investments in Canada, we will take a look at that under that national security review process.

[*Translation*]

Senator Maltais: Thank you for your comments on the governmental aspect. Now I will speak about enterprises. Let's say a Canadian business negotiates a contract in good faith with another country that is on the "pirate state" list. Will your service be in contact with the business to warn them to be very careful? Do you do that? The enterprise is negotiating in good faith with a country that sanctions piracy.

M. Hatfield : Pour ce qui est de dire quels mécanismes et lois il convient d'adopter, l'examen de la cybersécurité est en cours et porte justement sur cette question. Le gouvernement entend proposer une nouvelle voie d'avenir pour le pays à ce sujet.

[*Français*]

Le sénateur Maltais : Merci, messieurs, d'être ici. Je vais m'adresser à M. Lowson. Dans votre mémoire à la page 4, aux deuxième et troisième paragraphes, on parle de vol de propriété intellectuelle parrainée par un État qui veut nécessairement obtenir des informations qui permettraient à des sociétés étrangères de jouir d'un avantage concurrentiel. Je vous cite : « Cela peut nuire aux négociations liées à des projets d'investissement ou d'achat avec des entreprises canadiennes et au gouvernement du Canada. Cela pourrait entraîner des pertes d'emploi de part et d'autre, soit du gouvernement, des entreprises. » Là-dessus, je vous crois à 100 p. 100. Ces États « pirates » figurent-ils sur une liste et leur nom est-il transmis au pouvoir exécutif du Canada, c'est-à-dire au bureau du premier ministre?

M. Lowson : Merci beaucoup, sénateur, pour la question.

[*Traduction*]

Comme je l'ai expliqué dans mon exposé, le Service canadien du renseignement de sécurité a notamment pour rôle de prodiguer des conseils au gouvernement fédéral, ce qu'il fait à propos des menaces à la sécurité nationale, y compris celles venant d'acteurs étatiques étrangers. Les personnes qui, au sein du gouvernement, doivent savoir qui sont ces acteurs seront mises au fait de la situation.

J'ajouterais que l'investissement étranger au Canada constitue une question importante. Il est essentiel pour notre économie que les investisseurs étrangers continuent de vouloir investir au Canada. Nous devons toutefois nous montrer prudents. Voilà pourquoi la Loi sur Investissement Canada comprend une disposition exigeant un examen relatif à la sécurité nationale. Le gouvernement prend la question au sérieux, et quand des acteurs qui nous préoccupent proposent d'effectuer des investissements au pays, nous étudierons la question dans le cadre du processus d'examen relatif à la sécurité nationale.

[*Français*]

Le sénateur Maltais : Merci pour le volet gouvernement. Maintenant, je vais aller du côté des entreprises. Disons qu'une entreprise canadienne de bonne foi négocie un contrat avec un autre pays, qui est sur la liste des « pirates ». Votre service va-t-il communiquer avec l'entreprise pour les prévenir d'être extrêmement prudents? Faites-vous cela? L'entreprise négocie de bonne foi avec un État « qui accepte le piratage ».

[*English*]

Mr. Lowson: Perhaps my colleague from Public Safety Canada would like to comment on this, because they are also responsible for the administration of the Investment Canada Act. But when there's a national security review going on, all the parties involved in the transaction are part of the process.

Senator Tannas: Thank you for being here. We've been reading a lot about artificial intelligence over the last few months, and I'm wondering if you could give us your thoughts on the idea of all of this switching from really bright people duking it out, good guys and bad guys, to all of a sudden really bright machines that are constantly changing their methods of attacking and so on, and correcting themselves based on the reactions and so on. Is that going on now? Is it a likely trend that we'll see artificial intelligence in this area develop and expand?

Mr. Hatfield: Senator, whether we have artificial intelligence is not an on-off switch. It's not a destination that we're going to arrive at; it's a process of development of technology.

Absolutely already today there are examples of malicious actors who have attempted to automate attacks. In turn, we have automated our defences. Right now today, a great deal of Internet is machine speaking to machine to make everything work, and folks are trying to disrupt, leverage or exploit it, and there are machines that are combatting that in real time to ensure that doesn't happen.

Many organizations could give you statistics of the hundreds of millions or billions of spam emails they get every day, which are stopped at a firewall. The number of reconnaissance probes across networks are in the hundreds of millions, and machines stop those in real time, and they never touch a human.

That is already going on today, and any new technology that has come into the high-tech field has been used for the good guys and unfortunately also for the bad guys. That will simply be a trend we see continue.

Senator Tannas: But in terms of machine-driven creativity, I guessing is what I'm getting at — I know there are bright guys that construct something that will go and attack 50,000 targets and on and on. But the creativity that comes from humans, the bad guys and the good guys who figure out — are we ever going to move into an area, or are we already, where you're actually seeing machines replace humans in the creativity around how to do this?

[*Traduction*]

M. Lowson : Peut-être que mon collègue de Sécurité publique Canada voudrait répondre à cette question, car cet organisme est également responsable de la gestion de la Loi sur Investissement Canada. Sachez toutefois que lorsqu'un examen relatif à la sécurité nationale est en cours, toutes les parties concernées par la transaction prennent part au processus.

Le sénateur Tannas : Merci de témoigner. Nous avons beaucoup lu au sujet de l'intelligence artificielle au cours des derniers mois, et je me demandais si vous pourriez nous dire ce que vous pensez du concept voulant qu'on passe soudainement d'une lutte entre des personnes vraiment brillantes et des gens malintentionnés a des machines très intelligentes qui modifient constamment leurs méthodes d'attaque et corrigent le tir en fonction des réactions. Est-ce ce qui est en train de se passer? Risquons-nous de voir l'intelligence artificielle se développer dans ce domaine?

M. Hatfield : Sénateur, l'intelligence artificielle n'arrivera pas du jour au lendemain. Ce n'est pas une destination à laquelle nous allons arriver, mais un processus d'évolution de la technologie.

Il ne fait aucun doute qu'aujourd'hui déjà, des acteurs malintentionnés tentent d'automatiser les attaques, ce à quoi nous avons réagi en automatisant nos défenses. À l'heure actuelle, Internet est géré en grande partie par des machines qui échangent entre elles pour tout faire fonctionner, et des gens tentent de perturber le processus ou d'exploiter le réseau. Des machinent leur font la lutte en temps réel pour qu'ils ne réussissent pas.

De nombreuses organisations pourraient vous fournir des statistiques sur les centaines de millions ou les milliards de pourriels qu'elles reçoivent quotidiennement, lesquels sont arrêtés par un pare-feu. Les sondages de reconnaissance se comptent par centaines de millions sur les réseaux, mais des machines les arrêtent en temps réel et ils n'atteignent jamais d'être humain.

Ces activités sont déjà en cours, et toutes les nouvelles technologies lancées dans le domaine de la technologie de pointe ont été utilisées par des gens de bonne foi, mais aussi par des personnes aux noirs dessins. Nous continuerons de surveiller cette tendance.

Le sénateur Tannas : C'est toutefois à la créativité des machines que je veux en venir. Je sais que des esprits brillants conçoivent quelque chose qui attaquera 50 000 cibles. Mais il s'agit là d'une créativité humaine, issue de bonnes et de mauvaises personnes qui trouvent moyen de parvenir à leurs fins. Les machines remplaceront-elles un jour les humains au chapitre de la créativité, à moins que ce ne soit déjà le cas?

Mr. Hatfield: I would say that a lot of things humans used to do are now being done by machines, both offensively and defensively, but the humans haven't gone away; they have simply gone to another level of work and obstruction. I will tell you that my team spends a lot of time trying to tell our very smart computers what to do, and I still need a lot of people to help me tell computers what to do.

Senator Tannas: I have one more question, and it's for fun. I loved the movie that Leonardo DiCaprio played Frank Abagnale, one of the best fraudster-counterfeit guys. At the end of the show, it turns out he goes to work for the FBI. Do we have bad guys switching to the good guys' teams the way we always hear about and read about in books and movies, where you catch some guy who's particularly talented and, instead of sending him to jail, you give him a chance to work for the good guys?

Mr. Flynn: I can say that from our recruiting, retention and engagement of employees, we're fortunate that we have enough very bright and talented individuals working on the problems that we're working on.

Senator Ringuette: You were saying that Equifax was the victim. However, when an entity says that your personal data you give us is protected, they're no longer the victim; they're also the perpetrator because that commitment has not been fulfilled. How do you handle that? Earlier you were saying they're the victim, in a way, but there's another series of crimes that occurred.

Mr. Doran: Absolutely. I would agree with you. I didn't mean to isolate Equifax as the only victim. Clearly, those who had their personal identities stolen or harmed in that case or in any case are victims as well.

While it is unfortunate, it's not necessarily a crime. It's a contract entered into between a corporation and a citizen, and the breach of the contract does not constitute a crime, necessarily. So a security breach on Equifax or the number of companies we've heard over the last number of years, while unfortunate and maybe a breach of some arrangement between client and service provider, doesn't necessarily make it a crime that we would investigate per se.

My point was that the evidence that we need to pursue is within Equifax holdings. Unless, of course, the victims' material is needed as well, then we would, of course, see the victims. But from an investigative point of view, not a holistic, policing, crime prevention point of view.

M. Hatfield : Je dirais que les machines réalisent maintenant un grand nombre de tâches que les humains accomplissaient, que ce soit à des fins offensives ou défensives, mais les humains n'ont pas disparu de l'équation; ils travaillent simplement sur d'autres plans de travail et d'obstruction. Mon équipe passe beaucoup de temps à dire quoi faire à nos très brillants ordinateurs, et j'ai encore besoin de bien des gens pour m'aider à leur donner des instructions.

Le sénateur Tannas : J'ai une autre question, simplement pour s'amuser. J'ai adoré le film dans lequel Leonardo DiCaprio incarne Frank Abagnale, un fraudeur et faussaire extrêmement doué. À la fin du film, il finit par travailler pour le FBI. Est-ce que des pirates passent à l'équipe des bons, comme on le lit ou le voit toujours dans les livres et dans les films, quand on donne aux personnes particulièrement talentueuses l'occasion de travailler pour les bons au lieu de les envoyer derrière les barreaux?

M. Flynn : Grâce au recrutement, au maintien en poste et à la motivation de nos employés, nous avons la chance de disposer d'un nombre suffisant d'esprits brillants et talentueux qui s'attachent à résoudre les problèmes auxquels nous nous attaquons.

La sénatrice Ringuette : Vous disiez qu'Equifax est une victime. Cependant, quand une entreprise a affirmé que les renseignements personnels sont protégés, elle n'est plus la victime, mais aussi l'auteur, car elle a failli à son engagement. Que faites-vous en pareil cas? Vous disiez plus tôt que les entreprises sont en quelque sorte des victimes, mais une autre série de crimes a eu lieu.

M. Doran : Je suis entièrement d'accord avec vous. Je ne voulais pas dire qu'Equifax est la seule victime. Il est évident que les gens dont l'identité a été volée et qui ont été lésés dans cette affaire et dans n'importe quel cas sont également des victimes.

Bien que ce soit malheureux, le fait que l'entreprise n'ait pas honoré son engagement ne constitue pas nécessairement un crime. Elle a conclu un contrat avec un citoyen, et le non-respect de ce dernier ne constitue pas nécessairement un crime. Les atteintes à la sécurité dont ont été victimes Equifax et un certain nombre d'entreprises dont nous avons entendu parler ces dernières années, bien qu'elles soient malheureuses et constituent peut-être un non-respect d'un arrangement entre un client et un fournisseur de service, ne constituent pas nécessairement un crime à propos duquel nous enquêterions.

Ce que je voulais dire, c'est que les preuves que nous cherchons sont détenues par Equifax, à moins, bien entendu, que nous n'ayons besoin des documents des victimes également, auquel cas nous rencontrerions aussi ces dernières, mais aux fins d'enquête et non pour des motifs holistiques ayant trait au maintien de l'ordre et à la prévention du crime.

Senator Ringuette: If there was a piece of legislation that would say that it is a crime that if a company says that your personal data will be protected by us, and is not, because you're in the process of reviewing all your mechanisms. Again, there's another loophole there, from my perspective.

Mr. Doran: Whether or laws are created is certainly not within my purview. We will enforce the laws that exist. Any laws that are enacted that provide us with extra tools in the toolbox are certainly welcome.

[*Translation*]

Senator Carignan: In the same vein, I am trying to assess what resources are needed. There are different types of cybercrime offences. Certain criminals use technology to commit an offence, and others target the technology needed to commit one. Do you make a distinction between the two in your investigations? What percentage of your resources is focused on technology as a target, as opposed to technology being used to commit fraud?

[*English*]

Mr. Flynn: We look at both types of offences, and we do use that separation to help us understand the problem better. We're very concerned with both the targeting of technology and the criminal use of technology, as my colleague Chief Superintendent Doran said, to increase their victimization, their global access to move ahead.

We're continuously analyzing how we raise our game and capabilities internally to address both of them. We're seeing a significant rise in both areas. We're seeing criminals adopt the use of technology very quickly. They don't have those internal large government entities or elements that we have to slow our adoption of technology. We're trying to overcome those and seek out the appropriate resources and apply them to the problem to enable our traditional investigators to move ahead better.

In cybercrime, we're fortunate with the large private industry investments in cybersecurity, the other government organizations in cybersecurity, that if we do it right, we have a lot of areas that we can leverage to help us tackle the problem, and we're making strong efforts to do that.

Senator Wetston: We've been touching on a lot of areas in our discussion today, and the area that I'd like to pursue in my last question is around Mr. Lowson's area, if I may. We talk a lot about hackers and cybercrime and cybersecurity and states of readiness. We know that Canadian industry, whether financial institutions, insurance and others, have spent billions of dollars protecting themselves against cyberattacks. I think billions

La sénatrice Ringuette : Comme vous êtes en train d'examiner l'ensemble de vos mécanismes, que diriez-vous si une loi stipulait que le fait qu'une entreprise qui affirme protéger les renseignements personnels faillit à son devoir constitue un crime? À mon avis, il existe une autre échappatoire à cet égard.

M. Doran : Il ne me revient certainement pas de dire s'il convient d'adopter des lois. Nous appliquerons celles qui existent, et toutes les lois adoptées qui nous procurent des outils supplémentaires sont assurément les bienvenues.

[*Français*]

Le sénateur Carignan : Toujours dans le même esprit, j'essaie d'évaluer les ressources qui sont nécessaires. Il y a différents types d'infractions liées à la cybercriminalité. Certains criminels utiliseront la technologie pour commettre une infraction et d'autres cibleront la technologie pour commettre une infraction. Faites-vous la distinction lors de vos enquêtes? Quel pourcentage de vos ressources concentre ses efforts sur la technologie comme cible par rapport à la technologie utilisée pour commettre une fraude?

[*Traduction*]

M. Flynn : Nous nous intéressons aux deux genres d'infractions et nous utilisons cette distinction pour nous aider à mieux comprendre le problème. Nous nous préoccupons fort du fait que des gens ciblent la technologie et utilisent cette dernière à des fins criminelles, comme mon collègue le surintendant principal Doran l'a indiqué, afin de faire davantage de victimes et d'élargir leur champ d'action à l'échelle internationale.

Nous analysons continuellement la manière dont nous pourrions nous améliorer et renforcer nos capacités internes afin de nous attaquer aux deux problèmes. Nous observons une recrudescence dans les deux domaines. Les criminels adoptent la technologie très rapidement, n'étant pas ralentis par la lourde machine gouvernementale. Nous tentons de surmonter ces obstacles, d'obtenir les ressources appropriées et de les appliquer au problème afin de permettre aux enquêteurs traditionnels de mieux progresser.

Au chapitre de la cybercriminalité, c'est une chance que le secteur privé et d'autres organismes gouvernementaux investissent des sommes substantielles dans la cybersécurité, car si nous agissons adéquatement, nous pouvons faire appel à bien des secteurs pour nous aider à lutter contre le problème. Nous déployons des efforts considérables en ce sens.

Le sénateur Wetston : Nous avons abordé bien des sujets aujourd'hui, et le domaine sur lequel porterait ma dernière question relève de M. Lowson. Nous parlons beaucoup des pirates, de la cybercriminalité, de la cybersécurité et de l'état de préparation. Nous savons que l'industrie canadienne, qu'il s'agisse des institutions financières, des compagnies d'assurance ou d'autres d'entreprises œuvrant dans d'autres domaines, a

would be the right number, although that's not a number in itself, but it's a lot of money.

Are we seeing increased attacks to national security? Is it on the increase from the point of view of CSIS and its experience to date? I'm not asking for specifics, but what are you doing about it with respect to dealing with these potential attacks to national security, which, of course, are state-specific rather than business oriented?

Mr. Lowson: As I mentioned previously, cyber is viewed by the service as a tool which enables actors to carry out threats to the security of Canada that have always been there. The CSIS Act was created in 1984, and it identified the categories of threats that I outlined for you in my opening comments. Those threat categories haven't changed since that time. What has changed is how the actors who are perpetrating those threats carry them out, and cyber certainly has become a tool that has enabled them to carry out those activities in a new and different way.

It is a domain that is evolving rapidly. It's a domain, as I said, that allows for actors to fly under the radar. It's difficult sometimes to attribute who is responsible for those activities. Is it posing a challenge? Yes, it's posing a challenge. But what I would also say is that this is what we do — this is our job — and looking at those threats to the security of Canada is fundamental. It's what the men and women of CSIS do every day, and we work in collaboration with our partners in the RCMP, CSE, CCIRC, and other organizations, to make sure we are responding adequately.

Senator Moncion: Can you give us a comment on prevention versus reaction? Are we more preventive or are we more reactive to cyberattacks?

Mr. Hatfield: I would say all of the above. I mean that very deliberately. Because we have seen situations where a technological breach occurred in a network, and it was the organization's ability to respond quickly, as a team of people, not just as computers, that enabled them to detect what was happening, stop what the malicious actor was trying to do, and ensure that there was no business or human impact. It simply remained a technological event.

So cybersecurity, not unlike emergency management with natural disasters, goes all the way from prevention through mitigation to preparedness for something to go wrong, the ability to react rapidly and the ability to recover and get things back to normal quickly. So the answer is yes.

dépensé des milliards de dollars afin de se prémunir contre les cyberattaques. Je pense qu'il est juste de parler de milliards de dollars; bien que ce ne soit pas un chiffre en soi, il s'agit d'une coquette somme.

Observe-t-on un accroissement des attaques contre la sécurité nationale? Fort de son expérience jusqu'à présent, le SCRS considère-il que ces attaquent augmentent? Je ne vous demande pas de fournir de détails, mais que faites-vous pour prévenir les attaques potentielles à la sécurité nationale, lesquelles visent le gouvernement plutôt que les entreprises, bien entendu?

M. Lowson : Comme je l'ai souligné précédemment, le service considère la cybertechnologie comme un outil permettant aux acteurs de concrétiser des menaces à la sécurité nationale qui ont toujours existé. La Loi sur le Service canadien du renseignement de sécurité, édictée en 1984, énumère les catégories de menace dont j'ai traité dans mon exposé. Ces catégories n'ont pas changé depuis. Ce qui a changé, c'est la manière dont les acteurs mettent en œuvre les menaces, et la cybertechologie est certainement devenue un outil qui leur permet de mener à bien leurs activités d'une manière nouvelle et différente.

C'est un domaine qui évolue rapidement, un domaine qui, comme je l'ai indiqué, permet aux acteurs d'échapper à la surveillance. Il est parfois difficile de déterminer qui est responsable de ces activités. Cela pose-t-il un défi? Oui, cela en pose un. J'ajouterais toutefois que c'est notre travail et qu'il est primordial de surveiller les menaces à la sécurité du pays. C'est ce que font quotidiennement les hommes et les femmes du SCRS, et nous travaillons en collaboration avec nos partenaires de la GRC, du Centre de la sécurité des télécommunications et du Centre canadien de réponse aux incidents cybernétiques pour nous assurer de réagir adéquatement.

La sénatrice Moncion : Pouvez-vous formuler un commentaire sur la prévention et la réaction? Sommes-nous plus portés à prévenir les cyberattaques ou à y réagir?

M. Hatfield : Je dirais que nous faisons les deux, et je le dis très délibérément, car il est arrivé qu'en cas d'atteinte technologique dans un réseau, ce soit la capacité de l'organisation à réagir promptement, grâce à son personnel et pas seulement aux ordinateurs, qui lui a permis de détecter le problème et d'empêcher l'acteur d'arriver à ses fins pour que l'attaque n'ait aucune répercussion sur les activités ou les gens. Toute l'affaire est demeurée un incident technologique.

La cybersécurité, à l'instar de la gestion des urgences en cas de catastrophe naturelle, englobe donc la prévention, les mesures d'atténuation, la préparation en vue de problèmes, ainsi que la capacité de réagir sans tarder, de se rétablir et de reprendre le cours normal des choses rapidement. Je répondrais donc par l'affirmative.

Senator Enverga: It's a very quick question, if you don't mind. A few months ago, Hytera Communications of China bought Norsat. It's a communications satellite company and I'm just wondering have you been consulted on this? It is a high-tech Canadian company that was bought by the Chinese. Should you be consulted on these activities? Was that something that you did?

Mr. Doran: That would be out of my purview. I don't know about others.

Mr. Lowson: I would go back to the comments I made earlier about the national security review provisions.

Certainly, the government would have been alerted to that acquisition and it would have been examined through the lens of whether it requires a national security review.

However, I'm not in a position right now to respond as to whether or not that took place.

Senator Enverga: According to the report there was no formal national security review. However, would you suggest that in the next instance where we are selling our industrial secrets that you should be consulted?

Mr. Lowson: I think there is a process in place already that makes that determination and I would rely on that process to arrive at that conclusion.

[*Translation*]

Senator Maltais: I am going to play devil's advocate. Is the banking sector not to some degree the artisan of its own misfortune? Today, almost everyone uses computers. However, certain people of 55 or more cannot use computers to deposit their money in their bank account. If they want a statement, they have to pay for it. These small devices, such as cell phones, for instance — are they totally risk-free in financial transactions?

[*English*]

Mr. Doran: I can't speak to the level of security of devices, I'm sorry. Any system is potentially a victim of a cyber-attack. A good defence system may prevent it and a clever hacker may defeat it. I can't really say specifically whether or not your system or others are secure.

[*Translation*]

Senator Massicotte: We've discussed things all evening from a defensive position, like goalies. On occasion, it is good to take up an offensive position.

Le sénateur Enverga : Je vous poserais une très brève question, si vous le voulez bien. Il y a quelques mois, l'entreprise chinoise Hytera Communications a acquis Norsat, une entreprise de satellites. Je me demande si vous avez été consultés à ce sujet. Il s'agit d'une entreprise canadienne de technologie de pointe qui a été achetée par les Chinois. Devriez-vous être consultés à propos de ces activités? Êtes-vous intervenus dans le dossier?

M. Doran : La question serait de mon ressort. J'ignore si les autres témoins souhaitent intervenir.

M. Lowson : Je reviendrais aux observations que j'ai formulées plus tôt au sujet des dispositions relatives à l'examen relatif à la sécurité nationale.

Le gouvernement aura certainement été avisé de cette acquisition et l'aura examinée pour déterminer si elle requiert un tel examen.

Je ne suis toutefois pas en mesure de vous dire si cet examen a eu lieu ou non.

Le sénateur Enverga : D'après le rapport, il n'y a pas eu d'examen officiel relativement à la sécurité nationale. Considérez-vous toutefois que vous devriez être consultés la prochaine fois que nous vendons nos secrets industriels?

M. Lowson : Je pense qu'il existe déjà un processus à cette fin et je m'y fierais pour en arriver à une conclusion.

[*Français*]

Le sénateur Maltais : Je vais faire l'avocat du diable. Le secteur bancaire n'est-il pas un peu l'artisan de son propre malheur? Aujourd'hui, pratiquement tout le monde se sert de l'informatique. Par contre, certaines personnes de 55 ans et plus sont incapables de se servir de l'informatique pour déposer leur argent dans leur compte de banque. S'ils veulent un relevé bancaire, ils doivent le payer. Ces petits dispositifs, les téléphones cellulaires, par exemple, sont-ils totalement sans risque en matière de transactions financières?

[*Traduction*]

M. Doran : Je suis désolé, mais je ne peux traiter du niveau de sécurité des appareils. Tout système peut être la cible d'une cyberattaque. Un solide système de défense peut prévenir une attaque, mais un pirate futé peut le vaincre. Je ne peux vraiment pas dire précisément si notre système ou d'autres réseaux sont sécuritaires ou non.

[*Français*]

Le sénateur Massicotte : On a parlé toute la soirée en prenant une position défensive, comme un gardien de but. À l'occasion, on a raison de prendre une position offensive.

[*English*]

You don't score any goals if you don't do it offensively. Under what circumstances would we be offensive in terms of national security? What are the criteria by which we will take action against someone as opposed to simply protecting our interests?

Mr. Lowson: As I mentioned in my opening comments, one of the provisions that is available to CSIS is threat reduction measures. That was something that was made available to us in some recent legislation, and we're expecting that, as part of Bill C-59 that's going through now, that's part of the reexamination. But assuming that those powers remain with us, it does provide us with the ability to be more proactive against any of the threats to the security of Canada that we may face. That is a tool that we do have in our tool kit at the moment.

Senator Massicotte: That is on the basis that it reduces the eventual threat to us. Is that the only condition or the only time we can be offensive if it is a threat reduction mechanism?

Mr. Lowson: I would say that we would probably need to define exactly what we mean by "offensive." I would argue that the reason for having an intelligence service like CSIS is to be able to gather information, analyze that information and provide advice to the Government of Canada on what to do about these situations. That is not always in reactive mode, to come back to a previous question. That also does provide some proactive ability.

Senator Massicotte: Thank you.

The Deputy Chair: Thank you, Senator Massicotte. Just before we conclude, we had an undertaking by the chief superintendent to provide us with some statistics. You made a note of that. Can you give us indication as to when we might hear back from you?

Mr. Doran: When would you like to hear back from me? From an RCMP perspective, I think we can manage that.

The Deputy Chair: We will diary it for a week forward. Colleagues, we will continue tomorrow at 10:30 with the same topic.

I would like to thank our witnesses this evening from Public Safety Canada, the Royal Canadian Mounted Police — thank you, gentlemen — and the Canadian Security Intelligence Service. You helped us get started on this new study. Thank you.

(The committee adjourned.)

[*Traduction*]

On ne marque pas de buts si on ne passe pas à l'attaque. En quelles circonstances passerions-nous à l'offensive au chapitre de la sécurité nationale? Sur quels critères nous basons-nous pour décider d'intervenir contre quelqu'un au lieu de simplement protéger nos intérêts?

M. Lowson : Comme je l'ai fait remarquer au cours de mon exposé, une disposition autorise le SCRS à prendre des mesures de réduction de la menace. C'est une possibilité qui lui a été offerte dans une récente mesure législative, et nous nous attendons à ce que ces pouvoirs fassent l'objet d'un réexamen dans le cadre de l'étude du projet de loi C-59. Toutefois, si on présume que nous les conserverons, ces pouvoirs nous permettent d'être plus proactifs afin de lutter contre les menaces à la sécurité du Canada. C'est un outil que nous avons actuellement à notre disposition.

Le sénateur Massicotte : Nous ne pouvons agir que si c'est pour réduire les menaces contre nous. Est-ce à cette condition seulement que nous pouvons passer à l'offensive au moyen d'un mécanisme de réduction de la menace?

M. Lowson : Nous devrions probablement définir ce que nous entendons exactement par « offensive ». Si un service du renseignement comme le SCRS existe, c'est pour pouvoir recueillir et analyser des renseignements, et prodiguer des conseils du gouvernement fédéral sur ce qu'il convient de faire dans ces situations. Nous ne sommes pas toujours en mode de réaction, pour en revenir à votre question précédente. La loi nous permet aussi d'être proactifs.

Le sénateur Massicotte : Merci.

Le vice-président : Merci, sénateur Massicotte. Juste avant de conclure, je vous rappelle que le surintendant principal s'est engagé à nous fournir des statistiques. Vous l'avez pris en note. Quand pensez-vous nous les communiquer?

M. Doran : Quand souhaitez-vous les recevoir? Je pense qu'à la GRC, nous pouvons nous adapter en conséquence.

Le vice-président : Nous nous attendrons à les recevoir d'ici une semaine. Mesdames et messieurs, nous poursuivons la discussion sur le même sujet demain à 10 h 30.

Je voudrais remercier nos témoins de ce soir, lesquels représentaient Sécurité publique Canada, la Gendarmerie royale du Canada — merci, messieurs — et le Service canadien du renseignement de sécurité. Vous nous avez aidés à entamer cette nouvelle étude. Merci.

(La séance est levée.)

EVIDENCE

OTTAWA, Thursday, October 19, 2017

The Standing Senate Committee on Banking, Trade and Commerce met this day at 10:33 a.m., to continue its study on issues and concerns pertaining to cybersecurity and cyberfraud.

Senator Joseph A. Day (*Deputy Chair*) in the chair.

[*Translation*]

The Deputy Chair: Welcome, honourable senators. We are going to be continuing our study on issues and concerns pertaining to cybersecurity and cyberfraud.

I would like to introduce our first witness this morning. Please welcome Benoît Dupont, Scientific Director, who is joining us by videoconference.

Benoît Dupont, Scientific Director, Smart Cybersecurity Network (SERENE-RISC): Thank you, Mr. Chair. Honourable senators, I would like to thank you for this opportunity to appear before you today as part of your study on cybersecurity and cyberfraud.

My name is Benoît Dupont. I hold the Canada Research Chair in cybersecurity at the Université de Montréal, where I am also a professor of criminology. As you indicated, I am the Scientific Director of the Smart Cybersecurity Network, also known by the acronym SERENE-RISC, which is one of Canada's Networks of Centres of Excellence (NCE).

[*English*]

I will begin my remarks by providing some contextual information on the current state of Canadian cybersecurity before going into more details about what the Smart Cybersecurity Network does, why it is important and what future challenges will have to be addressed from a research and development perspective.

Canada is one of the most connected societies on earth, and its economic growth depends on the development of a productive and healthy digital ecosystem.

The technology is not only an asset, it has also become a major source of risks. According to PwC, in its Global CEO Survey published in 2016, 61 per cent of Canadian CEOs believe that cybersecurity is the biggest potential business threat to their organizations' growth prospect, topping availability of key skills, volatile commodity prices and consumer spending behaviours.

TÉMOIGNAGES

OTTAWA, le jeudi 19 octobre 2017

Le Comité sénatorial permanent des banques et du commerce se réunit aujourd'hui, à 10 h 33, pour poursuivre son étude sur les questions et préoccupations relatives à la cybersécurité et à la cyberfraude.

Le sénateur Joseph A. Day (*vice-président*) occupe le fauteuil.

[*Français*]

Le vice-président : Honorables sénateurs et sénatrices, soyez les bienvenus. Nous allons continuer notre étude sur les questions et préoccupations relatives à la cybersécurité et à la cyberfraude.

J'aimerais donner la parole à notre témoin pour commencer ce matin. Nous accueillons M. Benoît Dupont, directeur scientifique, qui témoignera par vidéoconférence.

Benoît Dupont, directeur scientifique, Réseau intégré sur la cybersécurité (SERENE-RISC) : Merci, monsieur le président. Honorables sénateurs, j'aimerais vous remercier de l'occasion que vous m'offrez de comparaître devant vous aujourd'hui dans le cadre de l'étude sur la cybersécurité et la cyberfraude.

Mon nom est Benoît Dupont, et je suis le titulaire de la Chaire de recherche du Canada en cybersécurité, à l'Université de Montréal, où je suis également professeur de criminologie. Comme vous l'avez indiqué, je suis le directeur scientifique du Réseau intégré sur la cybersécurité, connu également sous l'acronyme de SERENE-RISC, qui est l'un des Réseaux de centres d'excellence (RCE) du Canada.

[*Traduction*]

Je vais commencer mon exposé avec de l'information contextuelle sur la situation actuelle de la cybersécurité au Canada. Je parlerai ensuite plus en détail de ce que fait le Réseau intégré sur la cybersécurité, de son importance et des défis futurs qui devront être relevés en matière de recherche et de développement.

Le Canada est l'une des sociétés les plus branchées de la planète et sa croissance économique dépend du développement d'un écosystème numérique robuste et productif.

La technologie est certes un atout, mais force est de reconnaître qu'elle est aussi devenue une très importante source de risque. Selon l'Enquête mondiale menée auprès des chefs de direction que PricewaterhouseCoopers a publiée en 2016, 61 p. 100 des chefs de direction canadiens considèrent que la cybersécurité est, en puissance, l'aspect opérationnel le plus risqué pour les perspectives de croissance de leurs organisations

Also, in a recent study by Scalar, titled "The Cybersecurity Readiness of Canadian Organizations," published in 2017, the study shows the negative impacts of cyberattacks on productivity. In 2016, 53 per cent of companies surveyed reported an incident that resulted in the loss of sensitive information, with an average of 44 events per year and per company, and a marked increase in the sophistication and severity of attacks.

Small- and medium-sized enterprises, which have very limited resources to devote to IT and online security, are particularly vulnerable, while they contribute more than 50 per cent of business-sector GDP. Cyber risks will therefore have a disproportionate impact on this key segment of our economy.

Canadian citizens are also exposed to a growing number of online scams and cyber-frauds. Reliable statistics are missing in Canada, but the most recent victimization survey for England and Wales suggests that online fraud and computer hacking now represent the number one form of property crime and amount to half of all crimes taken together. That's all property and person crimes.

Unfortunately, Internet users still receive very limited or even contradictory advice on what good digital habits they should adopt to minimize their chances of victimization, and they lose trust in the reliability of online transactions in the process. At the same time, Canadian police services have not yet mobilized the financial and human resources required to deal with this crime epidemic, and they are unsure of how to best tackle this massive challenge.

We now stand at the critical technological juncture where we are shifting from an industrial society, heavily reliant on manufacturing, to a digital society fuelled by information and data. We also have legacy critical infrastructures that are almost all connected to the Internet, which creates an unprecedented level of interdependency and generates an endless stream of vulnerabilities.

Meanwhile, through the Internet of Things, we are about to add more than 50 billion unsecured new devices with varying degrees of autonomy to this already unpredictable threat landscape. This will increase the complexity of the cybersecurity challenge by at least one order of magnitude.

respectives, surpassant en cela les compétences clés, la volatilité des cours des produits de base et les habitudes de dépenses des consommateurs.

De plus, dans L'état de préparation en matière de cybersécurité des organisations canadiennes, une étude publiée en 2017 par Scalar, on décrit les effets négatifs qu'ont les cyberattaques sur la productivité. En 2016, 53 p. 100 des entreprises sondées ont rapporté un incident ayant causé la perte d'information sensible. La moyenne est de 44 incidents par année par entreprise, et l'on note une augmentation marquée de la complexité et de la gravité des attaques.

Les petites et moyennes entreprises, qui ont très peu de ressources à consacrer à la sécurité des TI et aux activités en ligne, sont particulièrement vulnérables, même si ce sont elles qui contribuent à plus de 50 p. 100 du PIB du secteur des affaires. C'est ce qui explique pourquoi les risques cybernétiques ont un impact disproportionné sur ce segment de notre économie.

Les citoyens canadiens sont, eux aussi, de plus en plus exposés à des arnaques en ligne et à des cyberfraudes. Nous n'avons pas de statistiques canadiennes fiables à ce sujet, mais la plus récente enquête sur la victimisation en Angleterre et au pays de Galles indique que la fraude en ligne et le piratage informatique sont désormais la principale forme d'infraction contre les biens, et qu'ils sont à l'origine de la moitié de toutes les infractions commises, c'est-à-dire de toutes les infractions contre les biens et les personnes.

Malheureusement, les internautes reçoivent encore très peu de conseils — quand ils ne sont pas contradictoires — sur les comportements qu'ils devraient adopter pour réduire au minimum les risques de se faire prendre au piège, et il en résulte une perte de confiance relativement à la fiabilité des transactions en ligne. Parallèlement à cela, les services policiers canadiens n'ont pas encore mobilisé les ressources humaines et financières nécessaires pour contrer cette forme de criminalité qui prend des proportions épidémiques, et ils ne sont pas tout à fait certains de ce qu'ils doivent faire pour régler cet énorme problème de la façon la plus efficace possible.

Nous sommes à la croisée des chemins technologiques. Nous sommes en train de passer d'une société industrielle vastement dépendante du secteur de la transformation à une société numérique carburant aux données et à l'information. Nous avons aussi des infrastructures héritées du passé, mais qui jouent un rôle névralgique puisqu'elles sont presque toutes branchées à Internet, ce qui crée une interdépendance sans précédent et donne lieu à un flux interminable de vulnérabilités.

Entretemps, avec l'Internet des objets, nous sommes sur le point d'ajouter à ce paysage imprévisible du risque plus de 50 milliards de nouveaux appareils non sécurisés fonctionnant avec divers degrés d'autonomie, ce qui décuplera la complexité du défi de la cybersécurité.

So far, Canada has not placed cybersecurity very high on its list of economic, research and development and policy priorities, while other nations, such as the U.S., the U.K., Australia, Israel, the Netherlands or Singapore, to name a few, are forging ahead and becoming global leaders in cybersecurity.

Cybersecurity Ventures, a consulting firm, estimates that $1 trillion will be spent globally on securing cyber systems between 2017 and 2021. In our country, existing efforts to address this gap, while valuable, lack coordination and have not achieved the critical mass required to spur innovation and adaptation to this new risk landscape. Canada could very well be falling behind at this crucial moment.

The Smart Cybersecurity Network has identified more than 250 academics from 47 universities carrying out research on various aspects of cybersecurity; 65 per cent of them are from the computer science faculties and departments and 35 per cent stem from the social sciences. We have also identified 34 institutional partnerships between public and private stakeholders to mitigate cyber risks. But there is no national network that could systematically connect these fragmented resources, despite multiple ad hoc collaborations.

The Smart Cybersecurity Network's role is limited by its current resources and mandate, which is to do knowledge mobilization, which we define as getting the right information in the right format at the right time to the right people.

Our network is made up of 33 institutional partners from industry, government and the non-profit sector, as well as 42 academics from eight disciplines based at 23 universities and colleges from coast to coast.

We deliver six key activities: We host biannual workshops that have brought together almost 850 cybersecurity thought leaders and practitioners from 250 public and private sector organizations over the past three years. We host and curate an online knowledge-sharing platform that now contains more than 800 documents, original videos and research summaries about cybersecurity. We also produce quarterly knowledge digests that summarize leading-age cybersecurity research relevant to practitioners in a practical format.

We have hosted eight relationship forums that bring together stakeholders with common interests in cybersecurity in our country's main tech hubs. We develop and host professional

Jusqu'ici, le Canada n'a pas placé la cybersécurité très haut sur sa liste de priorités en matière d'économie, de recherche et développement, et de politiques, alors que d'autres, comme les États-Unis, le Royaume-Uni, l'Australie, Israël, les Pays-Bas ou Singapour, pour ne nommer que ceux-là, sont en train de prendre les devants et de devenir des meneurs mondiaux à cet égard.

Cybersecurity Ventures, une société d'experts-conseils, évalue à 1 000 milliards de dollars le montant qui sera consacré aux systèmes de cybersécurité entre 2017 et 2021. Dans notre pays, les efforts investis pour combler cette lacune sont louables, mais ils manquent de coordination; ils n'ont pas encore atteint la masse critique nécessaire pour stimuler l'innovation et favoriser l'adaptation à cette nouvelle dynamique du risque. Nous sommes à un moment charnière et le Canada risque fort bien de prendre du retard.

Le Réseau intégré sur la cybersécurité a recensé plus de 250 chercheurs répartis dans 47 universités qui s'intéressent à divers aspects de la cybersécurité; 65 p. 100 d'entre eux sont de facultés et de départements d'informatique, et 35 p. 100 évoluent dans le domaine des sciences sociales. Nous avons également recensé 34 partenariats institutionnels entre intervenants des secteurs public et privé qui se sont donné pour mission d'atténuer les risques cybernétiques. Toutefois, malgré les nombreuses collaborations ponctuelles, il n'y a pas de réseau national qui pourrait systématiquement lier entre elles ces ressources fragmentées.

Le rôle du réseau intégré sur la cybersécurité est limité par ses ressources et son mandat actuels. Le réseau s'est donné pour mandat de mobiliser les connaissances, c'est-à-dire d'acheminer la bonne information aux bonnes personnes dans le format qui convient et en temps opportun.

Notre réseau regroupe 33 partenaires institutionnels issus de l'industrie, du secteur gouvernemental et du secteur sans but lucratif, ainsi que 42 universitaires travaillant dans 8 disciplines et répartis dans 23 institutions postsecondaires à l'échelle du Canada.

Voici les six grands secteurs où nous œuvrons. Deux fois par année, nous organisons des ateliers. Au cours des trois dernières années, nos ateliers ont mobilisé près de 850 théoriciens et professionnels du domaine de la cybersécurité issus d'organismes des secteurs public et privé. Nous hébergeons un forum en ligne pour le partage des connaissances, forum qui contient déjà plus de 800 documents, vidéos originales et sommaires de recherche portant sur la cybersécurité. Nous publions également des synthèses de connaissances sur une base trimestrielle. Il s'agit en fait de bulletins qui s'adressent aux professionnels du domaine et qui, dans un format pratique, font le point sur la recherche de pointe en cybersécurité.

Au fil des ans, nous avons organisé huit forums afin de rassembler les intervenants des grands centres de haute technologie du Canada qui ont un intérêt commun pour la

development activities that engage post-secondary students and early career professionals, and we are proud to have attracted 42 per cent female participants in a field where only 11 per cent of positions are filled by females.

Finally, with generous financial support from Public Safety Canada, we developed and delivered an innovative awareness and training tool named Cybersec 101 delivered in both languages through public libraries across the country. We are targeting older users for this awareness and training tool.

By designing and delivering knowledge-mobilization activities tailored to the needs of government decision-makers, industry practitioners and the general public, the Smart Cybersecurity Network makes a strategic contribution that tries to enhance the capacities of the Canadian digital ecosystem, to understand the complexity of the current threat landscape and to try to forecast emerging risks, to address cyber risks by understanding the evidence that can support effective and efficient decision-making and to enhance the resilience of the Canadian digital ecosystem by training a new generation of cybersecurity professionals.

Although I would like to close on a positive note, I would like to stress that cybersecurity is not only a technical problem. Cybersecurity has multiple social and policy implications that are rarely addressed alongside its already complicated technical aspects. The complexity of the challenge is such that only, in my view, a cross-disciplinary network of researchers and end-users from industry and government can expect to discover, develop and implement the innovative solutions that are so urgently needed. I am afraid to say that we do not have such a network in place in our country yet.

Thank you very much for your attention. I look forward to your questions.

[*Translation*]

The Deputy Chair: Thank you very much for your comments, Professor Dupont.

Senator Massicotte: Thank you for joining us this morning to talk about a subject I see as very important. Yesterday afternoon, we had with us four representatives of the Canadian government who are responsible for security matters. They tried hard to put the subject in contact by saying that there have always been attacks, or the fear of attacks, to our security and our personal information and that this is just a different method of electronic transmission. However, I am still concerned by cyberthreats. Just think about the credit agencies, the American elections and the

cybersécurité. Nous avons également mis au point des activités de développement professionnel à l'intention des étudiants postsecondaires et des jeunes professionnels. Nous sommes d'ailleurs fiers de dire que 42 p. 100 de nos participants étaient des femmes, ce qui est toute une réussite si l'on considère que les femmes n'occupent que 11 p. 100 des postes dans ce domaine.

Enfin, grâce au généreux soutien financier de Sécurité publique Canada, nous avons mis au point un outil de sensibilisation et de formation novateur, Cybersec 101, que nous offrons en français et en anglais dans des bibliothèques publiques d'un peu partout au pays. L'outil s'adresse essentiellement aux aînés.

En concevant et en offrant des activités de mobilisation des connaissances adaptées aux besoins des décideurs gouvernementaux, des professionnels de l'industrie et du grand public, le Réseau intégré sur la cybersécurité contribue de façon stratégique à améliorer les capacités de l'écosystème numérique du Canada, à comprendre la complexité des menaces actuelles et à tenter d'anticiper les risques émergents, à faire face aux risques cybernétiques en cernant les éléments de preuve susceptibles d'appuyer la prise de décisions efficaces et efficientes, ainsi qu'à améliorer la résilience de l'écosystème numérique du Canada en formant une nouvelle génération de professionnels de la cybersécurité.

Bien que je souhaite terminer sur une note positive, je tiens à souligner que la cybersécurité n'est pas seulement une question technique. La cybersécurité a de multiples répercussions sociales et stratégiques qui retiennent rarement l'attention comparativement aux aspects techniques. La question est d'une telle complexité que, selon moi, la découverte, l'élaboration et la mise en œuvre des solutions innovatrices dont nous avons instamment besoin ne pourront se faire que par un réseau interdisciplinaire de chercheurs et d'utilisateurs finals de l'industrie et du gouvernement. Or, j'ai bien peur que nous n'ayons pas encore de réseau de la sorte dans notre pays.

Merci beaucoup de votre attention. Je serai heureux de répondre à vos questions.

[*Français*]

Le vice-président : Professeur Dupont, merci beaucoup pour vos commentaires.

Le sénateur Massicotte : Merci d'être parmi nous ce matin pour parler d'un sujet que je considère comme étant très important. Hier après-midi, nous avons reçu quatre représentants du gouvernement canadien qui ont des responsabilités en matière de sécurité. Ils ont fait l'effort de relativiser le sujet en disant qu'il y a toujours eu des attaques ou des craintes d'attaques à notre sécurité et à notre information personnelle, et que c'est une différente méthode de transmission électronique. Cependant, je demeure toujours inquiet de la cybermenace. On parle d'agences

elections in Kenya. These are very real and it's very threatening for our personal information, our habits, and also for companies. Is it a serious problem or is it solely the fact that we are reacting disproportionately because we feel threatened?

Mr. Dupont: Personally, I feel that it is a serious problem that comes with societal change. We are becoming a digital society in all aspects of our human activities. It is normal that the risks will also become digital.

The problem that I see is not that risks are more numerous than before, it is that the institutions that are supposed to respond to those risks are perhaps slower to adapt to this new reality. A concrete example that I use is the police, which is an institution created to respond to security problems during the industrial revolution at the end of the 19th century. It is an institution created at a different time, for a different situation, and it now has to adapt to a new revolution, one that is not industrial but digital. We may need to create new institutions to respond to those risks. To answer your question, I feel that the problem is quite serious. For me, the problem is as serious as climate change.

Senator Massicotte: It is huge. We are seeing problems with confidentiality violations in a number of American companies that have been hit, like Target and Equifax. I think that it is just as serious in Canada. However, perhaps there is less transparency, less information being communicated. One might say that those companies — ones that we trust by providing them with personal information — are suffering no consequences, financial, criminal, or any other kind. Why are there no consequences? Something, some information breach, happens every week. It means that the companies have not taken the measures required to protect the confidential information that we have shared with them in complete trust. There is a breach of trust in that relationship.

Mr. Dupont: I will answer your question in two stages. Why do we hear less about this in Canada? It is because our regulatory framework for companies and organizations does not require them to disclose this kind of incident when they are victims of one. The situation is slightly different in the United States where legislation requires companies that are victims to disclose the incident. At times, there are delays in doing that. We may hear about incidents several months later and, in some cases, several years later.

But the regulatory framework is different in the United States and it requires companies to disclose that information. However, in the United States, the regulatory framework does not impose

de crédit, des élections américaines et des élections au Kenya. On parle de choses très présentes, et c'est très menaçant pour nos renseignements personnels, nos coutumes et aussi pour les entreprises. Est-ce un grave problème ou est-ce seulement nous qui réagissons avec démesure, parce que nous nous sentons menacés?

M. Dupont : Personnellement, je pense que c'est un grave problème qui accompagne des changements de société. Nous devenons une société numérique dans tous les aspects de nos activités humaines. Il est normal que les risques deviennent aussi numériques.

Le problème que je constate, ce n'est pas que les risques sont plus nombreux qu'auparavant, c'est que les institutions qui sont censées répondre à ces risques sont peut-être plus lentes à s'adapter à cette nouvelle réalité. Un exemple concret que je donne, c'est la police, qui est une institution qui a été créée pour répondre à des problèmes de sécurité de la révolution industrielle à la fin du XIX^{e} siècle. C'est une institution qui a été créée à une autre période, dans un autre contexte et qui, maintenant, doit s'adapter à une nouvelle révolution qui n'est pas industrielle, mais qui est numérique. Peut-être qu'on aura besoin de créer de nouvelles institutions pour répondre à ces risques. Pour répondre à votre question, je pense que le problème est relativement grave. Pour moi, c'est un problème aussi grave que les changements climatiques.

Le sénateur Massicotte : C'est majeur. Lorsqu'on regarde les problèmes de violation de la confidentialité, on parle de plusieurs entreprises américaines qui sont ciblées, comme Target et Equifax. Je pense que c'est aussi grave au Canada. Cependant, peut-être qu'il y a moins de transparence, moins de communication de l'information. On dirait que ces entreprises — à qui l'on a fait confiance en leur divulguant de l'information personnelle — ne subissent aucune conséquence financière, criminelle, ou autre. Pourquoi n'y a-t-il pas de conséquence? Chaque semaine, il se passe quelque chose, un autre bris d'information. Cela signifie que les entreprises n'ont pas pris les mesures nécessaires pour protéger les renseignements confidentiels que nous avons partagés avec eux en toute confiance. Il y a un abus de confiance dans cette relation.

M. Dupont : Je vais répondre à votre question en deux phases. Pourquoi en entend-on moins parler au Canada? C'est parce que notre encadrement réglementaire des entreprises et des organisations ne les force pas à divulguer ce type d'incident lorsqu'elles en sont victimes. La situation est légèrement différente aux États-Unis, où il y a des lois qui obligent les entreprises victimes à divulguer les incidents. Cela se passe parfois à retardement. On apprend la nouvelle quelques mois plus tard et, dans certains cas, plusieurs années plus tard.

Mais il y a un encadrement réglementaire qui est différent aux États-Unis, qui oblige les entreprises à divulguer ces renseignements. Par contre, aux États-Unis, il n'y a pas

any very harsh penalties. That also partly explains why we may feel that companies are not very exposed to sanctions that could encourage them to take more robust measures to protect our personal information.

[*English*]

Senator Wallin: Thank you. I am following up on the issue that you have just touched on. We discussed yesterday at length the question of no reporting requirements. There is no way to force a company to admit or to report to either a police or a governmental structure that they have been hacked or in some way influenced and that our personal information might be in jeopardy. I know you come at this from the research side, but I would like your personal view on whether or not that should be the case, that we should be more like the Americans in this, that companies must be forced to report. If they don't, there are consequences; even if they do, there may be. In that quite legalistic approach, what is your opinion on that?

Mr. Dupont: First, I like to stress that there is a law that is going to come into action very soon in Canada. It's the Digital Privacy Act. I think the regulatory framework is being finalized, but it will force, under a number of circumstances, companies to disclose to the Privacy Commissioner cases of data breaches, and it will force them to notify their customers or their employees when such incidents happen.

Personally, for the sake of transparency, I think that it's a positive thing. It's a positive development. I think companies that suffer data breaches should be forced to disclose these incidents publicly, not because of the shaming dimension but because it makes things more transparent and consumers can learn about the situation of their own private information. They can make more informed choices with regard to the companies that they choose to patronize or entrust with their money or their personal information.

There are also measures that will very quickly be implemented in Europe, where the fines for such incidents will be major. I think we're talking about 4 per cent of annual revenues. Europe is moving in a much more coercive approach to companies that suffer data breaches.

Senator Wallin: What is the fine for? Is the fine for not reporting or for the breach occurring?

d'encadrement réglementaire qui impose des pénalités très sévères. C'est ce qui explique aussi pourquoi, en partie, on a le sentiment que les entreprises sont peu exposées à des sanctions qui pourraient les inciter à prendre des mesures plus robustes pour protéger nos renseignements personnels.

[*Traduction*]

La sénatrice Wallin : Merci. Je vais poursuivre sur le sujet que vous venez tout juste d'aborder. Hier, nous avons discuté en long et en large de la question de l'absence d'obligations redditionnelles. Il n'y a aucune façon de forcer une entreprise à admettre ou à rapporter soit à la police ou à une structure gouvernementale qu'elle a été piratée ou influencée de quelque façon, et que les renseignements personnels qu'elle détient à notre sujet pourraient être en danger. Je sais que vous approchez cette question du point de vue de la recherche, mais j'aimerais savoir si, personnellement, vous croyez que nous devrions être davantage comme les Américains à cet égard et forcer les entreprises à rapporter de telles choses. À défaut de rapporter, il y aurait des conséquences. Il pourrait y en avoir même si elle rapportait. Comme tenu de cette optique très législative, quelle serait votre opinion en la matière?

M. Dupont : Tout d'abord, il importe de dire qu'une nouvelle loi va très bientôt entrer en vigueur au Canada, et c'est la Loi sur la protection des renseignements personnels numériques. Je crois qu'on est en train de mettre la dernière touche au cadre réglementaire, mais essentiellement, la loi forcera les entreprises à informer le commissaire à la protection de la vie privée des occurrences d'atteintes à la protection des renseignements personnels, du moins, dans un certain nombre de circonstances. Le cas échéant, les entreprises seront également tenues d'informer leurs clients ou leurs employés que de telles fuites se sont produites.

Personnellement et par souci de transparence, je crois que c'est une très bonne chose, un changement positif. J'estime que les entreprises où ces fuites se produisent devraient être tenues d'en informer le public, pas pour les mettre dans leurs petits souliers, mais bien parce que cela ajoute à la transparence et que les consommateurs devraient savoir ce qui se passe avec leurs renseignements personnels. Cela leur permettra de faire des choix mieux éclairés au sujet des entreprises à qui ils décideront de donner leurs affaires et leur confiance, leur argent ou leurs renseignements personnels.

Il y a aussi des mesures qui sont sur le point d'être mises en œuvre en Europe et qui prévoient des amendes salées pour ce type d'incidents. Je crois qu'il est question d'environ 4 p. 100 des revenus annuels. L'approche de l'Europe à l'égard des entreprises où se produisent des fuites de données est beaucoup plus coercitive.

La sénatrice Wallin : Quel est le motif de l'amende? Est-ce pour punir le défaut de rapporter la fuite ou l'occurrence de la fuite?

Mr. Dupont: The breach occurring.

Senator Wallin: Okay.

Mr. Dupont: If the regulatory authority determines that there was a major case of negligence or lack of protective measures implemented.

Senator Wallin: I just have one follow up on this. With the reporting to the Privacy Commissioner, are they then obliged to report to the RCMP or to public safety, or what is the point of just reporting to the Privacy Commissioner?

Mr. Dupont: I'm not a lawyer, so I can't be 100 per cent sure, but I do not believe that they will have any obligation to report to anyone else but the Privacy Commissioner, because the Privacy Commissioner is the authority in charge of enforcing the Digital Privacy Act. It's not an act on data breach notification. It has a data breach component to it, but it's a broader piece of legislation that is under the authority of the Privacy Commissioner.

Senator Wallin: So for actual breaches, there is still no obligation to report to any investigative body, including the RCMP or CSIS if there are international implications?

Mr. Dupont: That is correct.

Senator Wallin: Thank you.

Senator Black: Good morning, sir, and thank you for being here. I don't know whether you had the opportunity to listen to the evidence that we would have heard last night. Did you hear that?

Mr. Dupont: I just read some of the transcripts this morning.

Senator Black: At the end of the session yesterday, I took tremendous comfort thinking, my goodness, maybe the RCMP and Public Safety Canada, or the organization that gentleman referenced, and CSIS have this file under control. I hear what you have shared with us this morning, and I'm not sure that my view is necessarily accurate or that you would necessarily agree with that.

You have pointed out a couple of things in your evidence. You have said it's a crime epidemic, and you do not believe that Canada has the resources to address that. You have also indicated that Canada as a nation is not high on the global success file of countries that are effectively dealing with this. You mentioned Singapore, the Netherlands, the U.K.and the U.S. Yesterday, we heard exactly the opposite, which, of course, is troubling.

M. Dupont : Elle sert à punir l'occurrence de la fuite.

La sénatrice Wallin : D'accord.

M. Dupont : Une amende est donnée si l'autorité réglementaire établit qu'il y a eu une négligence manifeste ou qu'on a omis de mettre en place des mesures de protection.

La sénatrice Wallin : J'aurais une question complémentaire à ce sujet. Après avoir rapporté l'incident au commissaire à la protection de la vie privée, les entreprises seront-elles ensuite obligées d'avertir la GRC ou la sécurité publique? Sinon, pour quelle raison seraient-elles tenues de n'avertir que le commissaire à la protection de la vie privée?

M. Dupont : Je ne suis pas un avocat, alors je ne suis pas sûr à 100 p. 100, mais je ne crois pas qu'elles seront obligées d'avertir qui que ce soit d'autre que le commissaire, puisque c'est lui qui est l'autorité chargée de faire appliquer la Loi sur la protection des renseignements personnels numériques. Ce n'est pas une loi sur la notification des fuites de données. Une partie de la loi porte là-dessus, mais la loi qui est sous l'autorité du commissaire est plus vaste que les simples fuites de données.

La sénatrice Wallin : Si je comprends bien, il n'y a aucune obligation de rapporter les fuites proprement dites à un organisme d'enquête — dont la GRC ou le SCRS —, et ce, même s'il y a des conséquences à l'étranger?

M. Dupont : C'est exact.

La sénatrice Wallin : Merci.

Le sénateur Black : Bonjour, monsieur, et merci de votre présence parmi nous. Avez-vous eu la chance d'écouter le témoignage que nous avons entendu ici, hier soir?

M. Dupont : J'ai lu une partie des transcriptions, ce matin.

Le sénateur Black : À la fin de la séance d'hier, je me suis réjoui de penser que la GRC, Sécurité publique Canada — ou l'organisme dont le témoin a parlé — et le SCRS avaient ce dossier bien en main. J'ai entendu ce que vous nous avez dit ce matin, et je ne suis pas certain que j'ai un portrait fidèle de la réalité ou que vous seriez nécessairement d'accord avec l'idée que je m'en fais.

Dans votre exposé, vous avez souligné deux choses. Vous avez dit que ces crimes atteignaient des proportions épidémiques, et vous avez dit ne pas croire que le Canada ait les ressources voulues pour s'attaquer à ce problème. Vous avez aussi dit qu'en tant que nation, le Canada n'était pas haut sur la liste des pays du monde qui traitent efficacement cette forme de criminalité. Vous avez mentionné Singapour, les Pays-Bas, le Royaume-Uni et les États-Unis. Hier, nous avons entendu tout le contraire, ce qui, bien entendu, est consternant.

I would ask you to comment on that, and then I would ask you to tell us the two or three things that we should be addressing at this committee, from your point of view.

Mr. Dupont: I don't want to contradict anyone from CSIS or the RCMP or Public Safety Canada, because I think they were probably very truthful when they told you yesterday that they had what falls under their responsibility probably under control. But that may only represent a tiny fraction of what is really happening out there.

I think that yesterday, the witness from the RCMP mentioned that there is a tiny, tiny fraction of cyber crimes that are being reported to the police by companies or individuals. In some countries, the statistics seem to show that less than 10 per cent of cyber crimes are being reported to the police. So to the extent that they are probably able to deal with the tiny fraction that is being reported to the police, yes, they probably were correct in their statement, but my worry is that there is probably more than almost 90 per cent of cyber crimes that are not being reported to the police.

They are real crimes. They have real impact on victims and on companies. They can threaten the survivability of SMEs and other companies. They are not being addressed by law enforcement organizations, but they are being addressed sometimes, from a company's perspective, by private cybersecurity investigative companies. The government doesn't necessarily see all the incidents, and that prevents us from having a full picture of what is happening out there and from protecting citizens and consumers on an individual basis who don't have the resources to hire private companies to investigate a cyber fraud.

Yes, the banks are also investing massive amounts of money to protect their consumers. But again, you know, it's a private sector effort. I think that the government probably has a responsibility to do a lot more. The countries that I mentioned are investing billions of dollars to address this problem because they have recognized that this is a strategic issue that will make or break the economic prosperity of their economies.

Senator Black: If you were going to draw our attention to two or three countries around the globe that you think are leading practices, what countries would you suggest?

Mr. Dupont: In terms of the role of government, I would say the U.K. I will pick countries that have similar political and policy experiences so that we maybe would be able to transfer some lessons from them. I would say the U.K. from a government role. I would say Israel and the Netherlands from an economic prosperity approach. They are two smaller countries that don't necessarily have huge resources, like us, and they still manage to do a lot of great things because they have been able to

J'aimerais vous entendre là-dessus, puis j'aimerais que vous nous disiez quelles sont les deux ou trois choses sur lesquelles notre comité devrait insister.

M. Dupont : Je ne veux pas contredire qui que ce soit du SRCS, de la GRC ou de Sécurité publique Canada, car je crois qu'ils disaient l'absolue vérité, hier, et qu'ils ont probablement le contrôle sur ce qui relève d'eux. Sauf que cela ne représente peut-être qu'une petite fraction de ce qui se passe dans le grand monde.

Je crois que c'était hier qu'un témoin de la GRC expliquait que les entreprises et les personnes ne rapportent à la police qu'une minuscule fraction des crimes cybernétiques qui se produisent. Dans certains pays, des statistiques laissent entendre que moins de 10 p. 100 des crimes cybernétiques sont rapportés à la police. Alors, dans la mesure où ils sont probablement capables de traiter avec cette petite fraction qui leur est signalée, oui, leur déclaration était sans doute fidèle à la réalité, mais ce qui m'inquiète c'est de savoir que près de 90 p. 100 des crimes cybernétiques ne sont pas rapportés à la police.

Ce sont des crimes bien réels. Ils ont des répercussions bien réelles sur les victimes et sur les entreprises. Ils peuvent mettre en péril la survie même des PME et d'autres sociétés. Ces crimes ne sont pas combattus par des organismes d'application de la loi, mais parfois, ce sont les entreprises elles-mêmes qui prennent les choses en main ou des sociétés privées spécialisées dans les enquêtes en cybersécurité. Le gouvernement ne voit pas nécessairement tous les incidents, et c'est pour cette raison que nous n'avons pas un portrait complet de la situation et que nous ne sommes pas en mesure de protéger les citoyens. Du reste, sur une base individuelle, les consommateurs n'ont pas les ressources voulues pour retenir les services de sociétés privées aptes à enquêter sur des cyberfraudes.

Oui, les banques investissent elles aussi des sommes colossales pour protéger leurs clients, mais encore une fois, c'est un effort qui vient du secteur privé. Je crois que le gouvernement a la responsabilité de faire beaucoup plus. Les pays dont j'ai parlé investissent des milliards de dollars pour faire face à ce problème parce qu'ils reconnaissent que c'est un enjeu stratégique déterminant pour la prospérité ou la déchéance de leur économie.

Le sénateur Black : Quels sont les deux ou trois pays qui, selon vous, ont des pratiques exemplaires dont nous devrions nous inspirer?

M. Dupont : Pour ce qui est du rôle de l'État, je dirais le Royaume-Uni. Je choisirai des pays qui ont des expériences politiques et stratégiques similaires aux nôtres, puisque cela facilitera le transfert des éventuelles leçons à retenir. Bref, je dirais le Royaume-Uni pour le rôle de l'État. Je dirais Israël et les Pays-Bas pour ce qui est de la prospérité économique. Ce sont deux petits pays qui, comme nous, n'ont pas nécessairement d'énormes ressources, sauf qu'ils arrivent quand même à faire

network and to kind of connect industry, government and academia.

I think that's really a message I would like to share with you today, the need to coordinate a lot better. The government here in Canada is doing great work in coordinating within government. I'm not blaming anyone. I'm just saying that there is so much more we need to do, and we need to connect a lot more different groups of stakeholders if we want to have an impact that will move the needle.

Senator Campbell: Thank you so much for being here today. I'd like to continue on. It's like we heard a tale of two cities. Yesterday we heard that everything is great, we're on top of this, and Canada is a leader in so many different areas. We mainly dealt with underreporting, which again is one of those areas where who knows how you act on that.

I noticed two things. You list all of your partners. It's pretty impressive, but I note that, for instance, there are no banks in your industry partners, although you do have the Bank of Canada down as an internship. Is that an oversight? It would seem to me that the banking sector would be one that you would really want to have involved with cybersecurity.

Mr. Dupont: That's correct. The banking sector is very mature and has been dealing with and addressing cybersecurity issues for probably the longest time compared to other types of organizations.

We engage with the banking sector through a different entity called CCTX, the Canadian Cyber Threat Exchange. That's another great initiative where not only the banking sector but also the telecommunications sector and other large Canadian companies share threat intelligence. I sit on the board of this organization as a permanent invitee to connect this sector and this initiative with the research world. We engage with the banking industry in a different format than through the Smart Cybersecurity Network, but we're very closely connected with them as well.

We have Desjardins, which is not listed yet in the PowerPoint slides I shared with you because we are finalizing the MOU with them, but they are joining the network. Here in Quebec, they are the largest financial institution, covering 80 per cent of consumers here in Quebec and beyond the province.

beaucoup de choses formidables parce qu'ils ont été en mesure de créer une sorte de réseau reliant l'industrie, le gouvernement et les milieux universitaires.

Je crois que le message que je tiens à vous laisser, c'est qu'il est très important que nous nous coordonnions mieux, beaucoup mieux. Ici, au Canada, l'État fait de l'excellent travail de coordination à l'interne. Je ne blâme personne. Tout ce que je dis, c'est qu'il y a tellement plus de choses que nous devons faire. Nous devons tisser des liens entre différents groupes d'intervenants si nous voulons faire pencher la balance du bon côté.

Le sénateur Campbell : Merci beaucoup de votre présence. J'aimerais poursuivre là-dessus. C'est comme si nous avions entendu le conte de deux villes. Hier, on nous a dit que tout allait bien, que nous maîtrisions la situation et que le Canada était une figure de proue dans une foule de domaines. Nous nous occupons surtout de la divulgation déficiente, qui est encore un de ces domaines où il est bien difficile de savoir qui fait quoi.

J'ai remarqué deux choses. Vous énumérez tous vos partenaires. C'est assez impressionnant, mais je constate, par exemple, qu'il n'y a aucune banque parmi vos partenaires du secteur privé, même si vous faites mention de la Banque du Canada pour les possibilités de stages. Est-ce un oubli? Il me semble que le secteur bancaire serait un intervenant privilégié dans le domaine de la cybersécurité.

M. Dupont : C'est exact. Le secteur bancaire est très évolué à cet égard puisqu'il s'occupe de problèmes de cybersécurité depuis probablement bien plus longtemps que les autres types d'organisations.

Nous travaillons avec le secteur bancaire par l'intermédiaire d'une autre entité, appelée ECMC, soit l'Échange canadien de menaces cybernétiques. Il s'agit là d'une autre excellente initiative dans le cadre de laquelle non seulement le secteur bancaire, mais aussi le secteur des télécommunications et d'autres grandes entreprises canadiennes échangent des renseignements sur les menaces. Je siège au conseil d'administration de cette organisation en tant qu'invité permanent afin d'assurer une liaison entre le secteur bancaire, cette initiative et le milieu de la recherche. Nous collaborons avec l'industrie bancaire autrement que par l'entremise du Réseau intégré sur la cybersécurité, quoique nous entretenions des liens très étroits avec ce dernier aussi.

Ainsi, nous collaborons avec Desjardins, qui ne figure pas encore parmi les partenaires mentionnés dans les diapositives PowerPoint que je vous ai remises, car nous nous apprêtons à conclure un protocole d'entente avec cette institution, mais elle va se joindre au réseau. N'oublions pas qu'au Québec, Desjardins est la plus grande institution financière, couvrant 80 p. 100 de la clientèle à l'échelle de la province et au-delà.

Senator Campbell: So you are saying the banks are bringing their maturity to the SERENE-RISC?

Mr. Dupont: No. We are collaborating with them but through a different entity called CCTX. They are sharing the maturity of their approach not only with us but with all other industries in Canada.

Senator Campbell: The second thing is under "Government Partners," I don't see the RCMP anywhere in there.

Mr. Dupont: We have the anti-fraud centre, which is, I believe, a unit within the RCMP. We've also held discussions with the RCMP. We frequently collaborate with them. They attend our conferences. They also send speakers to our events. Although we don't have a formal MOU with the RCMP, we collaborate with them very closely.

Senator Campbell: Lastly, regarding this idea of industry, government and academia coming together, I don't think you're going to have that happen until you get all of these players, including the banks and the RCMP, in there. What I'm hearing is what I believe is classic silos. Each one of these organizations operates independently of each other. Although they say that they collaborate and work together, that's not what I'm hearing. That's not really what I heard yesterday. I agree that you need to bring all of these together, but to do that, somebody has to be in charge of this. I don't know who is in charge of it. I don't know if it's the Mounties. They say no, that they're criminal. CSIS says no unless it's coming from outside of Canada or it's a terrorist threat. The National Cyber Security Directorate — nobody is taking control of this.

I'd like to know who you believe should be leading this. Should it be government leading this? Should it be industry leading this? Should it be research and academia? I don't know, but I'd like to know who it should be.

Mr. Dupont: If you look at the countries I listed as being ahead of the pack, they have all one point in common: the authority leading these efforts is the head of state. It's either the prime minister or the president. It's all coordinated under the office of the prime minister or the office of the president. The reason for that is to send a strong signal that this is such an important issue that the prime minister takes the leadership on this to ensure that all the agencies are aligned, that industry collaborates to the table and that academia is very much aware of the importance of this societal challenge. In all the countries that are defined as leaders, the office in charge is the office of the president or the office of the prime minister.

Le sénateur Campbell : Donc, vous dites que les banques mettent à profit leur expérience dans le cadre du Réseau intégré sur la cybersécurité?

M. Dupont : Non. Nous collaborons avec elles, mais par le truchement d'une autre entité appelée ECMC. Elles nouent des liens non seulement avec nous, mais aussi avec toutes les autres industries au Canada pour mettre à contribution les résultats de leur approche.

Le sénateur Campbell : La deuxième chose que j'ai remarquée, c'est qu'il n'y a aucune mention de la GRC dans la liste des partenaires gouvernementaux.

M. Dupont : Il y a le Centre antifraude, qui relève, sauf erreur, de la GRC. Nous avons également tenu des discussions avec la GRC. Nous collaborons fréquemment avec ses représentants. Ils assistent à nos conférences. Ils nous envoient aussi des conférenciers. Même si nous n'avons pas de protocole d'entente officiel avec la GRC, nous collaborons très étroitement avec elle.

Le sénateur Campbell : Enfin, pour ce qui est de l'idée d'amener l'industrie, le gouvernement et le milieu universitaire à unir leurs efforts, je crois que cela ne se produira pas tant que vous ne ferez pas intervenir tous les joueurs, y compris les banques et la GRC. D'après ce que j'entends dire, c'est le cas classique du travail en vase clos. Chacune de ces organisations agit indépendamment l'une de l'autre. Même si elles affirment collaborer et travailler ensemble, ce n'est pas ce que les gens me disent. Ce n'est pas ce que j'ai entendu hier. Je conviens qu'il faut rassembler tous ces intervenants, mais pour ce faire, quelqu'un doit piloter cette initiative. J'ignore à qui revient cette tâche. Je ne sais pas si c'est la GRC qui doit assumer cette responsabilité. Elle prétend que non, parce qu'elle s'occupe d'enquêtes criminelles. Le SCRS dit non, lui aussi, sauf si la menace provient de l'extérieur du Canada ou s'il s'agit d'une menace terroriste. La Direction générale de la cybersécurité nationale… bref, personne ne prend ce dossier en main.

J'aimerais savoir qui, d'après vous, devrait diriger cette initiative. Le gouvernement? L'industrie? Le milieu de la recherche et les universités? Je ne sais pas, mais j'aimerais bien connaître la réponse.

M. Dupont : Si on examine les pays que j'ai énumérés comme étant en tête du peloton, on constate qu'ils ont tous un point en commun: l'autorité qui dirige ces efforts est le chef d'État. C'est soit le premier ministre, soit le président. Le tout est coordonné sous l'égide du cabinet du premier ministre ou du président. Le but est d'envoyer un message clair: c'est un enjeu tellement important que le premier ministre prend les devants dans ce dossier pour s'assurer que tous les organismes travaillent main dans la main, que l'industrie apporte sa contribution et que le milieu universitaire est très conscient de l'importance de ce défi sociétal. Dans tous les pays qui sont définis comme des

Senator Campbell: That's what I wanted to hear. Thank you very much.

Senator Unger: Thank you very much for your presentation. I certainly concur with what all of my colleagues have been saying about yesterday's meeting.

From the witnesses yesterday, it sounds like cyberattacks on businesses are inevitable and just a cost of doing business. Would that hold true for our national infrastructure? Are attacks inevitable? Do we have adequate systems to prevent them? If we do, why wouldn't that be possible for business as well?

Mr. Dupont: I think you're right when you state that attacks are inevitable.

We learned last week that the NSA, the National Security Agency in the U.S., was hacked. That's probably the best-resourced intelligence agency in the world. If the NSA gets hacked, everyone will probably be hacked at one point. We learned that because the Israeli intelligence hacked into Kaspersky, another cybersecurity outfit, and they looked at Russian intelligence hacking the NSA. Everyone is hacking everyone, and businesses will not be immune to that phenomenon and wave of hacking.

To answer the second part of your question about our critical infrastructure, I think that, yes, they will probably also be exposed to hacks, but they have very limited metrics and data to understand their level of vulnerability as well as their level of protection. It's hard to make statements that are very reliable when you don't have strong data to back them up. I think one of the challenges in future years for critical infrastructure, companies and governments will be to be able to produce data and evidence that will tell us where we should direct our energies, efforts and investments to make sure that we reinforce our cybersecurity.

Finally, we will also need to develop a concept that is one possible answer to this new reality of everyone being exposed to hacks, which is the concept of resilience. How can we make sure our critical infrastructures in companies are still able to operate even in a hostile environment where they can assume that some of their systems are under attack or even compromised? I think that we also need to develop a complementary way of answering cybersecurity challenges, which is to make organizations more robust and resilient and able to adapt to this new environment, which is going to be here for a long time.

chefs de file, la responsabilité incombe au cabinet du président ou du premier ministre.

Le sénateur Campbell : C'est ce que je voulais entendre. Merci bien.

La sénatrice Unger : Merci beaucoup de votre exposé. J'abonde certainement dans le sens de ce que tous mes collègues ont dit au sujet de la réunion d'hier.

À en juger par les témoignages d'hier, on dirait que les cyberattaques contre les entreprises sont inévitables et qu'il s'agit simplement d'un prix à payer pour faire des affaires. Cela vaut-il aussi pour nos infrastructures nationales? Les attaques sont-elles inévitables? Disposons-nous des systèmes adéquats pour les empêcher? Si oui, pourquoi alors cela ne serait-il pas possible pour les entreprises également?

M. Dupont : Je crois que vous avez raison de dire que les attaques sont inévitables.

Nous avons appris la semaine dernière que la NSA, la National Security Agency des États-Unis, avait été victime de piratage. Ce service du renseignement est probablement doté des meilleures ressources au monde. Si la NSA peut se faire pirater, alors tout le monde le sera sans doute à un moment donné. Nous avons appris cette nouvelle parce que le service du renseignement israélien a piraté Kaspersky, un autre organisme de cybersécurité, et a constaté que son homologue russe s'était introduit dans le système de la NSA. Tout le monde pirate tout le monde, et les entreprises ne seront pas à l'abri de ce phénomène ni de la vague de piratage.

Pour répondre à la deuxième partie de votre question sur nos infrastructures essentielles, je pense que oui, les entreprises seront probablement, elles aussi, exposées au piratage, mais elles ont des paramètres et des données trop limités pour comprendre leur degré de vulnérabilité ainsi que leur niveau de protection. Il est difficile de faire des déclarations très fiables lorsqu'on ne dispose pas de données solides pour les étayer. Selon moi, un des défis à relever au cours des prochaines années du point de vue des infrastructures essentielles, des entreprises et des gouvernements, ce sera de pouvoir produire des données et des preuves qui nous indiqueront où concentrer nos énergies, efforts et investissements pour nous assurer de renforcer notre cybersécurité.

Enfin, nous devons également élaborer un concept qui se veut une réponse possible à cette nouvelle réalité, à savoir que personne n'est à l'abri du piratage, et il s'agit du concept de résilience. Comment pouvons-nous veiller à ce que les infrastructures essentielles au sein des entreprises soient toujours en état de fonctionner même dans un environnement hostile où il y a lieu de supposer que certains de leurs systèmes risquent d'être attaqués, voire compromis? Je crois que nous devons également trouver une façon complémentaire de répondre aux défis de cybersécurité, c'est-à-dire rendre les organisations plus

Senator Unger: I heard recently that one of our five national banks was sending people to Israel to be trained in cybersecurity. You mentioned that banks have very good and reliable, if you can use that word, security. Obviously this bank felt that it needed to go to a country that teaches people better. I guess that's the new brave world that we're in. Thank you.

The Deputy Chair: Mr. Dupont, did you have any comment with respect to banks going to Israel?

Mr. Dupont: Yes and no. I think what they're doing, when they're going to Israel, is they're indicating that this is a global problem that has to be addressed globally and some of the expertise is not necessarily in Canada. My aim today is not to generate fear among us because there is expertise in Canada, and it's not all doom and gloom, but when banks are sending people to Israel to be trained, they are acknowledging that this is a global problem and some of the expertise is overseas and we need to connect with that expertise as well.

Senator Wetston: Thank you for coming today. I wanted to pursue this area of cybersecurity somewhat differently. I asked this of one of the witnesses yesterday, and my thought was that the Internet is becoming more of the 21st century crime scene. The reason I mention that is because obviously we had RCMP officers here as well as CSIS.

The question I wanted to get your opinion on is you recall very well the financial crisis of 2007-08. It's now the tenth year anniversary of the financial crisis. Much of what occurred in that crisis was enabled by technology. The interconnectivity allowed the risk to spread from nation to nation, which created a global recession. I think you might agree with me on that point.

My question to you is: Because the world is faster and the world is smaller because of technology, we often look at technology and say it is technology that has created the problem, when, frankly, probably technology has enabled the problem but not created the problem. The problem is with human behaviour. Are you able to comment on your views with respect to the relationship between behaviour and technology from the perspective of your work?

Mr. Dupont: Yes. I'll try not to pontificate too much. I entirely agree with you. I would add a third component to your model of interactions. It is technology, behaviours and policies. The way technology develops can be strongly influenced by

fortes et plus résilientes et être en mesure de s'adapter à ce nouvel environnement, qui restera ici pendant longtemps.

La sénatrice Unger : J'ai récemment entendu dire qu'une des cinq banques canadiennes envoie des gens à Israël pour qu'ils y suivent une formation sur la cybersécurité. Vous avez mentionné que les banques ont des systèmes de sécurité très efficaces et très fiables, pour ainsi dire. Visiblement, cette banque a jugé bon d'aller dans un pays qui offre une meilleure formation aux gens. Je suppose que c'est le nouveau monde merveilleux dans lequel nous vivons. Merci.

Le vice-président : Monsieur Dupont, aviez-vous des commentaires à faire à ce sujet?

M. Dupont : Oui et non. Je crois qu'en envoyant des employés à Israël, les banques indiquent, d'une part, qu'il s'agit d'un problème planétaire qui doit être réglé à l'échelle mondiale et, d'autre part, que le Canada ne dispose pas nécessairement de tout le savoir-faire en la matière. Mon but, aujourd'hui, n'est pas de semer la peur chez vous parce que le Canada dispose bel et bien des compétences voulues, et ce n'est pas tout noir, mais quand les banques envoient des gens à Israël pour leur permettre de suivre une formation, elles reconnaissent qu'il s'agit d'un problème mondial et que certaines des compétences se trouvent à l'étranger, d'où la nécessité d'établir des liens avec ces experts.

Le sénateur Wetston : Merci d'être des nôtres aujourd'hui. Je voulais aborder le sujet de la cybersécurité sous un angle quelque peu différent. J'ai posé la même question à l'un des témoins d'hier en partant de l'idée qu'Internet devient de plus en plus une scène de crime au XXIe siècle. Si je le mentionne, c'est parce que nous avons également reçu, de toute évidence, des agents de la GRC ainsi que des représentants du SCRS.

La question que je voulais vous poser concerne la crise financière de 2007-2008, un événement dont on se souvient très bien. C'était il y a 10 ans. L'essentiel de ce qui s'est produit pendant cette crise a été attribuable à la technologie. En effet, l'interconnectivité a permis la propagation du risque d'un pays à un autre, ce qui a créé une récession mondiale. Je crois que vous serez peut-être d'accord avec moi sur ce point.

J'en viens donc à ma question : puisque le monde évolue de plus en plus rapidement et que les frontières se rétrécissent de plus en plus grâce à la technologie, nous avons souvent tendance à penser que c'est la technologie qui crée le problème, alors que ce n'est pas le cas en réalité: oui, la technologie contribue probablement au problème, mais elle ne le crée pas. Le problème tient au comportement humain. Pouvez-vous nous dire ce que vous pensez de la relation entre les comportements et les technologies dans le contexte de votre travail?

M. Dupont : Oui. J'essaierai de ne pas trop pontifier. Je suis tout à fait d'accord avec vous. En revanche, j'ajouterai un troisième composant à votre modèle d'interactions: technologies, comportements et politiques. La façon dont la technologie évolue

policy. So far, we have been very shy about regulating technology. The rationale has been that if we regulate technology and the Internet too much, we will stifle innovation and that will be a bad thing. Now we are learning that we have under-regulated technology, and we are paying the price because we have allowed technology to develop very chaotically, and it's hard for us to take back control. I mean in democracies. I'm not advocating doing what China is doing or Russia is doing with technology and regulation, but there is still a level of protection that we must be providing to citizens.

peut être fortement influencée par les politiques. Jusqu'à présent, nous n'avons pas trop osé réglementer les technologies. Le raisonnement est le suivant: si nous réglementons trop les technologies et Internet, nous étoufferons l'innovation, et ce sera une mauvaise chose. Or, nous apprenons maintenant que nous n'avons pas suffisamment réglementé les technologies, et nous en payons le prix parce que nous avons permis un développement très chaotique dans ce domaine, d'où la difficulté que nous éprouvons à reprendre le tout en main. Je parle de la situation dans les démocraties. Je ne préconise pas l'approche adoptée par la Chine ou la Russie en matière de technologie et de réglementation, mais nous devons tout de même offrir une certaine protection aux citoyens.

To your initial question of behaviour and technology, I also agree that we probably need to do a much better job of training people and raising awareness as to what technology enables people to do and the risks that are coming out of technology. At the same time, very often people are appropriating technology in ways that were never anticipated by the designers of those technologies. The inventors of the Internet 50 years ago never imagined that the Internet would become so embedded into every single aspect of human activity.

Pour répondre à votre question initiale sur les comportements et les technologies, je suis d'avis, moi aussi, que nous devons probablement faire mieux pour former les gens et les sensibiliser non seulement aux possibilités offertes par les technologies, mais aussi aux risques qui en découlent. En même temps, il arrive très souvent que les gens s'approprient des technologies et s'en servent à des fins qui n'avaient jamais été prévues par les concepteurs de ces technologies. Il y a 50 ans, les inventeurs d'Internet n'auraient jamais imaginé qu'Internet serait si présent dans les moindres aspects de l'activité humaine.

That's why we probably need to get — and that's one of the objectives of our network — the computer engineers inventing the technology of tomorrow to also understand the security and privacy implications of what they are designing. There is this concept of privacy by design, security by design, and we probably need to do a much better job of training computer engineers in those practices and disciplines to ensure that the new technologies that will be deployed in smart cities, in the Internet of Things, will have much stronger security and privacy features than what we have seen in the past.

Voilà sans doute pourquoi nous devons — et c'est l'un des objectifs de notre réseau — amener les ingénieurs informaticiens qui inventent la technologie de demain à comprendre également les répercussions de leurs inventions sur la sécurité et la protection de la vie privée. Il y a le principe de la protection de la vie privée et de la sécurité dès la conception, et nous devons probablement consacrer beaucoup plus d'efforts à la formation des ingénieurs informaticiens au sujet de ces pratiques ou disciplines pour nous assurer que les nouvelles technologies qui seront déployées dans les villes intelligentes, dans l'Internet des objets, auront des fonctions plus solides en matière de sécurité et de protection de la vie privée que ce que nous avons vu dans le passé.

Senator Wetston: This is really to put this on the record because I don't know the answer to this. It's my feeling that the regulated banks and insurance companies who are regulated by OSFI, the Office of the Superintendent of Financial Institutions, might — and I don't know and it would be interesting to find out — require the banks to report data breaches, unlike potentially other industry sectors that may not have that reporting responsibility. I'm simply following up from Senator Massicotte and Senator Wallin's question. We should probably try to get an answer to that question because obviously financial institutions are important. You may not have an answer to that question, so I am simply noting it.

Le sénateur Wetston : J'aimerais faire une observation simplement aux fins du compte rendu parce que je ne connais pas la réponse à la question. Dans le cas des banques et des compagnies d'assurance qui sont réglementées par le BSIF, le Bureau du surintendant des institutions financières, il me semble — et je n'en suis pas sûr, mais il serait intéressant de tirer les choses au clair — que les banques sont tenues de signaler les atteintes à la protection des données, contrairement peut-être à d'autres secteurs d'activité qui pourraient ne pas avoir une telle obligation. Je fais simplement suite à la question posée par le sénateur Massicotte et la sénatrice Wallin. Nous devrions probablement essayer d'obtenir une réponse à ce sujet parce que, de toute évidence, les institutions financières sont importantes. Vous n'avez peut-être pas de réponse à cette question, alors je ne fais que la poser.

The other thing I might follow up with is that when I asked you my question about interconnectivity, which I think you agree obviously enables this, and when I was discussing risk — and the Banking Committee is often concerned about risk in the financial markets — the risk that may have been spread from country to country, from institution to institution, was not necessarily as a result of bad behaviour. Whether it's good behaviour or bad behaviour, that risk will spread and be very difficult to control and manage in the financial markets. I's the technology operating in the way that perhaps the initial developers did not intend, as you point out. I don't know if you have any comments on this. I was looking at it from both perspectives.

Mr. Dupont: I also agree with you. I will add an additional layer of complexity because we are about to add to this mix artificial intelligence that will have a lot of autonomy and be making autonomous decisions and will increase the velocity of the spread of certain decisions and the interconnectivity, with very limited human control. That's also something that we need to think about now because the progress and the speed of innovation in the field of artificial intelligence is huge, and we need to also take stock of what's going to happen when we're going to hand over the keys of technological infrastructure to AIs — maybe not tomorrow, but very quickly.

Senator Wetston: You will have a good future if you're an algorithm, is your point.

Senator Enverga: Thank you for the presentation. Let me go back to what you mentioned earlier, that cybersecurity is a major priority of this country. You mentioned that there are so many things we have to do. My question is, what do we have to do? Can you give me three things that the government has to do to secure our network or have cybersecurity?

Mr. Dupont: I'll give you only one. I think that the government is doing very well in securing its own systems, but it needs to coordinate the efforts of provincial and municipal governments, certain industries and consumers. I think one thing that would probably have an impact is the creation of a new agency, probably under the Office of the Prime Minister, that would have this role and responsibility of coordinating efforts.

For now, we are suffering from an excess of fragmentation and everyone has a slice of responsibility. Because everything is interconnected and interdependent, it would be useful to have an overarching agency that would have the capacity and the authority to understand the multiplicity of efforts being undertaken, to incentivize and prioritize some of them and to

Il y a un autre point sur lequel j'aimerais revenir. Quand je vous ai posé ma question sur l'interconnectivité, grâce à laquelle tout cela est possible, vous en conviendrez sans doute, j'ai parlé de risque — et le comité des banques s'intéresse souvent aux risques sur les marchés financiers —, mais il se trouve que le risque susceptible de s'être proposé d'un pays à l'autre, d'une institution à l'autre, n'est pas nécessairement attribuable à un mauvais comportement. Qu'il s'agisse d'un bon ou d'un mauvais comportement, ce risque se répandra, et on aura beaucoup de difficulté à le maîtriser et à le gérer sur les marchés financiers. Comme vous l'avez dit, il se peut que la technologie fonctionne d'une façon bien différente de ce que les créateurs avaient prévu au départ. Je ne sais pas si vous avez des commentaires à ce sujet. Je voulais donc aborder la question sous ses deux angles.

M. Dupont : Je suis d'accord avec vous. J'ajouterai un autre élément de complexité, à savoir le recours imminent à l'intelligence artificielle, ce qui permettra beaucoup d'autonomie au chapitre de la prise de décisions, augmentera la vitesse de propagation de certaines décisions et favorisera l'interconnectivité, moyennant une intervention humaine très limitée. C'est une chose à laquelle nous devons penser dès maintenant parce que les progrès et les innovations dans le domaine de l'intelligence artificielle se multiplient à un rythme effréné, et nous devons également réfléchir à ce qui arrivera le jour où nous déléguerons la gestion des infrastructures technologiques aux intelligences artificielles — peut-être pas demain, mais très bientôt.

Le sénateur Wetston : Autrement dit, l'avenir sera prometteur pour les algorithmes.

Le sénateur Enverga : Merci de l'exposé. J'aimerais revenir sur ce que vous avez mentionné tout à l'heure, à savoir que la cybersécurité est une des grandes priorités de notre pays. Vous avez dit que beaucoup de mesures s'imposent. Ma question est la suivante: que devons-nous faire? Pouvez-vous me nommer trois mesures que le gouvernement doit prendre pour protéger notre réseau ou pour assurer la cybersécurité?

M. Dupont : Je vais vous en indiquer une seule. Je crois que le gouvernement s'en tire très bien pour ce qui est de protéger ses propres systèmes, mais il doit continuer de coordonner les efforts des gouvernements provinciaux, des administrations municipales, de certaines industries et des consommateurs. À mon avis, une mesure qui pourrait avoir une incidence, c'est la création d'un nouvel organisme, probablement sous l'égide du Cabinet du premier ministre, organisme dont le rôle serait justement de coordonner les efforts.

Pour l'instant, nous souffrons d'une fragmentation excessive, car la responsabilité est répartie entre tous les intervenants. Puisque tout est lié et interdépendant, il serait utile d'avoir un organisme qui chapeauterait le tout et qui serait doté des capacités et des pouvoirs nécessaires pour comprendre la multiplicité des efforts déployés afin d'en promouvoir certains

collect metrics that would enable us to have a general understanding of the situation.

I would say one thing would be the creation of a new cybersecurity agency that wouldn't steal responsibilities from existing organizations but would be the coordinating point for the whole of government.

Senator Enverga: With this new agency, are there other countries that have the same model? Is it the same thing for Singapore or maybe China, as you earlier indicated?

Mr. Dupont: Yes.

Senator Enverga: I asked this yesterday with regard to our status right now, and somehow I didn't get a direct answer. On a scale of one to ten, how would you rate our cybersecurity, our infrastructure and our preparedness as a country?

Mr. Dupont: Well, as a scientist, I couldn't answer your question because we don't have any data, or very limited data. The data we have is not useful.

Senator Enverga: That's helpful for us. Thank you.

Mr. Dupont: It's not a direct answer either, I'm afraid.

[*Translation*]

Senator Massicotte: We were talking about breaches of confidentiality earlier. Would it not be useful for victims of a security breach to be compensated, or to have the right to sue companies that have not taken the measures required to protect confidential information? At some stage or other, we have all signed waivers releasing companies from responsibility? But should they perhaps be held responsible? If there were consequences for companies that had not taken the required measures, they might work harder to protect us in the future. Is that a good idea? Is it possible? Is it doable?

Mr. Dupont: Once again, as I said, I am not a lawyer. I imagine that everything is doable. Before allowing that type of lawsuit, it might be useful to help companies who hold those that personal information to understand what is expected of them and the security measures that have been shown to produce tangible results in terms of protection. Currently, organizations and companies have very few guidelines that let them know with any certainty about which measures they might take that will be effective.

selon l'ordre de priorité, en plus de recueillir des données qui nous permettraient d'avoir une idée générale de la situation.

Je dirais donc qu'une des mesures à prendre serait de créer un nouvel organisme de cybersécurité qui n'empiéterait pas sur les responsabilités des organismes existants, mais qui servirait de point de coordination pour l'ensemble du gouvernement.

Le sénateur Enverga : Parlant de créer un nouvel organisme, y a-t-il d'autres pays qui ont adopté le même modèle? Est-ce le cas pour Singapour ou peut-être la Chine, comme vous l'avez dit plus tôt?

M. Dupont : Oui.

Le sénateur Enverga : J'ai posé hier une question sur le bilan de la situation actuelle au Canada et, pour une raison quelconque, je n'ai pas réussi à obtenir une réponse directe. Sur une échelle de 1 à 10, comment évalueriez-vous la cybersécurité, les infrastructures et l'état de préparation de notre pays?

M. Dupont : Eh bien, en tant que scientifique, je ne pourrais pas répondre à votre question, car nous n'avons aucune donnée ou, à tout le moins, les données dont nous disposons sont très limitées et, par conséquent, inutiles.

Le sénateur Enverga : Cette information nous est utile. Merci.

M. Dupont : Je crains que ce ne soit pas non plus une réponse directe.

[*Français*]

Le sénateur Massicotte : On a parlé plus tôt des bris de confidentialité. Ne serait-il pas utile que les victimes d'un manquement à la sécurité soient indemnisées ou aient le droit de poursuivre les compagnies qui n'auraient pas pris les mesures nécessaires pour protéger les renseignements confidentiels? Nous avons tous, à un moment ou un autre, signé une décharge quant à la responsabilité des compagnies. Toutefois, peut-être devraient-elles être tenues responsables? Si on imposait des conséquences aux compagnies qui n'ont pas pris les mesures nécessaires, celles-ci s'assureraient de mieux nous protéger à l'avenir. Est-ce une bonne idée? Est-ce possible? Est-ce faisable?

M. Dupont : Encore une fois, comme je l'ai indiqué, je ne suis pas juriste. J'imagine que tout est faisable. Avant de permettre ce type de poursuite, il pourrait être utile d'aider les entreprises qui détiennent ces renseignements personnels à comprendre ce à quoi on s'attend d'elles et les mesures de sécurité qui ont été démontrées comme produisant des résultats tangibles en matière de protection. À l'heure actuelle, les organisations et les entreprises disposent de très peu de directives qui leur permettent de savoir avec certitude quelles mesures elles peuvent prendre qui seront efficaces.

In a few minutes, you will be hearing from two officials from the Communications Security Establishment, which is actually trying to distribute information about the issue. The information remains incomplete. That information will be useful. Before we let consumers sue large companies on their own, which is not likely to be a fair fight, it could be helpful to send companies, large and small, clearer expectations and more specific guidelines on the levels of the security expected from them. At that point, if they do not implement the necessary measures, we could then eventually foresee penalties or allow lawsuits if we see that they have not done the basic minimum.

[*English*]

Senator Unger: I have a follow-up question to one I asked yesterday. Researchers at a university in Flanders, Belgium, discovered a way for an attacker to read sensitive information that is sent over Wi-Fi networks using WPA2. It affected tablets and e-readers. It had significant impact — you're probably aware of it — affecting services such as Amazon and Echo. Apparently the answer was yes, the government knew about it in February and they did whatever they had to do about it. But if this is so widely affecting people who use Wi-Fi and tablets and all of these things, why weren't we told about this? What is the obligation? Google gets a patch and they push it through, but people don't know that this has happened.

Mr. Dupont: I think an answer to your question might be that there are so many alerts and so many incidents and vulnerabilities that get discovered, that it's just a matter of prioritizing. I think that government agencies have been very busy over the past few months and during the summer trying to warn people about ransomware, for example, and cryptoware, all these malicious applications that encrypt all your data and you have to pay a ransom to regain access.With the limited resources that government agencies have, they may have chosen to prioritize something that was happening to a fairly large number of people here in Canada and to maybe leave for later this case of the WPA2 vulnerability, which was more something that came out of a researcher's lab than something that was happening in the wild.

Senator Unger: Thank you.

The Deputy Chair: Colleagues, join me in thanking Dr. Benoît Dupont, who is a scientific director for the Smart Cybersecurity Network. He's the Canada Research Chair in

Vous entendrez dans quelques minutes deux représentants du Centre de la sécurité des télécommunications, lequel essaie justement de diffuser de l'information à ce sujet. Cependant, l'information demeure incomplète. Cette information sera utile. Avant de laisser les consommateurs poursuivre de grandes entreprises à titre individuel, ce qui risque d'être un combat inégal, il pourrait être intéressant de transmettre aux grandes et aux petites entreprises des attentes plus claires et des directives plus explicites sur les niveaux de sécurité auxquels on s'attend de leur part. À partir de là, si elles ne mettent pas en place les mesures nécessaires, on pourra ensuite, éventuellement, envisager des pénalités ou autoriser des poursuites si on se rend compte qu'elles n'ont pas fait le strict nécessaire.

[*Traduction*]

La sénatrice Unger : J'ai une question à vous poser pour donner suite à celle que j'ai formulée hier. Des chercheurs d'une université de Flandre, en Belgique, ont découvert une façon pour un pirate de lire les renseignements de nature délicate transmis à l'aide de réseaux Wi-Fi protégés par le protocole WPA2. Ce problème touchait les utilisateurs de tablettes et de liseuses numériques. Comme vous le savez probablement, cela a eu des répercussions considérables sur des services tels que ceux offerts par Amazon et Echo. Apparemment, oui, le gouvernement connaissait l'existence du problème en février, et il a fait ce qu'il fallait faire pour y remédier. Toutefois, si ce problème touche un nombre aussi important de gens qui utilisent des réseaux Wi-Fi, des tablettes et tous les appareils de ce genre, pourquoi n'en avons-nous pas été informés? Quelles obligations existent à cet égard? Google met au point un correctif et le distribue, mais les gens ignorent que le problème est survenu.

M. Dupont : Je pense qu'une des réponses à votre question pourrait être qu'en raison de la découverte d'un grand nombre d'alertes, d'incidents et de vulnérabilités, le gouvernement doit établir des priorités. Je crois qu'au cours des derniers mois et de l'été, les organismes gouvernementaux ont été très absorbés par leurs tentatives visant à mettre les gens en garde contre, par exemple, les rançongiciels, les crypto-verrouilleurs et toutes les applications malveillantes qui chiffrent l'ensemble de vos données et vous forcent à payer une rançon pour y avoir de nouveaux accès. Compte tenu des ressources limitées dont disposent les organismes gouvernementaux, il se peut qu'ils aient choisi d'accorder la priorité à un problème qui touchait un nombre assez important de Canadiens et de remettre à plus tard la question de la vulnérabilité du protocole WPA2, ce problème ayant été découvert en laboratoire par des chercheurs plutôt que dans la nature.

La sénatrice Unger : Merci.

Le vice-président : Chers collègues, veuillez vous joindre à moi pour remercier M. Benoît Dupont, qui est directeur scientifique du Réseau intégré sur la cybersécurité. Il est aussi titulaire de la Chaire de recherche du Canada sur la sécurité,

Security, Identity and Technology. Dr. Dupont is also a professor at the School of Criminology at the University of Montreal.

[*Translation*]

Thank you very much for meeting with us today, Professor Dupont.

Mr. Dupont: Thank you for inviting me.

[*English*]

The Deputy Chair: We will now hear from our second panel of witnesses today. I'm pleased to welcome the Communications Security Establishment, which was referred to a number of times during our hearing yesterday. We are pleased to hear you are here to fill in the gaps, Mr. Scott Jones, Deputy Chief, IT Security, and André Boucher, Director General, Cyber Security Partnerships.

Thank you very much for being here. I understand that you have a presentation to make and then we'll engage in a question and answer dialogue. Thank you.

Scott Jones, Deputy Chief, IT Security, Communications Security Establishment: Thank you very much. My name is Scott Jones, and I'm the Assistant Deputy Minister responsible for the IT Security Program at the Communications Security Establishment. With me is André Boucher, Director General of Cyber Security Partnerships. It is our pleasure to appear before you today as you undertake your study on cybersecurity and cyberfraud.

[*Translation*]

This topic is both timely and extremely important. Canada, as you are well aware, is among the most connected countries in the world. Every day we are witness to stories of how online commerce is driving economic growth and creating opportunities in all sectors of the economy, including online banking and online sales. But, of course, Canadians can only reap the benefits of online commerce when they can conduct their online activities with confidence and trust.

[*English*]

Unfortunately, we've all borne witness to cyber compromises that result in significant financial loss, loss to intellectual property and even loss to a company's reputation. Today's cyber-threat actors represent different threat levels, motivations and capabilities. They include state actors, hacktivists, criminals and terrorists capable of a broad range of disruption, from ransomware attacks to the exposure of personal information.

l'identité et la technologie. De plus, M. Dupont enseigne à l'École de criminologie de l'Université de Montréal.

[*Français*]

Merci beaucoup, professeur Dupont, d'être venu nous rencontrer aujourd'hui.

M. Dupont : Merci de m'avoir invité.

[*Traduction*]

Le vice-président : Nous allons maintenant entendre notre deuxième groupe de témoins de la journée. J'aimerais souhaiter la bienvenue aux représentants du Centre de la sécurité des communications, qui a été mentionné à plusieurs reprises au cours de notre audience d'hier. Il s'agit de M. Scott Jones, chef adjoint, Sécurité des TI, et de M. André Boucher, directeur général, Partenariats en cybersécurité. Nous sommes heureux d'apprendre que vous êtes ici pour combler certaines lacunes en matière d'information.

Je vous remercie beaucoup de votre présence. Je crois comprendre que vous avez un exposé à donner. Nous échangerons ensuite des questions et des réponses. Merci.

Scott Jones, chef adjoint, Sécurité des TI, Centre de la sécurité des télécommunications : Merci beaucoup. Je m'appelle Scott Jones, et je suis sous-ministre adjoint de la Sécurité des TI, au Centre de la sécurité des télécommunications. André Boucher, directeur général des Partenariats en cybersécurité, m'accompagne aujourd'hui. Nous sommes heureux d'être des vôtres pour vous assister dans votre étude sur la cybersécurité et la cyberfraude.

[*Français*]

Il s'agit d'un sujet fort à propos et extrêmement important. Comme vous le savez, le Canada fait partie des pays comptant le plus grand nombre de connexions à Internet. Chaque jour, nous entendons parler de la façon dont le commerce électronique stimule la croissance économique et offre de nouvelles occasions à tous les secteurs de l'économie, ce qui comprend, entre autres, les services bancaires et les ventes en ligne. Bien entendu, les Canadiens ne peuvent récolter les fruits du commerce électronique que s'ils sont en mesure de mener en toute confiance leurs activités en ligne.

[*Traduction*]

Malheureusement, nous avons tous été témoins de cybercompromis qui ont mené à d'importantes pertes financières, ou encore porté atteinte à la propriété intellectuelle ou à la réputation d'une entreprise. De nos jours, les auteurs de cybermenaces ont des motivations et des capacités diverses, et présentent différents niveaux de menaces. Il s'agit notamment d'auteurs parrainés par un État, d'hacktivistes, de criminels et de terroristes capables de provoquer maintes perturbations, allant

I can tell you, as the head of IT security for CSE, the government's lead technical cyberagency, we are very concerned about the vulnerabilities Canadians face online from these threats actors. My goal today is to answer your questions and leave you with a better understanding of who we are, what we do and how we work with our governmental partners and, in particular, the private sector to help protect Canada's important information.

[*Translation*]

As this is my first time appearing before this committee, please allow me to take a few moments to introduce CSE. CSE is one of Canada's key security and intelligence organizations. Our mandate and authorities are defined in the National Defence Act, and we report to the Minister of National Defence.

Our mandate is comprised of three parts. The first part of our mandate, Part A, involves the collection of foreign intelligence in accordance with Government of Canada intelligence priorities. The second part of our mandate, and the work that I lead, Part B, involves providing advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada. And finally, the third part of our mandate, Part C, is the provision of technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

CSE is Canada's centre of excellence for cyberoperations. We use our cyber and technical expertise to monitor federal government systems in order to identify, prepare for, and respond to sophisticated cyberthreats.

Our work also extends beyond the federal government. Because cybersecurity is everyone's responsibility, we work to support the private sector, including critical infrastructure operators, by sharing cyberthreat information and mitigation advice. This helps them better protect their systems and the important information they contain.

[*English*]

Partnerships are key to our success. We know that effective information sharing can help manage and mitigate the impact of cyber-threats, and that's why we work closely with key partners, like Public Safety, the Canadian Cyber Incident Response Centre, the Canadian Cyber Threat Exchange and the Canadian

des attaques par rançongiciel à la divulgation de renseignements personnels.

Je peux d'ailleurs vous dire qu'à titre de responsables de la Sécurité des TI au CST, le principal organisme technique chargé de la cybersécurité du gouvernement, nous nous préoccupons grandement des vulnérabilités auxquelles les Canadiens s'exposent en ligne en raison de ces auteurs de menaces. Mon objectif aujourd'hui est de répondre à vos questions et de vous aider à mieux comprendre ce qu'est le CST, ce qu'il fait et la façon dont il collabore avec ses partenaires du gouvernement et, plus particulièrement, avec le secteur privé, pour contribuer à protéger l'information importante du Canada.

[*Français*]

Comme il s'agit de mon premier témoignage devant ce comité, permettez-moi de prendre quelques instants pour vous parler du CST. Le CST et l'un des principaux organismes de sécurité et de renseignement du Canada. Le mandat du CST est énoncé dans la Loi sur la défense nationale et l'organisme relève du ministre de la Défense nationale.

Notre mandat compte trois volets. La partie A comprend la collecte de renseignements étrangers, conformément aux priorités en matière de renseignement du gouvernement du Canada. La deuxième partie de notre mandat, la partie B, autorise le CST à fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada. Ce sont les activités qui sont menées sous ma direction. Enfin, le troisième volet de notre mandat, la partie C, consiste à fournir de l'assistance technique et opérationnelle aux organismes fédéraux qui sont chargés de l'application de la loi et de la sécurité en vertu des fonctions que la loi leur confère.

Le CST est le centre d'excellence du Canada en matière de cyberopérations. Nous misons sur notre expertise technique du cyberenvironnement pour assurer la surveillance des systèmes du gouvernement fédéral, afin de repérer les cybermenaces complexes et d'agir pour les neutraliser.

Nos activités s'étendent bien au-delà du gouvernement fédéral. En outre, puisque la cybersécurité est la responsabilité de tous, le CST contribue à soutenir le secteur privé, particulièrement les infrastructures essentielles, en prodiguant de l'information et des conseils sur l'atténuation des cybermenaces. Il est ainsi possible de mieux protéger leurs systèmes et l'information importante qu'ils renferment.

[*Traduction*]

Les partenariats sont essentiels à la réussite de la mission de notre organisme. Nous savons qu'un échange d'information efficace facilite la gestion et l'atténuation des répercussions d'une cybermenace, et c'est pourquoi nous travaillons en étroite collaboration avec nos principaux partenaires, dont le ministère

Security Telecommunications Advisory Committee, amongst others, to build a stronger capacity to resist and defend against today's diverse cyber-threats.

de la Sécurité publique, le Centre canadien de réponse aux incidents cybernétiques, l'organisme Échange canadien des menaces cybernétiques et le Comité consultatif canadien pour la sécurité des télécommunications, afin de concevoir une capacité plus robuste, capable de résister aux menaces et de défendre nos systèmes contre les diverses cybermenaces qui planent aujourd'hui.

But still, even the most secure systems can be rendered ineffective if not used properly. A core part of our work is to increase awareness and education of cybersecurity issues. We have developed the top 10 IT security actions, building on years of mitigation advice to Government of Canada departments and agencies, which help dramatically reduce the threat to all types of organizations. You can find them listed on our website along with much of our advice, guidance and alerts. We also frequently post cybersecurity best practices to our Twitter account and website in an effort to increase public awareness.

Il importe toutefois de souligner que même les systèmes les plus sécurisés peuvent se révéler inefficaces s'ils ne sont pas utilisés correctement. Notre travail consiste essentiellement à mieux faire connaître les enjeux liés à la cybersécurité. À la lumière des nombreux conseils sur l'atténuation des cybermenaces que nous avons offerts aux ministères du gouvernement du Canada au fil des ans, nous avons dressé la liste des 10 meilleures mesures de sécurité des TI en vue d'aider à réduire considérablement la menace contre tous les types d'organismes. Vous trouverez la liste sur notre site web ainsi qu'une panoplie de conseils, d'avis et d'alertes. Par ailleurs, nous publions souvent des messages traitant des pratiques exemplaires en matière de cybersécurité sur notre compte Twitter et notre site web afin de mieux sensibiliser le public.

I am especially pleased to appear before you today on this important issue because October is Cyber Security Awareness Month. This annual event encourages Canadians and organizations of all sizes, including the Government of Canada departments and agencies, to promote strong cybersecurity practices.

Je suis particulièrement heureux de m'adresser à vous sur cet enjeu important en ce mois de la sensibilisation à la cybersécurité. Dans le cadre de cet événement, on incite les Canadiens, les ministères et les organismes du gouvernement du Canada, à faire la promotion des pratiques à adopter pour accroître la cybersécurité.

I want to emphasize that cybersecurity is the responsibility of all of us and no single entity can do it alone. We do need to adopt a cyber neighbourhood watch. So it's crucial that everyone get involved in cybersecurity initiatives to better protect Canada's sensitive information. Together, we can collectively make Canada stronger and more resilient against cyber-threats.

Je ne saurais trop insister sur le fait que la cybersécurité est une responsabilité qui incombe à tous; aucune entité ne peut la garantir à elle seule. Nous devons mettre en place une cybersurveillance de quartier. Pour mieux protéger l'information sensible du Canada, il est primordial que nous prenions tous part aux initiatives liées à la cybersécurité. En unissant nos efforts, nous rendrons le Canada plus fort et plus résilient contre les cybermenaces.

As part this effort, today CSE is releasing a product called Assemblyline, a malware detection and analysis tool developed within CSE's Cyber Defence program to detect and analyze malicious files as they are received. Assemblyline will benefit businesses by allowing them to better protect their data from theft and compromise. Most software of a similar nature is proprietary to a company and not available to the software development company. We change that today.

Dans le cadre de cet effort, le CST procède aujourd'hui à la diffusion d'un produit appelé Chaîne de montage, un outil d'analyse et de détection des logiciels malveillants développé par l'organisme dans le cadre de son Programme de cyberdéfense en vue de détecter et d'analyser les fichiers malveillants dès leur réception. Chaîne de montage aidera les petites et grandes entreprises à mieux protéger leurs données contre le vol et les compromis. La plupart des logiciels de ce type sont exclusifs à une entreprise et ne sont pas mis à la disposition des développeurs de logiciels. Nous modifions cette tendance aujourd'hui.

CSE is releasing Assemblyline to businesses, malware and private researchers, industry and academia. The release of Assemblyline benefits the country and CSE's work to protect Canadian systems and allows the cybersecurity community to jointly evolve this valuable open-source software.

Le CST met son outil Chaîne de montage à la disposition des entreprises, des chercheurs du secteur privé dans le domaine des logiciels malveillants, de l'industrie et du milieu universitaire. La diffusion de Chaîne de montage sert à la fois les intérêts du Canada et le travail qu'effectue le CST pour protéger les

[*Translation*]

If I have the opportunity to appear before this committee a second time, I hope I will be able to share with members the results of Assemblyline. In the meantime, I thank you for the opportunity to participate in this study.

My colleague and I will be pleased to answer any questions you may have.

[*English*]

The Deputy Chair: Thank you very much.

Senator Wetston: Let's talk about Assemblyline. Obviously you're here and quite proud of this accomplishment. I really don't understand it since it's the first I have ever heard of it. Can you inform the committee what it is and what it is expected to do.

Mr. Jones: Assemblyline is a tool that has been described by some people as the Swiss Army Knife of malware analysis tools. It enables a malware analysis team to really plug in different types of tools to automate their process. It makes it easier for them to do their job. It is taking away the manual effort that they spend looking at every threat and really focuses on those new, undiscovered threats and essentially maximizes their valuable time.Wwe use that to triage a tremendous amount of the cyberactivity against the government. We wanted to make that available to others to do the same thing and not have to spend time investing in the infrastructure rather than the actual malware tools. Now we can focus on those.

Senator Wetston: It's not for a fee?

Mr. Jones: It's free, open-source, available for download for anybody.

Senator Wetston: We heard from a number of witnesses yesterday: the RCMP, CSIS, and Public Safety. One of the issues that we explored yesterday was collaboration and the state of readiness of cybersecurity in Canada. Can you inform the committee about where the Communications Security Establishment fits into that collaborative framework? I notice you listed a number of entities here, but other than Public Safety, I didn't see CSIS or the RCMP. So can you comment on that?

systèmes canadiens. La collectivité de la cybersécurité pourra ainsi assurer de concert l'évolution de ce logiciel de source ouverte fort utile.

[*Français*]

Si j'ai l'occasion de m'adresser à ce comité une deuxième fois, j'espère être en mesure de faire part aux membres du comité des résultats de la Chaîne de montage. Entre-temps, je vous remercie de me donner l'occasion de participer à cette étude.

Mon collègue et moi serons heureux de répondre à vos questions.

[*Traduction*]

Le vice-président : Merci beaucoup.

Le sénateur Wetston : Parlons de Chaîne de montage. Manifestement, vous êtes ici, et vous êtes très fier de cette réalisation. Je ne comprends pas vraiment en quoi consiste cet outil étant donné que c'est la première fois que j'en entends parler. Pourriez-vous renseigner le comité sur la nature de cet outil et sur ce qu'il est censé accomplir?

M. Jones : Chaîne de montage est un outil que certaines personnes décrivent comme le couteau suisse des outils d'analyse des logiciels malveillants. Il permet à une équipe d'analystes des logiciels malveillants d'y insérer divers types d'outils afin d'automatiser leurs processus. Il facilite le travail des analystes en éliminant les efforts manuels qu'ils doivent déployer pour examiner chacune des menaces. Il leur permet de se concentrer vraiment sur les nouvelles menaces non découvertes et d'optimiser leur temps précieux. Nous utilisons cet outil pour procéder au triage d'une énorme quantité d'activités cybernétiques visant le gouvernement. Nous souhaitions mettre cet outil à la disposition des autres afin qu'ils puissent faire la même chose que nous et éviter de passer du temps à élaborer l'infrastructure plutôt que des outils liés aux logiciels malveillants. Maintenant nous pouvons mettre l'accent sur ces menaces.

Le sénateur Wetston : Son utilisation n'entraîne pas de frais?

M. Jones : Ce logiciel de source ouverte est gratuit et peut être téléchargé par n'importe qui.

Le sénateur Wetston : Nous avons entendu un certain nombre de témoins hier, à savoir la GRC, le SCRS et le ministère de la Sécurité publique. Nous avons abordé alors certains enjeux, dont la collaboration et l'état de préparation de la cybersécurité canadienne. Pouvez-vous indiquer au comité où le Centre de la sécurité des télécommunications se situe dans ce cadre de collaboration? Je remarque que vous avez énuméré un certain nombre d'organisations, mais, mis à part le ministère de la Sécurité publique, je n'aperçois pas le SCRS ou la GRC dans la liste. Alors, pourriez-vous formuler des observations à ce sujet?

Mr. Jones: Within the government, we absolutely work with our partners. So the RCMP, with responsibility for criminal investigations, we support with both our technical expertise, but also as we're seeing things in the general cyber environment, making sure we keep the community abreast of everything that we're finding out as well so that the community is as informed as we can have it. The service as well, due to national security investigations, et cetera, we partnered closely with them. In fact, they are our closest next-door neighbours in our new facility.

But where we concentrate on providing the in-depth technical expertise, this has been our bread and butter in my program for the last 70 years. So rather than duplicate that, we want to play our part. That is the in-depth expertise on how the IT systems work, how they interoperate, the knowledge of the IT environment, the knowledge of the threat actors that comes from our experience in foreign signals intelligence and what we see the foreign actors doing, and then working with the community when we respond to an incident, making sure there is one lead, but with the full knowledge of all the organizations behind. If it's the private sector, CCIRC is the lead and Public Safety is the lead. We'll make sure we are providing whatever support we can to help them.

Senator Wetston: I didn't ask this of the RCMP yesterday, but I have a bit of an interest in where cybercrime is heading and the investigation tools necessary to gather the evidence, assess whether there has been a criminal violation, investigating and taking a case to court. Would your organization ever be in a position to assist the RCMP in a criminal investigation? If so, has there been one?

Mr. Jones: If the RCMP requested our assistance, they would do so under the third part of our mandate, Part C, which is the support to lawful law enforcement and security agencies. At the same time, we want to ensure that law enforcement is performed by the people who are best able to do it, and that is the Royal Canadian Mounted Police. We would provide any support they requested under their lawful authorities for that type of thing.

In terms of whether there have been any incidents, we work with the RCMP on a regular basis just for general situational awareness. If there was a particular investigation, to be honest, we would keep that very contained because it would be for the RCMP to comment on. I actually am not aware of a specific case. We have done a lot of general work with them, though.

M. Jones : Au sein du gouvernement, nous collaborons assurément avec nos partenaires. Par conséquent, la GRC étant responsable des enquêtes criminelles, nous l'appuyons non seulement grâce à nos compétences techniques, mais aussi en la tenant au courant des éléments que nous observons dans l'environnement cybernétique en général. Nous nous assurons de tenir le milieu de la sécurité informé de tout ce que nous découvrons afin qu'elle soit aussi renseignée que nous. En outre, dans le cadre de la prestation de notre service, nous travaillons étroitement avec ses membres en raison des enquêtes liées à la sécurité nationale. En fait, dans notre nouvelle installation, ils sont nos plus proches voisins.

Nous nous employons à fournir nos compétences techniques approfondies; c'est le rôle fondamental que notre programme a joué au cours des 70 dernières années. Alors, au lieu de reproduire ce que font les autres, nous voulons apporter notre propre contribution, c'est-à-dire notre connaissance du milieu des TI, notre connaissance des auteurs des menaces qui découlent de notre expérience en matière de renseignements électromagnétiques étrangers et notre observation des activités des acteurs étrangers. Lorsque nous intervenons dans le cadre d'un incident, nous travaillons avec le milieu de la sécurité en nous assurant qu'un groupe est responsable, mais en reconnaissant également le rôle de toutes les organisations participantes. S'il s'agit du secteur privé, le CCRI et le ministère de la Sécurité publique seront les organisations responsables. Nous veillerons alors à leur apporter toute l'aide que nous pouvons.

Le sénateur Wetston : Je n'ai pas posé cette question à la GRC hier, mais j'aimerais savoir dans quelle direction la cybercriminalité s'engage et connaître les outils d'enquête qui sont nécessaires pour recueillir les éléments de preuves, pour évaluer si une infraction criminelle a été commise, pour procéder à l'enquête et pour mener l'affaire devant les tribunaux. Votre organisation pourrait-elle aider la GRC à mener une enquête criminelle? Dans l'affirmative, une telle enquête a-t-elle déjà été menée?

M. Jones : Si la GRC demandait notre aide, elle le ferait en vertu de la troisième partie de notre mandat, la partie C, qui correspond au soutien de l'application de la loi et des organismes de sécurité. En même temps, nous voulons nous assurer que l'application de la loi est exercée par les gens qui sont les mieux placés pour le faire, et ces gens sont les membres de la Gendarmerie royale du Canada. Nous leur apportons l'aide qu'ils demandent en vertu des pouvoirs légitimes dont ils sont investis pour exercer ce genre d'activités.

En ce qui concerne la question de savoir si des incidents de ce genre sont survenus, je dirais que nous travaillons régulièrement avec les membres de la GRC afin de leur faire part de la situation générale. En toute honnêteté, si une enquête particulière survenait, nous limiterions grandement nos communications à ce sujet, car il reviendrait à la GRC de formuler des commentaires.

Senator Wetston: I was just wondering whether there was a prosecution that would have been public and whether or not the various entities in government would support the RCMP because, obviously, they have a lot of tools, but they don't have all the tools. I understand that you may not have that information, obviously.

[*Translation*]

Senator Massicotte: My thanks to both of you for joining us this morning. I am still at the stage where I am trying to form an opinion about how serious hacking is and the threats we are under as consumers, members of the public, and business leaders. Is this a really major problem? We have heard a lot of talk about it in the United States, particularly during the last elections. Recently, Equifax Canada was the target of a cybersecurity incident. As a client of businesses like that, I am frustrated to know that my confidential information has been compromised, that people I trusted have betrayed me, and that necessary measures to prevent such incidents have not been taken.

Is it a matter of bad luck or is it something very serious? As Canadians and as the government, should we be changing our way of doing things in order to devote more effort or to invest more money in order to better manage all those risks?

André Boucher, Director General, Cyber Security Partnerships, Communications Security Establishment: Good morning, and thank you for your question. Yes, this is a clear and present danger for Canadians. What you are actually seeing is a shift. Previously, it was done by people on the move. Someone went and knocked on the door of your bank in order to get your information and your money. Now, these criminal acts are done electronically. Unfortunately, I feel that it is inevitable. People with bad intentions are evolving with the technology available and are trying to make it work to their advantage. In fact, Canadians are just as much targets as anyone else in the world.

In terms of knowing whether we are making enough effort, I would say that there is still a parallel. I feel that governments definitely must play a role in implementing measures to fight cybercrime. The bad guys we knew in the past have simply evolved towards the world of technology. The CSE has a technical role to play as an expert in the field. We have gone through the technological revolution, we are part of it, we have used it in our work and, through those activities, we have watched the bad guys evolve. It puts us into a strategic position to be able to intervene in our community.

Je ne suis pas au courant d'un cas en particulier, mais nous avons accompli beaucoup de travail général avec eux.

Le sénateur Wetston : Je me demande simplement si des poursuites rendues publiques ont été intentées et si les divers organismes gouvernementaux ont appuyé la GRC, parce qu'elle dispose peut-être de nombreux outils, mais elle ne dispose pas de la totalité d'entre eux. Évidemment, je comprends que vous puissiez ne pas avoir accès à cette information.

[*Français*]

Le sénateur Massicotte : Merci à vous deux d'être parmi nous ce matin. Je suis toujours à étape où j'essaie de me faire une opinion sur la gravité du piratage et de la menace qu'on subit en tant que consommateur, citoyen et chef d'entreprise. Est-ce un problème très important? On en a entendu beaucoup parler aux États-Unis, particulièrement lors des dernières élections. Récemment, Equifax Canada a été la cible d'un incident de cybersécurité. En tant que client de ces entreprises, cela me frustre de savoir que mes renseignements confidentiels ont été compromis, que quelqu'un en qui j'avais confiance m'a trahi et qu'on n'a pas pris les mesures nécessaires pour prévenir de tels incidents.

Est-ce une question de malchance ou est-ce quelque chose de très important? En tant que citoyens canadiens et comme gouvernement, devrions-nous changer notre façon de faire en consacrant plus d'efforts ou en investissant plus d'argent pour mieux gérer tous ces risques?

André Boucher, directeur général, Partenariats en cybersécurité, Centre de la sécurité des télécommunications : Bonjour, et merci de votre question. Oui, il s'agit d'un problème concret et réel pour les Canadiens et les Canadiennes. Ce que vous voyez, en fait, c'est une migration. Auparavant, on le faisait en se déplaçant. Une personne allait cogner à la porte de votre banque pour prendre vos renseignements et votre argent. Ce mode de criminalité se fait désormais par voie électronique. Malheureusement, je pense que c'est inévitable. Les gens qui ont de mauvaises intentions évoluent avec la technologie qui est disponible et essaient d'en tirer avantage. En fait, les Canadiens sont tout aussi ciblés que n'importe qui dans le monde.

Pour ce qui est de savoir si on déploie suffisamment d'efforts, je crois que le parallèle demeure. Je pense que les gouvernements doivent définitivement jouer un rôle en prenant des mesures pour contrer la cybercriminalité. Les mauvais acteurs qu'on a connus par le passé ont tout simplement évolué vers le monde technologique. Le CST a un rôle d'expert technique à jouer dans cette sphère. On a vécu l'évolution technologique, on en a fait partie, on s'en est servi dans notre travail et on a vu, dans le cadre de nos activités, l'évolution des mauvais acteurs. Cela nous donne une position stratégique pour pouvoir intervenir au sein de notre communauté.

Senator Massicotte: I really get the impression that we are likely to lose the battle against organized crime. We receive emails looking for information every day and they are often very good imitations of our banks in Canada. We are on guard against those false alarms. Imagine those who are less well equipped, who are not as knowledgeable or who are less accustomed to the situation. I am sure that major amounts of money are collected every day because no one is turning these fraudsters in.

I see it as a race between yourselves, the order, and the criminal world that generates millions, if not billions, of dollars by manipulating information. It attracts better knowledge. That scares me too. We are going to lose the battle because they are well equipped, they are financially motivated and they are very well paid. What are we going to do? That is what we are dealing with, and I believe we are going to lose the battle.

Mr. Boucher: I would like to draw another parallel, because the situation can be looked at simply. We have all learned to deal with the people who come door to door to sell us products or services. We have learned to be selective, to determine whether someone is legitimate or not. Now we have to do that in an electronic world. It is more difficult, because we have to make decisions much more quickly than in the past. We have to recognize that it is a reality. We also have to raise awareness with consumers and the public, so that they learn to recognize what is legitimate and illegitimate in their activity on the Internet. More than 88 per cent of Canadians are connected. This is a very real problem.

Senator Massicotte: Thank you.

[*English*]

Senator Enverga: Thank you for your presentation. You mentioned foreign actors. Are there particular countries that seem to be more of a concern to us? You don't have to say the names. I just want to know whether there are particular countries that maybe we should focus on.

Mr. Jones: I think with regard to countries, both the power and the problem with the Internet is that it can come from anywhere. There are certainly countries that represent a greater challenge for the RCMP when they are going to do investigations, et cetera. This is one of the greatest challenges, I think, when rather than take technical counter measures, which we typically focus on when we're talking about cyber and use law enforcement, it's interjurisdictional and a significant amount of work just to get to the cyber criminals. You can hide on the Internet. You can jump around, jump through countries.

Le sénateur Massicotte : J'ai vraiment l'impression qu'on risque de perdre cette bataille contre le crime organisé. On reçoit des courriels à la recherche d'information presque tous les jours, et ce sont souvent de très bonnes imitations de nos banques canadiennes. Nous nous méfions de ces fausses alertes. Imaginez les personnes qui sont moins outillées, qui ont moins de connaissances ou qui sont moins habituées à ce concept. Je suis certain que des sommes importantes sont réclamées chaque jour parce que personne ne dénonce ces fraudeurs.

Je vois cela comme une course entre vous, l'ordre et le milieu criminel qui génère des millions, sinon des milliards de dollars en manipulant l'information. Cela attire les meilleures connaissances. Cela me fait peur aussi. Nous allons perdre la bataille parce que ces personnes sont bien outillées, sont motivées financièrement et sont très bien payées. Qu'est-ce qu'on fait? Nous sommes exposés à cela et je crois que nous allons perdre la bataille.

M. Boucher : J'aimerais faire un autre parallèle, parce que la situation peut être envisagée de façon simple. Nous avons tous appris à répondre aux colporteurs qui viennent frapper à notre porte pour nous vendre un produit ou un service. Nous avons appris à faire preuve de discernement, à déterminer si une personne est légitime ou non. Il faut maintenant le faire dans le monde électronique. C'est plus difficile, parce qu'il faut faire un bon en avant beaucoup plus rapide que par le passé. Il faut reconnaître que c'est une réalité. Il faut aussi sensibiliser les consommateurs et les citoyens pour qu'ils apprennent à reconnaître, dans leurs interactions sur Internet, ce qui est légitime et illégitime. Plus de 88 p. 100 des Canadiens sont branchés. Il s'agit d'un problème bien réel.

Le sénateur Massicotte : Merci.

[*Traduction*]

Le sénateur Enverga : Je vous remercie de votre exposé. Vous avez mentionné les acteurs étrangers. Y a-t-il des pays en particulier qui semblent nous préoccuper davantage? Vous n'avez pas besoin de les nommer. Je veux simplement savoir s'il y a des pays précis dont nous devrions peut-être nous soucier.

M. Jones : En ce qui concerne les pays, je crois que l'avantage et l'inconvénient d'Internet, c'est que l'information peut provenir de n'importe quel endroit. Il y a certainement des pays qui causent plus de difficultés à la GRC lorsqu'elle s'apprête à mener des enquêtes. À mon avis, l'un des plus grands défis à relever, c'est qu'au lieu de prendre des contre-mesures techniques, sur lesquelles nous nous concentrons habituellement lorsqu'il est question de cybermenaces, et d'avoir recours à l'application de la loi, il faut déployer d'importants efforts intergouvernementaux pour attraper les cybercriminels. On peut dissimuler sa présence sur Internet, et on peut passer d'un pays à l'autre.

I would say while it looks like there are countries where the origin is, they will very quickly migrate, depending on the circumstances and where they think they can better hide. That's for cybercrime where they will go to the jurisdiction that is the best fit and the easiest to work in. Then when you go to states, it's the exact same problem, where you have states that have different objectives, depending on what they are looking for on the Internet. But the fact is it is very easy to hide.

One of the things people really look for is attribution. That's the first question I get any time there is an incident: Who did it? It is difficult now to tell states from criminals. Their level of sophistication, as has been pointed out before, has gone up. So it's not really a matter of which state or country makes it easier or which cyber criminals. It's whether we can make ourselves more resilient and how the world needs to react to the fact that the Internet is a boundless environment where territoriality doesn't really apply. You can hide. It's almost a new domain that we haven't caught up with yet.

Senator Enverga: You mentioned Assemblyline. Is it going to be available to almost everybody? I mean, it's going to be some sort of a freeware for everybody.

Mr. Jones: Yes.

Senator Enverga: With your experience and expertise, would you expect this to help in every way, as in replacement of other anti-virus or anti-spam software? Is that how you think it is going to be used?

Mr. Jones: It doesn't replace any commercial products that are out there, the things that we should all be doing, running good anti-virus products that are up to date, patching our systems and making sure that we are continuously upgrading our technology.

What it does is it will allow malware researchers, malware analysts, people on the front lines of bigger organizations, to plug different tools together so they don't have to do it manually. You don't have to run through tool A, then take it manually and put it through tool B. Assemblyline lets you assemble all these different components and tools in a way that automates that workflow. It really is a tool that is focused on academia for malware research, businesses who are cyber-defence organizations or large companies that need to do this type of thing.

Je dirais que, lorsque des pays d'origine semblent ressortir, les auteurs de ces crimes se déplacent très rapidement selon les circonstances et les endroits où ils pensent être en mesure de mieux se cacher. Les cybercriminels se rendent dans l'État qui convient le mieux à leurs activités et avec lequel il est le plus facile de transiger. Il en va de même des États, en ce sens qu'ils visent différents objectifs en fonction de ce qu'ils recherchent sur Internet. Le fait est qu'il est très facile de passer incognito.

Entre autres choses, les gens cherchent vraiment à attribuer la responsabilité à quelqu'un. C'est la première question qu'on me pose lorsqu'un incident survient: qui est le responsable? Il est maintenant difficile de faire la distinction entre les États et les criminels. Comme cela a été signalé auparavant, leur degré de perfectionnement a augmenté. Par conséquent, la question n'est plus de savoir quels pays facilitent la tâche aux criminels et quels criminels sont à l'œuvre. La question est de savoir si nous pouvons accroître notre résilience et de déterminer comment le monde doit réagir au fait qu'Internet est un milieu sans borne où la territorialité ne s'applique pas vraiment. Il est possible de s'y cacher. Il s'agit presque d'un nouveau domaine que nous n'avons pas encore maîtrisé.

Le sénateur Enverga : Vous avez mentionné Chaîne de montage. Pratiquement tout le monde pourra avoir accès à cet outil? J'entends par là que ce sera un genre de logiciel gratuit à la disposition de tous.

M. Jones : Oui.

Le sénateur Enverga : Compte tenu de votre expérience et de vos compétences, vous attendez-vous à ce que cet outil apporte un soutien universel, en tant que solutions de rechange aux autres logiciels antivirus et anti-pourriels? Selon vous, sera-t-il utilisé ainsi?

M. Jones : L'outil ne remplace aucun produit commercial vendu en ce moment ni les mesures que nous devrions tous prendre, comme l'exécution de produits antivirus ou anti-pourriels efficaces et actualisés, l'application de correctifs à nos systèmes et la mise à niveau continuelle de nos technologies.

L'outil permet aux chercheurs et aux analystes du domaine des logiciels malveillants, ainsi qu'au personnel de première ligne des grandes organisations, de combiner différents outils afin d'éviter d'avoir à les exécuter manuellement. Vous n'êtes plus forcés d'exécuter l'outil A, puis de transférer manuellement les résultats à l'outil B. Chaîne de montage vous permet de regrouper tous ces différents éléments de manière à automatiser le déroulement du travail. L'utilisation de cet outil est vraiment axée sur la recherche universitaire dans le domaine des logiciels malveillants, sur les entreprises spécialisées en cyberdéfense ou sur les grandes sociétés qui doivent prendre en charge ce genre de travail.

It wouldn't be something, for example, that I would run at home if I wasn't a cybersecurity nerd. It would be something that I would look for a larger company to take on and to really run this. It's not a tool that us as citizens would each be looking for. It's something we are really looking to try to boost the whole level of the industry, knowing that we rely on them to provide us service.

Senator Enverga: With all the issues right now with cybercrime and cybersecurity, what is the first point of entry? Do you think our provider should be keeping an eye on this? Is there a way they can secure this so everybody else will have a secure line?

Mr. Jones: The real issue is the devices at the end of the link that are the vulnerable points, running out-of-date systems, old versions of operating systems, for example, not applying that patch to your smartphone when it is required, things like that. It is the Internet of Things, like the thermostat they put into our houses, et cetera. Those things are the points where they are vulnerable. For somebody in the middle as the defender, you would actually have to censor a tremendous amount of the activity. You would really start to get in the way of the use of the Internet.

What we really have to do is make the systems at the end more resilient and easily updated. You shouldn't have to worry about whether you are running a new software. How do we do security by default? Meaning we don't have to think about it as consumers. The device is secure by default, not secure because I have to take some sort of complicated action to keep it up to date. Right now, most of the things need a complicated action.

Senator Enverga: Can the provider stop the user from using his or her device so that everybody can be secure?

Mr. Jones: For example, with your e-mail provider at home, most of them are doing a lot of work to try to decrease spam, decrease known malware types of things, and they will try to protect you. At the end of the day, it's a balance between letting people do what they want to. There are some things they just can't prevent. They certainly can prevent things like e-mail, et cetera, as you use their services. That's the easy one. When the thermostat you have installed in your home actually is vulnerable to an external cyber-attack, there is very little they can do on that. They can maybe protect the rest of the world from your device, but probably not you from what your device is going to do.

Par exemple, ce n'est pas le genre de logiciel que j'exécuterais à la maison si je n'étais pas un mordu de la cybersécurité. Selon moi, c'est un outil qu'une grande entreprise téléchargerait et exécuterait. Ce n'est pas un outil que nous, les citoyens, rechercherions. Grâce à cet outil, nous tentons vraiment de stimuler toute cette industrie, sachant que nous dépendons d'elle pour la fourniture de ces services.

Le sénateur Enverga : Compte tenu de tous les problèmes actuellement liés à la cybercriminalité et à la cybersécurité, quel est le premier point d'entrée? Croyez-vous que nos fournisseurs de services devraient surveiller cet aspect? Peuvent-ils d'une certaine façon rendre le tout sécuritaire pour que tout le monde profite d'une connexion sécurisée?

M. Jones : Le véritable problème est que les appareils des utilisateurs sont les points vulnérables. Nous utilisons par exemple des systèmes désuets ou d'anciennes versions de systèmes d'exploitation ou nous n'installons pas la rustine sur notre téléphone intelligent au moment où il faut le faire. C'est l'Internet des objets, comme les thermostats que nous avons dans nos maisons. Ce sont les points d'entrée où nos fournisseurs sont vulnérables. Un fournisseur au milieu qui joue le rôle de défenseur devrait en fait interdire une énorme quantité d'activités. Vous commenceriez vraiment à entraver l'utilisation d'Internet.

Nous devons vraiment nous assurer que la résilience des systèmes des utilisateurs est renforcée et que ces systèmes peuvent être facilement mis à jour. Vous ne devriez pas avoir à vous inquiéter lorsque vous utilisez un nouveau logiciel. Comment nous assurer que c'est sécuritaire par défaut? Cela signifie que les consommateurs n'ont pas à s'en soucier. L'appareil est sécuritaire par défaut. Il n'est pas nécessaire de prendre des mesures complexes pour veiller à ce que l'appareil soit toujours à jour. Actuellement, dans la majorité des cas, une telle mesure complexe est nécessaire.

Le sénateur Enverga : Le fournisseur de services peut-il empêcher l'utilisateur de se servir de son appareil pour s'assurer que tout le monde peut être protégé?

M. Jones : Par exemple, dans le cas des fournisseurs de services de courriel à la maison, la majorité d'entre eux redoublent d'efforts pour essayer de réduire les pourriels et les maliciels connus; ils essaieront de vous protéger. Au bout du compte, c'est un équilibre pour laisser les gens faire ce qu'ils veulent. Il y a certaines choses que les fournisseurs ne peuvent simplement pas empêcher. Ils ne peuvent certainement pas bloquer les courriels, par exemple, étant donné que vous utilisez leurs services. C'est un exemple facile. Si le thermostat que vous avez installé dans votre domicile est vulnérable à une cyberattaque externe, il y a très peu de choses que peuvent faire à ce sujet vos fournisseurs de services. Ils peuvent protéger le reste du monde de votre appareil, mais ils ne pourront pas vous protéger de ce que fera votre appareil.

Mr. Boucher: It's really a complex problem because it is the inter-ecosystem you have to address. In addition to the device that you put into the system and your own responsibilities for using it properly, and as you point out, the people that bring the information to your house or to your home with your car, there are also those that make the devices or that provide the systems, that manufacture them, or those that operate certain systems on behalf of others. Every person involved in delivering and operating and supplying the ecosystem has the responsibility of creating the state of security that we need to have.

Senator Enverga: That's scary.

Senator Unger: Thank you, gentlemen, for your presentation. Mr. Jones, you mentioned that together we can collectively make Canada stronger and more resilient against cyber threats. What do we need to do to be more resilient?

Mr. Jones: I think there are a number of things that we can build on. One is, this is a team sport. The first thing is we need to work as citizens, us being better and more aware of what technology we are using. We need to demand better products as we're buying them. We should demand that security come in, just in the same way we expect certain things to come in, for example, if we buy a vehicle for safety. We should be asking for the security features to be in the Internet-connected devices.

We need to work with industry to make sure that we're applying that ecosystem we talked about and finding a new way of having a relationship. Right now, it tends to be very much based on an adversarial regulatory environment that, unfortunately, the Internet is outpacing how quickly those types of formal arrangements can react, which means we have to work together. We have to find a way of working together — win-win — to work on this problem as a whole collective, all the way from citizens, from information, asking the right questions, buying the products that have security built in from the start, making that something that the market values, all the way to figuring out how the government can make sure we do our piece with industry altogether.

It sounds a little Pollyanna-esque. I know it seems optimistic, but in reality with cybersecurity, it's going to be the only way that we can make it more resilient, by partnering and working together and finding ways to boost everybody up and looking for those opportunities. That's something that we really have been working on the last few years.

M. Boucher : C'est un problème vraiment complexe, parce que cela concerne l'écosystème interne. En plus de l'appareil que vous branchez au système, de vos propres responsabilités quant à son utilisation adéquate et, comme vous l'avez souligné, des gens qui apportent des données dans votre maison par l'entremise de votre véhicule, il y a également les fabricants des appareils, les fournisseurs et les fabricants des systèmes ou ceux qui exploitent certains systèmes au nom d'autres personnes. Toute personne qui participe à la prestation et à l'exploitation de l'écosystème doit générer le niveau de sécurité dont nous avons besoin.

Le sénateur Enverga : C'est inquiétant.

La sénatrice Unger : Je vous remercie de votre exposé. Monsieur Jones, vous avez mentionné qu'ensemble nous pouvons rendre le Canada plus fort et plus résilient contre les cybermenaces. Que devons-nous faire pour renforcer notre résilience?

M. Jones : Selon moi, nous pouvons tabler sur plusieurs éléments. Premièrement, c'est un sport d'équipe. En tant que citoyens, nous devons tout d'abord nous améliorer et être plus conscients de la technologie que nous utilisons. Nous devons demander de meilleurs produits lorsque nous magasinons. Nous devons demander que ce soit sécuritaire par défaut, tout comme nous nous attendons à ce que viennent de série certaines fonctionnalités de sécurité, par exemple, lorsque nous achetons un véhicule. Nous devrions exiger que des éléments de sécurité soient intégrés dans les appareils branchés à Internet.

Nous devons collaborer avec l'industrie pour nous assurer de mettre en œuvre l'écosystème dont nous avons parlé et de trouver une nouvelle manière d'établir des relations. Actuellement, nos relations ont énormément tendance à se fonder sur une réglementation qui repose sur la confrontation. Malheureusement, Internet évolue plus rapidement que nous arrivons à conclure de telles ententes officielles, ce qui signifie que nous devons collaborer. Nous devons trouver une manière de collaborer où tout le monde en sort gagnant pour nous attaquer ensemble à ce problème. Cela passe au départ par les citoyens et l'information; il faut poser les bonnes questions, acheter les produits qui sont sécuritaires dès le départ et faire en sorte que ce soit un aspect prisé par les consommateurs. Nous devons également déterminer la manière dont le gouvernement peut s'assurer que nous faisons notre travail de concert avec l'industrie.

Cela semble un peu naïvement optimiste. Je le sais, mais ce sera vraiment la seule façon de renforcer la résilience dans le domaine de la cybersécurité; nous devons établir des partenariats, collaborer, trouver des moyens de renforcer tout le monde et chercher de telles occasions. C'est vraiment un aspect sur lequel nous nous penchons depuis quelques années.

Senator Unger: There is a proposed CSE Act which will eliminate the ambiguities about what we're permitted and authorized to do in cyberspace. Could you talk about that?

Mr. Jones: The current National Defence Act provides CSE with its mandate. That part of the National Defence Act was written in 2001, and technologies have evolved quite extensively. The mandate we operate under is basically a single line in that act that says: Provide advice, guidance and services to help ensure the protection of information and information infrastructures of importance to the Government of Canada.

That was really before cybersecurity. Well, we didn't use the term "cyber." Smartphones had not been invented. We didn't know an iPhone was coming. Technology has changed quite remarkably. Frankly, we were very much focused on, "Well, our only job is the Government of Canada." As that has expanded and we started seeing what the impact could be on critical infrastructure on the various sectors, including finance, transportation, et cetera, we have realized, number one, we have some tools that we have that we use to defend the government that are world class. We haven't found anybody who defends their organization in the same way that we're able to defend the Government of Canada. For example, on many days we take up to a billion actions per day to protect the Government of Canada from malicious activity.

We would like to make that available. Right now the CSE Act would allow us, with the request of the company, the critical infrastructure provider, and the designation of the Minister of National Defence that it is important, to deploy those tools to protect, to use classified techniques to defend if we needed to. We don't have that authority today. That's the first ambiguity that would be resolved, and it would provide that authority. There is a belief that we can do that today. We can't. I am restricted to the Government of Canada only for those services.

Second would be how we share information. We never anticipated needing to share things like indicators of compromise, tools, techniques, how somebody would be compromising a system. We imagined our role in 2001 as being: Here is how you secure your home Windows 95 system — it would have been Windows 95 back then — Windows 2000. It would not be: Here is a quick indicator of compromise we need to release. By defending the government, sometimes we detect that Canadian infrastructure has been compromised. We need to be able to share that. It was never envisioned. This just clarifies our information-sharing components.

La sénatrice Unger : Il y a un projet de loi visant à créer la Loi sur le Centre de sécurité des communications qui éliminera les ambiguïtés en ce qui a trait à ce qu'il nous est permis de faire et à ce que nous sommes autorisés à faire dans le cyberespace. Pouvez-vous nous dire quelques mots à ce sujet?

M. Jones : Le mandat du Centre de sécurité des communications se trouve dans l'actuelle Loi sur la Défense nationale. Cette partie de la Loi sur la Défense nationale a été créée en 2001, et les technologies ont considérablement évolué depuis. Le mandat de notre organisme est en fait une ligne de cette loi: fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada.

Cela remonte à bien avant la cybersécurité. En fait, nous n'utilisions pas l'expression « cyber ». Les téléphones intelligents n'étaient pas encore inventés. Nous ne savions pas qu'un iPhone s'en venait. Les technologies ont considérablement évolué. Honnêtement, nous mettions passablement l'accent sur un aspect: notre seul travail est le gouvernement du Canada. La situation a pris de l'expansion, et nous avons commencé à en voir les effets potentiels sur les infrastructures essentielles dans les divers secteurs, y compris les finances, les transports, et cetera; nous avons premièrement réalisé que nous avons des outils de calibre mondial que nous utilisons pour défendre le gouvernement. Nous n'avons trouvé personne qui défend leur organisme comme nous sommes en mesure de défendre le gouvernement du Canada. Par exemple, il n'est pas rare de prendre un milliard de mesures par jour pour protéger le gouvernement du Canada d'activités malveillantes.

Nous aimerions rendre disponibles ces outils. Actuellement, la Loi sur le Centre de sécurité des communications nous permettrait, à la demande d'une entreprise ou d'un fournisseur d'infrastructure essentielle, si le ministre désigne cela comme étant important, de déployer ces outils pour assurer notre protection et d'utiliser des techniques classifiées pour assurer notre défense, au besoin. Nous ne pouvons pas le faire actuellement. Voilà la première ambiguïté qui serait réglée, et cette mesure législative nous donnerait un tel pouvoir. Certains croient que nous pouvons le faire actuellement, mais nous ne le pouvons pas. Je peux seulement offrir ces services au gouvernement du Canada.

Deuxièmement, cela définirait la forme que prendrait l'échange de renseignements. Nous n'avons jamais prévu le besoin d'échanger divers éléments comme des indicateurs de compromission, des outils, des techniques et la façon dont une personne peut compromettre un système. Nous avions imaginé en 2001 que notre rôle viserait à expliquer comment sécuriser votre système d'exploitation Windows 95 à la maison — c'était Windows 95 à l'époque — ou Windows 2000. Nous ne pensions pas que cela prendrait la forme d'un bref communiqué à publier sur un indicateur de compromission. En défendant le gouvernement, nous détectons parfois que des infrastructures

The third piece is adding the role of defensive cyber operations. That's taking action to protect Canadian systems but in foreign space. If something needs to be done, the defensive mechanism that needs to be done is to stop the activity before it hits the Canadian infrastructure and to be able to do that with obviously appropriate authorizations and oversight and the proper review mechanisms in place. That's the third piece of the mandate that is clarified.

Senator Unger: One more quick question: The government is really pushing studies on automated vehicles. I live in Edmonton, and it's a city that is wanting to push this agenda as well. In Edmonton, there are poles and high buildings that already have this special lens that will communicate with automated vehicles. I'm thinking this is still a few years away, but will it be that much easier?These cars can be hacked into for specific reasons. As we move into that, will that cause a huge increase in cybercrime?

Mr. Jones: We see the trend coming. The industry is starting to react, and that's part of the partnerships. We need to build security into those from the start. There are some things in your car, for example, the entertainment system, that if somehow somebody hacks into it, that's probably not great, but not detrimental, whereas if they hack into the brakes and lock the brakes up or lock the steering or change its course, that's a much bigger issue.Part of the security design needs to include the fact that pieces of this infrastructure need to be very heavily defended, protected and also isolated so that they can't be hacked into very easily.

Typically, what we see with any sort of cyber compromises, you usually don't hack the system directly that you're looking for. You hack something attached to it. You want to make sure that the control system of the car is very heavily defended and probably quite isolated. You're probably not going put the same level of security effort into the entertainment system. I'm using that as something that's probably the least important thing in your car from the automated car perspective. You have to design it properly. You have to apply the proper isolation and security design and also not let things be the jumping point. That's something also that we apply in today's environment as well.

canadiennes ont été compromises. Nous devons avoir les moyens de diffuser cette information. Cette possibilité n'a jamais été prévue. Ce projet de loi précise tout simplement les aspects ayant trait à l'échange de renseignements.

Troisièmement, la mesure législative ajoute un nouveau rôle : les cyberopérations défensives. Cela vise à intervenir dans l'infrastructure mondiale pour protéger des systèmes canadiens. Si quelque chose doit être fait, le mécanisme défensif vise à arrêter l'activité avant qu'elle touche l'infrastructure canadienne, mais nous devons évidemment pour ce faire obtenir les autorisations appropriées, assurer une surveillance adéquate et avoir les bons mécanismes d'examen en place. C'est le troisième élément du mandat qui est précisé par le projet de loi.

La sénatrice Unger : J'ai une dernière petite question. Le gouvernement exerce vraiment des pressions pour réaliser des études sur les véhicules automatisés. J'habite à Edmonton, et notre administration municipale souhaite également mettre l'accent sur cet aspect. À Edmonton, des dispositifs spéciaux sont déjà installés sur des poteaux et de grands édifices pour communiquer avec les véhicules automatisés. Je présume que ce sera une réalité dans quelques années, mais je me demande si ce sera vraiment plus facile. Des gens peuvent pirater ces véhicules à des fins précises. À mesure que cela deviendra réalité, constaterons-nous une forte hausse de la cybercriminalité?

M. Jones : Nous voyons la tendance se dessiner. L'industrie commence à réagir, et cela fait partie des partenariats. Nous devons intégrer dès le départ la sécurité dans ces véhicules. Si une personne pirate certains éléments de votre véhicule, comme votre système de divertissement, ce ne sera probablement pas plaisant, mais ce n'est pas dangereux. Par contre, si l'individu pirate vos freins et bloque vos freins ou votre volant ou vous fait dévier de votre route, c'est un problème beaucoup plus important. La conception de la sécurité doit notamment veiller à ce que les éléments de cette infrastructure soient hautement défendus, protégés et isolés pour éviter qu'ils soient très facilement piratables.

Normalement, ce que nous constatons dans les divers cas de cybercompromissions, c'est que les gens ne s'attaquent pas directement au système qu'ils cherchent à pirater. Ils piratent quelque chose qui est branché à ce système. Nous devons nous assurer que le système de contrôle du véhicule est très fortement défendu et probablement très isolé. Nous ne consacrerons probablement pas autant d'énergie à la sécurité du système de divertissement. J'utilise cela comme exemple, parce qu'il s'agit probablement du dispositif le moins important dans votre véhicule du point de vue des véhicules automatisés. Sa conception doit être adéquate. Nous devons adéquatement isoler le tout, et la conception de la sécurité doit être appropriée; nous devons nous assurer qu'aucun élément ne peut servir de point de départ. C'est également quelque chose que nous faisons dans l'environnement actuel.

I think there's a way forward. We're supporting the Department of Transport as we're working forward with that. We have a partnership with them. I know they're working with the auto industry as well, andI think that's something that is going on because it is the future.

Senator Unger: That's good to hear. Thank you.

[*Translation*]

Senator Maltais: Let us talk today about ordinary Canadians who just have cable, the Internet and Wi-Fi on their computers. They keep their personal accounting there. They access their bank accounts, their holdings, they follow the stock market, just like everyone does in Canada. If I understood you correctly, people like that are not at all safe. A lot of people could go and play in their computers.

One thing intrigues me. Drones are an awful source of information for criminals. They just have to position a drone over your house and they can then photograph and record everything. We now see that happening in airports. We had an example in Quebec City on the weekend, where a drone almost caused a disaster. How is it that, with all the security measures we have available today, we are not able to detect on basic radar or destroy them before they cause real disasters? We were lucky in Quebec City, because there was no disaster. However, things could well have been different. How is it that we cannot protect one of the most important modes of transportation, in Canada and everywhere else, from a small object that can cause the deaths of hundreds of people? How can you explain that?

Mr. Boucher: I am going to expand on your question, which is somewhat similar to that of Senator Unger on the various devices that are emerging and that are all connected electronically. It must be a two-pronged conversation. There are malicious users, and that responsibility is related to public safety. In your example, was there a problem with the design of the drone?

As Mr. Jones mentioned, I think we have work to do to ensure that the various devices that are built and connected to the Internet for various purposes, including the transportation of goods, meet minimum safety standards. These protections will make autonomous vehicles, drones and heating systems reliable, like a host of other devices.

I think it's a matter of safety standards. We see the problem arising, and we are already committed to solving it. People in research and development are working on it. Manufacturers are aware and they have everything to gain by doing things properly. I think it's a real problem that we understand and that we can do something about.

Je crois qu'il y a une solution, et nous appuyons le ministère des Transports pour réussir à la trouver ensemble. Nous avons établi un partenariat avec lui. Je sais que le ministère collabore également avec l'industrie automobile, et je crois que nous le faisons, parce que c'est l'avenir.

La sénatrice Unger : C'est bon à entendre. Merci.

[*Français*]

Le sénateur Maltais : Aujourd'hui, on va vous parler d'un citoyen ordinaire qui a simplement le câble, Internet et le Wi-Fi sur son ordinateur. Il sauvegarde sa comptabilité, il accède à ses comptes de banque, à ses avoirs, il suit la bourse, comme un peu tout le monde le fait au Canada. Si je vous ai bien compris, cet individu n'est pas du tout en sécurité. Plusieurs personnes pourraient aller jouer dans son ordinateur.

Une chose m'intrigue. Les drones sont une source épouvantable de renseignements pour les malfaiteurs. Il suffit pour eux de positionner le drone au-dessus de votre maison, et ils pourront alors photographier et tout enregistrer. Ce phénomène est maintenant présent dans les aéroports. On en a eu la preuve à Québec, en fin de semaine, où un drone a failli causer une catastrophe. Comment se fait-il qu'aujourd'hui, avec toutes les mesures de sécurité dont nous disposons, nous ne soyons pas en mesure de les capter à l'aide d'un simple radar ni de les détruire avant qu'ils ne causent de réelles catastrophes? Nous avons été chanceux, car il n'y a pas eu de catastrophe à Québec. Toutefois, il aurait pu en être autrement. Comment se fait-il qu'on ne puisse protéger un mode de transport parmi les plus importants au Canada et partout ailleurs d'un petit objet qui peut causer la mort de centaines de personnes? Comment pouvez-vous expliquer ce phénomène?

M. Boucher : Je vais élargir votre question, qui rejoint un peu celle de la sénatrice Unger sur les différents appareils qui voient le jour et qui sont tous connectés de façon électronique. La conversation doit comporter deux aspects. Il y a l'utilisateur malveillant, et cette responsabilité découle de la sécurité publique. Le drone, dans votre exemple, présentait-il un problème de design?

Comme l'a mentionné M. Jones, je crois que nous avons un travail à faire pour veiller à ce que les différents appareils construits et connectés à Internet pour différentes fonctions, y compris le transport des marchandises, respectent des normes minimales de sécurité. Ces protections rendront les véhicules autonomes, les drones et les systèmes de chauffage dignes de confiance, comme le sont une foule d'autres appareils.

Je crois que c'est une question de normes de sécurité. C'est un problème qu'on voit venir, et on est déjà engagé aujourd'hui à le résoudre. Il y a des gens en recherche et développement qui y travaillent. Les manufacturiers sont au courant et ils ont tout à gagner à bien faire les choses. Je crois que c'est un problème réel que l'on comprend et pour lequel on peut prendre des mesures.

Senator Maltais: I understand what you're saying. However, a drone is much more dangerous. I can stop my thermostat manually or I can turn off the electricity if it heats up. If I'm one of the 125 passengers in a Q400 aircraft, I cannot stop the drone.

Drones are nothing new. They have been around for a few years. Why is it that we are not able to stop them or to identify the sources? I do not know how many millions passengers travel by plane in the world. I cannot believe that research organizations have not already found a way to identify and destroy them, and to prosecute the individuals or groups who have put them into circulation. I have trouble understanding this phenomenon. It's 2017, it will soon be 2018. It's about protecting millions of people.

These days, we go to Mars, to the moon and everywhere. However, we are not able to destroy a small drone that can cause the death of a few thousand people. Can you tell us whether, in the near future, instead of developing the iPhone 3 to the iPhone 14, airports will have a small device that can detect nearby drones so that planes can land safely?

Mr. Boucher: I do not have a specific answer to your question. I think prioritizing our critical infrastructure and the related security measures will probably be in line with what you are asking. Thanks to the work we are doing right now, planned jointly with public safety agencies to be in a better position to work with the private sector in terms of critical infrastructure, this problem should come up and be examined. I agree with you in terms of the extent of the problem.

Senator Maltais: Someone whose bank account is drained may die, but it will take a little more time. A drone striking a plane causes death instantly. I think human beings are more valuable than bank accounts.

[*English*]

Senator Wallin: I am sorry that I was out of the room for your presentation. Ironically, I got a fraud call from my financial institution and had to go and deal.If you have dealt with this issue, please just say so and I will look at the records.

I know this is not your line of work, but I want your opinion because of your expertise. Do we actually need to make reporting of incidents mandatory, and if so, to whom?

Le sénateur Maltais : Je vous comprends. Toutefois, un drone est beaucoup plus dangereux. Mon thermostat, je peux l'arrêter manuellement ou en coupant l'électricité s'il chauffe. Si je fais partie des 125 passagers dans un appareil Q400, je ne peux arrêter le drone.

Ce n'est pas d'hier que les drones ont été inventés. Ils circulent depuis quelques années. Comment se fait-il qu'on ne soit ni en mesure de les arrêter ni capable d'identifier les sources? Je ne sais pas combien de millions de passagers dans le monde voyagent par avion. Je ne peux concevoir que les organismes de recherche n'aient pas déjà trouvé le moyen de les identifier, de les détruire et de poursuivre les individus ou groupes qui les ont mis en circulation. J'ai de la difficulté à comprendre ce phénomène. Nous sommes en 2017, nous serons bientôt en 2018. Il y va de la protection de millions de personnes.

Aujourd'hui, on va sur mars, sur la lune et un peu partout. Cependant, on n'est pas capable de détruire un petit drone qui peut causer le décès de quelques milliers de personnes. Pouvez-vous nous dire si, dans un avenir rapproché, au lieu de développer les iPhone 3 au iPhone 14, on aura un petit dispositif dans les aéroports qui puisse détecter les drones qui se trouvent à proximité afin que les avions puissent atterrir en toute sécurité?

M. Boucher : Je n'ai pas de réponse précise à votre question. Je crois que la mise en priorité de nos infrastructures critiques et les actions de sécurité qui s'y joindront se situeront probablement en aval de ce que vous demandez. Grâce au travail que nous faisons en ce moment, qui a été planifié conjointement avec les organismes de sécurité publique pour mieux nous situer dans le but d'intervenir auprès du secteur privé en ce qui concerne les infrastructures critiques, ce problème devrait émerger et être examiné. Je suis d'accord avec vous quant à l'ampleur du problème.

Le sénateur Maltais : Quelqu'un qui se fait vider son compte de banque peut en mourir, mais il faudra un peu plus de temps. Or, un drone qui frappe un avion cause la mort instantanément. La personne humaine a plus de valeur à mes yeux qu'un compte de banque.

[*Traduction*]

La sénatrice Wallin : Je m'excuse d'avoir manqué votre exposé. Ironie du sort, j'ai reçu un appel de mon institution financière concernant une fraude et j'ai dû m'en occuper. Si vous avez traité de cette question, vous n'avez qu'à me le mentionner, et je consulterai le compte rendu.

Je sais que cela ne vise pas votre champ de compétence, mais j'aimerais avoir votre opinion compte tenu de votre expertise. Devons-nous en fait rendre obligatoire la déclaration des incidents? Dans l'affirmative, à quel organisme les signalerions-nous?

Mr. Jones: That's actually a very complex question. There are a few things.

Right now, the victims of any cyberincidents are actually the ones paying the brunt of the cost. There's a significant reputational damage that happens with any sort of reporting, as well as a certain amount of panic. Unfortunately, this is part of the whole lack of security in the industry. We are trying to deal with the rapid growth and the economic incentive that comes with cybercrime.

Mandatory breach reporting is something that has to be done very carefully because it can actually have the opposite effect where you start to create some panic. In a lot of cases, what we have now is breach reporting, which doesn't allow you to actually take action.

The key thing is we have to really work on taking away the stigma of being the victim of cybercrime, helping to reinforce and really focus on enhancing their resiliency against it and looking for what those common causes are. It's almost always the same set of actions that have led to the breach. Very rarely, especially if you're looking at the financial sector, is it the financial industry themselves; it's usually buried down in the supply chain where the breach started. How do we look at the resiliency and start to apply those lessons as we're going forward?

Senator Wallin: We heard from our previous witness that there will be some requirement to report some breach activity through the Privacy Commissioner, but it's not clear to what end. Is it helpful to go to the RCMP, your institution, CSIS or anything else with this information? Is there anything you can actually do about it? What we are also continually hearing is that we're on circuit overload for this stuff.

Mr. Jones: One of the things we've tried to do is be the best victims possible. The Government of Canada does suffer compromises no matter what we do. That's kind of the sign of the times. What I advise when I go and give speeches to companies, I always say, "No matter what you do, you can suffer a cyber breach." There's no way of avoiding it other than disconnecting.

We are trying to be the best victim possible. So we come out, we inform people what's happened, and we take all the measures to protect and ensure what the privacy impacts are. We work with the Privacy Commissioner. We try to show the way so that hopefully it can start to reduce the stigma of being the victim of cyber and determine how to deal with this. How do we make sure we're more resilient? We should be held to make ourselves more resilient so the same thing doesn't happen again.

M. Jones : Vous posez en fait là une question très complexe. Il y a divers éléments.

Actuellement, les victimes de tout cyberincident sont en fait celles qui en font le plus les frais. Toute déclaration cause un grand tort à la réputation ainsi qu'une certaine panique. Malheureusement, c'est lié à la grande question des problèmes de sécurité dans l'industrie. Nous essayons de nous attaquer à la croissance rapide et à l'attrait économique de la cybercriminalité.

L'obligation de déclarer toute atteinte à la sécurité doit être faite très minutieusement, parce que cela peut en fait avoir l'effet contraire, soit de susciter une certaine panique. Dans bien des cas, ce que nous avons actuellement, c'est la déclaration des atteintes à la sécurité, ce qui ne vous permet pas de prendre de mesures.

Nous devons vraiment en priorité éliminer les préjugés entourant les victimes de cybercriminalité, contribuer à renforcer leur résilience en vue de contrer la cybercriminalité et cerner les causes communes. Ce sont pratiquement toujours les mêmes gestes qui ont mené à l'atteinte à la sécurité. C'est très rarement, en particulier dans le secteur financier, l'industrie financière qui est en cause. L'atteinte à la sécurité prend naissance normalement très loin dans la chaîne d'approvisionnement. Comment renforcer cette résilience et commencer à mettre en pratique les leçons retenues à l'avenir?

La sénatrice Wallin : Notre précédent témoin nous a expliqué qu'il faudra signaler toute atteinte à la sécurité au commissaire à la protection de la vie privée, mais le but n'est pas clair. Est-il utile de communiquer ces renseignements à la GRC, à votre organisme, au SCRS ou à d'autres? Pouvez-vous vraiment faire quelque chose à ce chapitre? Nous entendons également sans cesse que nous sommes surchargés dans le domaine.

M. Jones : Nous avons notamment essayé d'être les meilleures victimes possible. Le gouvernement du Canada subit des compromissions, peu importe ce que nous faisons. C'est l'époque dans laquelle nous vivons. Lorsque je prends la parole devant des entreprises, je dis toujours aux gens qu'une compromission est possible, peu importe ce qu'ils font. Il n'y a aucun moyen de l'éviter, mis à part de débrancher l'appareil.

Nous essayons d'être les meilleures victimes possible. Nous prenons la parole; nous informons les gens sur ce qui s'est passé et nous prenons toutes les mesures pour nous protéger et en déterminer les effets sur la protection des renseignements personnels. Nous collaborons avec le commissaire à la protection de la vie privée. Nous essayons de donner l'exemple. Avec un peu de chance, cela permettra de commencer à réduire les préjugés entourant les victimes de cybercriminalité et de trouver des moyens de nous y attaquer. Comment pouvons-nous nous assurer de renforcer notre résilience? Nous devrions être tenus de

Breach reporting is actually a really difficult topic just because of that. It tends to take away from the response and actually dealing with the privacy incident. You deal with a communications event and start to minimize it rather than actually exploring what the true event is. What I've learned in doing a number of incident responses is that what you thought on Day 1 is not how you end on Day 30. It's always something different and much more complex.

Senator Wallin: Maybe there has to be a process, because the answer is, "Well, it's complicated so therefore we shouldn't do it," right?

Mr. Jones: I think the goal would be let's do it in a way that we can help with the response, help with protecting whatever private information is breached and help with figuring out what happened. That's what stance we're trying to take. For anybody who comes and asks for help, we want to try to make sure the government is doing what we can to help them or provide advice.

I really want to put the emphasis on how do we look to make sure we never have to deal with that same type of breach again, but it's a really difficult topic to decide. It's one of those where there are pros and cons in every column.

Senator Wallin: Which way should we be leaning at this point?

Mr. Jones: I think we need to really focus on holding people to resiliency and to doing the things that make them stronger.

Senator Wallin: But how can you hold them to resiliency if you don't know anything happened?

Mr. Jones: That's by working with the industry to define some standards and to determine what good cybersecurity practices look like. The industry is getting better at starting to set baselines for those types of things. That's where I would put my emphasis, in really determining how we collectively define the bar so the bar is high enough. That would prevent a significant amount of cybercrime.

For example, the government is a victim of cybercrime as much as everyone else is. We're able to stop almost all of it. We're almost immune because we've built in enough resiliency that we can take blocks and can take actions. The government is getting better at implementing our basic top 10. It's not perfect — anybody who claims perfection in cybersecurity is lying — but it is getting better.

renforcer notre résilience pour que la même situation ne se reproduise plus.

La déclaration des atteintes à la sécurité est en fait un sujet vraiment difficile pour cette raison. Elle a tendance à mettre davantage l'accent sur l'atteinte à la vie privée plutôt que l'intervention. Vous examinez un incident dans le domaine des communications et vous commencez à le minimiser plutôt qu'à déterminer ce qui s'est vraiment passé. J'ai appris lors d'interventions en cas d'incident que votre opinion au jour 1 sera différente de ce que vous penserez rendu au jour 30. C'est toujours quelque chose de différent et de beaucoup plus complexe.

La sénatrice Wallin : Il faut peut-être un processus, parce que la réponse est que c'est complexe et que nous ne devrions donc rien faire, n'est-ce pas?

M. Jones : Selon moi, l'objectif est de trouver un moyen de contribuer à améliorer la situation grâce à nos interventions, à protéger les renseignements privés compromis et à cerner ce qui s'est produit. C'est la position que nous essayons d'adopter. Lorsqu'une personne vient nous demander notre aide, nous voulons essayer de nous assurer que le gouvernement fait ce qu'il peut pour l'aider et la conseiller.

Je tiens vraiment à mettre l'accent sur la façon de trouver le moyen de nous assurer que ce même type d'atteinte ne se reproduit plus jamais, mais c'est vraiment un sujet difficile. C'est un secteur où il y a des avantages et des inconvénients.

La sénatrice Wallin : De quel côté devrions-nous pencher pour l'instant?

M. Jones : Je crois que nous devrions vraiment mettre l'accent sur le renforcement de la résilience des gens et prendre des mesures pour les rendre plus forts.

La sénatrice Wallin : Cependant, comment pouvons-nous renforcer leur résilience si vous n'êtes pas au courant qu'un incident est survenu?

M. Jones : Nous le faisons en collaborant avec l'industrie pour définir des normes et déterminer les pratiques exemplaires dans le domaine de la cybersécurité. L'industrie réussit de mieux en mieux à établir des points de référence pour ces éléments. Je m'appliquerai à vraiment déterminer comment nous pouvons fixer ensemble des normes suffisamment élevées. Cela contribuerait à prévenir une grande partie de la cybercriminalité.

Par exemple, le gouvernement n'est pas plus à l'abri de la cybercriminalité que les autres, mais nous sommes en mesure de pratiquement arrêter toutes les attaques. Nous sommes pratiquement immunisés à ces attaques, parce que nous avons suffisamment renforcé notre résilience et que nous pouvons bloquer les attaques et prendre des mesures. Le gouvernement arrive de mieux en mieux à mettre en œuvre nos 10 grands

So that starts to take entire classes of bad activity out of the equation. Once you do that, your IT security resources can start to focus on the really sophisticated, the things they really should be looking for. Right now, the industry is being eaten alive by really low-quality cybercrime, except it is incredibly impactful.

Senator Wallin: That's an interesting point.

The Deputy Chair: Mr. Jones, before I go to round two and the two names on my list for second round for follow-up questions, we've had a lot of discussion about how you are supporting and working with the private sector. I think it would be helpful for us if you could explain, just briefly, these various partners that you list. You've listed several key partner organizations and what their mandates are, if you're able to help us with it. The Canadian Cyber Incidence Response Centre is the first one you referred to.

Mr. Jones: Absolutely. Adam Hatfield, who was here yesterday answering your questions, is the director of that organization within Public Safety Canada. That is the overall lead for cyber incident response, Canada's national cyber incident response team. That is what CCIRC is.

The Deputy Chair: If industry had a problem, they would know to contact that entity, and they'd have the phone number or e-mail address right on their desk?

Mr. Jones: That's what our hope is. Certainly if any industry asks us who they should contact if there's an incident, contact CCIRC and we'll make sure we work with them as part of Team Canada to respond.

The Deputy Chair: The Canadian Cyber Threat Exchange?

Mr. Jones: The Canadian Cyber Threat Exchange is a not-for-profit organization that was set up by Canadian industry to promote the sharing of cyber-related information. For example, it could be indicators of compromise. It's a way of removing that stigma of being the victim but sharing when the breach has happened, so sharing what happened, how it happened and what are the things that everybody else should be looking for to try and facilitate that. It was an initiative that the industry had

éléments fondamentaux. Ce n'est pas parfait, mais la situation s'améliore. Quiconque prétend avoir atteint la perfection dans le domaine de la cybersécurité est un menteur.

Bref, cela nous permet de faire abstraction de plusieurs catégories d'activités malveillantes. Ensuite, vos ressources en sécurité informatique peuvent se concentrer sur les attaques vraiment complexes et les activités que vous devez vraiment repérer. Actuellement, l'industrie se fait manger tout rond par de la cybercriminalité de bas étage, qui a, par contre, d'énormes répercussions.

La sénatrice Wallin : C'est un point intéressant.

Le vice-président : Monsieur Jones, avant de passer à la deuxième série de questions et aux deux sénateurs sur ma liste qui ont des questions complémentaires, nous avons beaucoup parlé de votre collaboration avec le secteur privé et du soutien que vous lui offrez. À mon avis, ce serait utile pour nous si vous pouviez nous décrire très brièvement les divers partenaires que vous avez nommés. Vous avez mentionné plusieurs importants organismes partenaires et leur mandat. Je vous saurais gré de bien vouloir nous aider à cet égard. Le Centre canadien de réponse aux incidents cybernétiques est le premier que vous avez mentionné.

M. Jones : Avec plaisir. Adam Hatfield, qui est venu répondre à vos questions hier, est le directeur de cet organisme relevant de Sécurité publique Canada. C'est l'organisme qui assume la direction générale des interventions en cas d'incident cybernétique, soit l'équipe nationale d'intervention en cas d'incident cybernétique. Voilà pour ce qui est du Centre canadien de réponse aux incidents cybernétiques.

Le vice-président : Si l'industrie a un problème, elle est au courant qu'elle peut communiquer avec cet organisme, et les membres de l'industrie ont son numéro de téléphone ou son adresse courriel sur leur bureau.

M. Jones : C'est ce que nous espérons. Si une industrie nous demande l'organisme avec lequel elle doit communiquer en cas d'incident, nous lui disons certainement de communiquer avec le Centre canadien de réponse aux incidents cybernétiques et nous nous ferons un devoir de collaborer avec nos collègues au sein d'Équipe Canada pour intervenir en cas d'incident.

Le vice-président : Qu'en est-il de l'Échange canadien de menaces cybernétiques?

M. Jones : L'Échange canadien de menaces cybernétiques est un organisme sans but lucratif qui a été mis sur pied par l'industrie canadienne en vue de favoriser l'échange de renseignements cybernétiques. Par exemple, il peut s'agir d'indicateurs de compromission. C'est un moyen de faire sauter les préjugés entourant les victimes et de communiquer lorsqu'une atteinte survient. Il faut communiquer ce qui s'est passé, ce qui a mené à l'incident et les éléments que les autres

started and that we are certainly supporting. We are an adviser to the board of directors. We also try to contribute our indicators to that organization to try to foster the sharing of information to make us all a little bit more resilient.

devraient surveiller pour essayer de faciliter le tout. C'était une initiative de l'industrie que nous appuyons évidemment. Notre organisme agit à titre de conseiller auprès du conseil d'administration. Nous essayons également de fournir nos indicateurs à cet organisme pour essayer de stimuler l'échange de renseignements et de renforcer un peu plus la résilience des divers partenaires.

The Deputy Chair: Would the work be duplicated by the Cyber Incident Response Centre?

Le vice-président : N'y a-t-il pas un double emploi avec ce que fait le Centre de réponse aux incidents cybernétiques?

Mr. Jones: No. Actually, I was negligent; I should have mentioned we partner with Public Safety on that as well. We're both advisers. We make sure that we do not duplicate the work there. We support CCTX in also making sure that that information is being shared as widely as possible.

M. Jones : Non. En fait, j'ai fait preuve de négligence. J'aurais dû mentionner que nous collaborons également avec le ministère de la Sécurité publique à cet égard. Nous agissons tous les deux à titre de conseillers. Nous nous assurons d'éviter un tel double emploi. Nous soutenons l'Échange canadien de menaces cybernétiques en nous assurant également que les renseignements sont diffusés au plus grand nombre possible de personnes.

The Deputy Chair: The final one, the Canadian Security Telecommunications Advisory Committee.

Le vice-président : Le dernier est le Comité consultatif canadien pour la sécurité des télécommunications.

Mr. Jones: That is an organization of the federal government and all of Canada's leading telecommunications providers where we work collaboratively on issues such as cybersecurity standards, the things that we all need to be preparing for. We try to share information on where the industry is going so we can get ahead of the technology trends. It's a very open, collaborative forum. It's led by Innovation, Science and Economic Development Canada.We partner there, as well as CSIS and Public Safety, to try and facilitate a productive dialogue with the telecommunications partners to share best practices and build on what things we should be doing together to make Canada more resilient at the foundation.

M. Jones : Il s'agit d'un organisme fédéral qui regroupe tous les principaux fournisseurs canadiens de télécommunications. Ce comité nous permet de collaborer sur des enjeux comme les normes de cybersécurité et les aspects auxquels nous devons tous nous préparer. Nous essayons d'échanger des renseignements sur les tendances dans l'industrie pour anticiper les tendances technologiques à venir. C'est un forum collaboratif très ouvert. Cela relève d'Innovation, Sciences et Développement économique Canada. Notre organisme, le SCRS et le ministère de la Sécurité publique sont des partenaires au sein de ce comité; nous tentons de faciliter la tenue d'un dialogue productif avec les partenaires des télécommunications pour échanger des pratiques exemplaires et mettre l'accent sur ce que nous devons faire de concert pour renforcer la résilience du Canada à la base.

The Deputy Chair: There have been a number of questions here over the last two days to make sure there is not duplication of effort and silos going on. You're satisfied that each of these organizations perform a distinctive function that is best operated separately from the others?

Le vice-président : De nombreuses questions ont été posées depuis deux jours pour nous assurer qu'il n'y a aucun chevauchement et que le travail ne se fait pas en vase clos. Êtes-vous convaincu que chacun de ces organismes remplit une fonction particulière et que la façon optimale de le faire est d'avoir des organismes distincts?

Mr. Jones: The one thing with cyber is it's very pervasive. When you start to look at cyber issues going to pipelines, pipeline security goes into electrical distribution, all of which are sectors with regulation into crossing over federal-provincial-territorial-municipal boundaries, et cetera. I think cybersecurity is one of those issues that is just so horizontal that it does require a lot of collaboration.

M. Jones : Les enjeux cybernétiques sont omniprésents. Lorsque nous commençons à nous pencher sur la cybersécurité quant aux pipelines, nous passons de la sécurité des pipelines au réseau de distribution électrique, et ce sont tous des secteurs réglementés qui touchent les administrations fédérale, provinciales, territoriales, municipales, et cetera. Je crois que la cybersécurité est un enjeu tellement horizontal qu'une grande collaboration est nécessaire.

We work very hard to try to ensure that we don't duplicate. We've gotten better. It's something that we've been working on trying to improve in the federal government. Many years ago, I

Nous travaillons d'arrache-pied pour essayer de nous assurer de ne pas faire double emploi. Nous le faisons mieux. Nous essayons de nous améliorer à ce chapitre au gouvernement

used to describe cybersecurity in the government, when something would happen, as being like six-year-olds playing soccer; everybody would run to the ball and nobody would really be playing. We've gotten better about saying, "Okay, who is playing which position" and working on that.

Right now, it's a matter of where the mandates are set. We're trying to maximize what we can do to support the industry, but it continues to be a challenge, especially with how quickly technology evolves and how quickly industry is changing to represent that.

The Deputy Chair: Who is taking the lead in saying you play that position and you do this and you do that? Who is taking the lead there?

Mr. Jones: We do it collaboratively with the departments, depending on the type of incident.For example, if it looked like it was something that was a compromise within the Government of Canada, we would work with Shared Services Canada and the Treasury Board to make sure we were responding. If it was an incident impacting critical infrastructure, a general cybersecurity incident, depending on whether it was a criminal investigation, RCMP, or general, it would be Public Safety.If it was a national security incident, for example, a state trying to corrupt our critical infrastructure, we would look to support the Canadian Security Intelligence Service in that lead. But really it depends on the type of authority. That's one of the things that we work diligently on, and it's on a constant basis. Whenever any incident comes up, the first thing is who is going to take the lead and how will we work together.

Senator Massicotte: We talked earlier about citizens and consumers. Let's talk about the big picture. What is the level of threat? How comfortable should we be that there's enough resiliency that we should not be threatened? For instance, there is critical infrastructure, hydroelectric plants and nuclear plants, and you referred to pipelines and as well as organizational things. For instance, you talked with your own government, Shared Services Canada. This summer, Revenue Canada was shut down for a couple of days because it was being attacked. All of us certainly were worried. That's a lot of information. We could be exposed. How comfortable are we that we're not exposed in those very serious areas of infrastructure or government information?

fédéral. Il y a de nombreuses années, j'avais l'habitude de comparer la cybersécurité au gouvernement lorsqu'un incident survenait à un groupe d'enfants de six ans qui jouent au soccer. Tout le monde court après le ballon, mais personne ne joue vraiment. Nous réussissons à mieux déterminer les fonctions des divers joueurs et nous y travaillons.

Actuellement, cela dépend de nos mandats. Nous essayons de maximiser ce que nous pouvons faire pour aider l'industrie, mais cela continue d'être un défi, en particulier en raison de la rapide évolution des technologies et de la vitesse à laquelle l'industrie s'y adapte.

Le vice-président : Qui prend l'initiative de déterminer les fonctions des divers organismes et de leur dire qui fait quoi? Qui s'en charge?

M. Jones : Nous le faisons de concert avec les ministères en fonction du type d'incident. Par exemple, si nous avons l'impression qu'il y a eu une compromission au sein du gouvernement du Canada, nous collaborerons avec Services partagés Canada et le Conseil du Trésor pour nous assurer d'intervenir. Dans le cas d'un incident qui touche une infrastructure essentielle ou d'un incident de cybersécurité de nature générale, selon qu'il s'agisse ou non d'une enquête criminelle, d'une enquête de la GRC ou d'une enquête générale, ce serait le ministère de la Sécurité publique. Dans le cas d'un incident lié à la sécurité nationale, soit un État qui tenterait de compromettre notre infrastructure essentielle, par exemple, nous offririons du soutien au Service canadien du renseignement de sécurité qui serait responsable du dossier. Cependant, tout dépend vraiment du type de pouvoirs. Nous poursuivons nos efforts diligents notamment dans ce domaine, et nous le faisons sur une base continue. Lorsqu'un incident survient, la première étape est de déterminer l'organisme qui sera responsable du dossier et la façon dont nous collaborerons.

Le sénateur Massicotte : Nous avons parlé plus tôt des citoyens et des consommateurs. Parlons du portrait global. Quel est le niveau de menace? À quel point devrions-nous être convaincus que notre résilience est suffisante et que nous ne devrions pas être menacés? Par exemple, nous avons des infrastructures essentielles et des centrales hydroélectriques et nucléaires, et vous avez fait allusion aux pipelines et aux questions organisationnelles. Par exemple, vous avez parlé avec des collègues de votre propre gouvernement, soit Services partagés Canada. Cet été, une attaque a interrompu durant quelques jours les services de l'Agence du revenu du Canada. Cela nous a certainement tous inquiétés. Il y a beaucoup d'information. Nos renseignements pourraient être compromis. À quel point sommes-nous convaincus que nous ne courrons aucun risque concernant ces secteurs très importants de notre infrastructure ou ces renseignements gouvernementaux?

Mr. Jones: Actually, it is a sector-by-sector approach. If you look, the level of threat is growing. Cybercrime especially is growing rapidly. There's a huge financial incentive for the criminals to spend money to do this.In many cases of cybercrime, there's a 24-hour hotline to buy tools, where you can get support, ask for help, et cetera. It's quite astounding how much infrastructure there is. The threat level continues to grow.

In the Government of Canada, we have done a lot to increase our resiliency. The incident you're referring to with Revenue Canada also impacted Statistics Canada. We took proactive measures to make sure we weren't breached. We had enough situational awareness that we could take a proactive measure when we found out that the system was vulnerable.

Depending on where you go, some organizations are quite mature in cybersecurity and some aren't. That's something that is a big concern. I'm not going to try to say that the level of cybersecurity in Canada is high. There are some places that are quite behind that we have to work with. There are some organizations that invest quite heavily in protection and in increasing their resiliency.

The banking sector is one of those where they do invest. They see this as something that is not only a threat but something they have to stay ahead of to ensure confidence. We work with them and with a number of banks organizations. They continue to invest. In fact, many banks have a larger cybersecurity organization than I run for the Government of Canada.

When you go to different pieces of critical infrastructure, it's really variable, but I would say that the level of resiliency in general in Canada is probably low.

Senator Unger: Mr. Jones, you talked about your mandate. Part A involves a collection of foreign intelligence in accordance with Government of Canada intelligence. Through your presentation, you talked about who you work with. How large is your organization?

Mr. Jones: The IT security portion of CSE or CSE in general?

Senator Unger: Your specific overall area.

M. Jones : En fait, c'est une démarche secteur par secteur. Si nous regardons la situation, le niveau de menace augmente. En particulier, la cybercriminalité connaît une croissance rapide. Les criminels ont un énorme intérêt financier à investir de l'argent dans ce domaine. Dans la majorité des incidents de cybercriminalité, il y a un numéro d'urgence où vous pouvez acheter des outils, obtenir du soutien, demander de l'aide, et cetera. La taille de l'infrastructure est assez étonnante. Le niveau de menace continue de croître.

Au gouvernement du Canada, nous avons pris énormément de mesures pour renforcer notre résilience. L'incident auquel vous avez fait allusion a touché l'Agence du revenu du Canada, mais ses effets se sont également fait sentir à Statistique Canada. Nous avons pris des mesures proactives pour nous assurer que nos données n'avaient pas été compromises. Nous étions suffisamment au courant de la situation pour prendre une mesure proactive lorsque nous avons découvert que le système était vulnérable.

Selon l'endroit où vous regardez, certains organismes ont beaucoup d'expérience dans la cybersécurité, mais nous ne pouvons pas en dire autant pour d'autres. C'est quelque chose de très inquiétant. Je ne vais pas essayer de vous laisser entendre que le niveau de cybersécurité au Canada est élevé. Il y en a certains qui accusent un énorme retard en la matière, et nous devons collaborer avec eux. À l'opposé, il y a des organismes qui investissent énormément dans leur protection en vue de renforcer leur résilience.

Le secteur bancaire est l'un des secteurs qui investissent en la matière. Il voit cela comme une menace, mais il le voit aussi comme un aspect au sujet duquel il doit conserver une longueur d'avance pour maintenir la confiance des consommateurs. Nous collaborons avec le secteur et bon nombre d'institutions bancaires. Ces groupes continuent d'investir. En fait, un grand nombre de banques participent à un important regroupement sur la cybersécurité que je dirige pour le gouvernement du Canada.

Si vous examinez divers éléments de l'infrastructure essentielle, c'est vraiment variable, mais je dirais que le niveau de résilience en général au Canada est probablement faible.

La sénatrice Unger : Monsieur Jones, vous avez parlé de votre mandat. La partie A comprend la collecte de renseignement étranger, conformément aux priorités en matière de renseignement du gouvernement du Canada. Dans votre exposé, vous avez parlé des organismes avec lesquels vous travaillez. Quelle est la grosseur de votre organisme?

M. Jones : La Sécurité des TI du CST ou le CST en général?

La sénatrice Unger : Votre secteur précis.

Mr. Jones: Right now, 497 is the number today. That is growing slightly. We have responsibilities ranging from what we've talked about today, which is primarily cyberdefence, but also we provide all the cryptographic equipment for the Government of Canada as well. For every piece of Canadian Forces communications equipment, we provide the cryptography for that, the equipment that they use to secure, the keys, et cetera, and we do that in a very tight partnership.The number is a little deceptive. Most of the cybersecurity side of things is probably on the order of around 200 or 250 people.

The Deputy Chair: Thank you very much. That's a good note to adjourn on. We very much appreciate the Communications Security Establishment representatives, Mr. Jones and Mr. Boucher. Thank you for being here. Keep up the good work. We're counting on you.

(The committee adjourned.)

M. Jones : Nous sommes actuellement 497, et cela augmente légèrement. Nos responsabilités touchent ce dont nous avons parlé aujourd'hui, soit principalement la cyberdéfense, mais nous fournissons aussi tout l'équipement cryptographique qu'utilise le gouvernement du Canada. Nous nous occupons du chiffrement de chaque dispositif de communication des Forces canadiennes. Nous leur fournissons l'équipement qu'elles utilisent pour protéger leurs données, les clés, et cetera. Nous collaborons très étroitement avec les Forces canadiennes pour ce faire. Toutefois, le nombre est un peu trompeur. Nous avons probablement environ 200 ou 250 personnes qui s'occupent en gros de la cybersécurité.

Le vice-président : Merci beaucoup. C'est un bon commentaire pour clore notre réunion. Nous sommes très reconnaissants des commentaires des représentants du Centre de la sécurité des télécommunications. Messieurs Jones et Boucher, merci de votre présence. Continuez votre bon travail. Nous comptons sur vous.

(La séance est levée.)

WITNESSES

Wednesday, October 18, 2017

Public Safety Canada:

Adam Hatfield, Acting Director General, National Cyber Security Directorate.

Royal Canadian Mounted Police:

Chief Superintendent Scott Doran, Director General, Federal Policing Criminal Operations;

Superintendent Mark Flynn, Director, Cybercrime, Federal Policing.

Canadian Security Intelligence Service:

Charles Lowson, Director General, Counter Intelligence and Counter Proliferation.

Thursday, October 19, 2017

Smart Cybersecurity Network (SERENE-RISC):

Benoît Dupont, Scientific Director (by video conference).

Communications Security Establishment:

Scott Jones, Deputy Chief, IT Security;

André Boucher, Director General, Cyber Security Partnerships.

TÉMOINS

Le mercredi 18 octobre 2017

Sécurité publique Canada :

Adam Hatfield, directeur général par intérim, Direction de la cybersécurité nationale.

Gendarmerie royale du Canada :

Surintendant principal Scott Doran, directeur général, Opérations criminelles de la Police fédérale;

Surintendant Mark Flynn, directeur, Cybercriminalité, Police fédérale.

Service canadien du renseignement de sécurité :

Charles Lowson, directeur général, Contre-espionnage et Lutte contre la prolifération.

Le jeudi 19 octobre 2017

Réseau intégré sur la cybersécurité (SERENE-RISC) :

Benoît Dupont, directeur scientifique (par vidéoconférence).

Centre de la sécurité des télécommunications :

Scott Jones, chef adjoint, Sécurité des TI;

André Boucher, directeur général, Partenariats en cybersécurité.