First Session
Thirty-seventh Parliament, 2001

SENATE OF CANADA

Proceedings of the Standing Senate Committee on

Defence and Security

Chair:
The Honourable COLIN KENNY

Thursday, July 19, 2001

Issue No. 2

Third and fourth meetings on:
An introductory survey of the major security and defence issues facing Canada with a view to preparing a detailed work plan for future comprehensive studies

WITNESSES:
(*See back cover*)

Première session de la
trente-septième législature, 2001

SÉNAT DU CANADA

Délibérations du Comité sénatorial permanent de la

Défense et de la sécurité

Président:
L'honorable COLIN KENNY

Le jeudi 19 juillet 2001

Fascicule nº 2

Troisième et quatrième réunions concernant:
Étude préliminaire des principales questions de défense et de sécurité qui touchent le Canada en vue de la préparation d'un plan de travail détaillé pour des études plus poussées

TÉMOINS:
(*Voir à l'endos*)

38256-38257

THE COMMITTEE ON DEFENCE AND SECURITY

The Honourable Colin Kenny, *Chair*

The Honourable J. Michael Forrestall, *Deputy Chair*

and

The Honourable Senators:

Atkins
Banks
* Carstairs, P.C.
(or Robichaud, P.C.)
Cordy
Lynch-Staunton
(or Kinsella)
Meighen
Oliver
Pépin
Stollery
Wiebe

* *Ex Officio Members*

(Quorum 4)

LE COMITÉ DE LA DÉFENSE ET DE LA SÉCURITÉ

Président: L'honorable Colin Kenny

Vice-président: L'honorable J. Michael Forrestall

et

Les honorables sénateurs:

Atkins
Banks
* Carstairs, c.p.
(ou Robichaud, c.p.)
* Lynch-Staunton
(ou Kinsella)
Meighen
Oliver
Pépin
Stollery
Wiebe

* *Membres d'office*

(Quorum 4)

MINUTES OF PROCEEDINGS

OTTAWA, Thursday, July 19, 2001
(6)

[*English*]

The Standing Senate Committee on Defence and Security met this day, at 8:45 a.m. in Room 705, Victoria Building, the Chair, the Honourable Colin Kenny, presiding.

Members of the committee present: The Honourable Senators Atkins, Banks, Cordy, Forrestall, Kenny, Meighen, Pépin, Wiebe (8).

In attendance: Grant Purves, Research Officer, Parliamentary Research Branch, Library of Parliament, and Mr. Roy Berlinquette, Adviser, Security.

WITNESSES:

From the Department of the Solicitor General:

Mr. Michel D'Avignon, Director General, National Security, Policing and Security Branch;

Ms Annie Leblanc, Acting Director, Technology and Lawful Access Division; and

Mr. Mike Theilmann, Acting Director, Counter-Terrorism Division.

From the Royal Canadian Mounted Police:

Superintendent J. Wayne Pilgrim, Officer in Charge, National Security Investigations Branch, Criminal Intelligence Directorate.

Pursuant to the Order of Reference adopted by the Senate on Thursday, May 31, 2001, the committee proceeded to its introductory survey of the major security and defence issues facing Canada with a view to preparing a detailed work plan for future comprehensive studies. *(See Issue No. 1, Monday, July 18, 2001, for the full text of the Order of Reference.)*

Mr. D'Avignon made an opening statement then, along with other witnesses, answered questions.

At 10:15 a.m., the committee suspended its meeting.

At 10:30 a.m., the committee resumed its meeting.

Superintendent Pilgrim made an opening statement and answered questions.

At 12:05 p.m., the committee adjourned to the call of the Chair.

ATTEST:

OTTAWA, Thursday, July 19, 2001
(7)

[*English*]

The Standing Senate Committee on Defence and Security met this day, at 2:15 p.m. in Room 705, Victoria Building, the Chair, the Honourable Colin Kenny, presiding.

PROCÈS-VERBAL

OTTAWA, le jeudi 19 juillet 2001
(6)

[*Traduction*]

Le Comité sénatorial permanent de la défense et de la sécurité se réunit aujourd'hui à 8 h 45, dans la pièce 705 de l'Édifice Victoria, sous la présidence de l'honorable Colin Kenny (*président*).

Membres du comité présents: Les honorables sénateurs Atkins, Banks, Cordy, Forrestall, Kenny, Meighen, Pépin et Wiebe (8).

Également présents: Grant Purves, recherchiste, Direction de la recherche parlementaire, Bibliothèque du Parlement, et M. Roy Berlinquette, conseiller, Sécurité.

TÉMOINS:

Du ministère du Solliciteur général:

M. Michel D'Avignon, directeur général, Sécurité nationale, Secteur de la police et de la sécurité;

Mme Annie Leblanc, directrice intérimaire, Division de la technologie et de l'accès légal; et

M. Mike Theilmann, directeur intérimaire, Division de la lutte contre le terrorisme.

De la Gendarmerie royale du Canada:

Le surintendant J. Wayne Pilgrim, officier responsable de la Sous-direction des enquêtes relatives à la sécurité nationale, Direction des renseignements criminels.

Conformément à l'ordre de renvoi adopté par le Sénat le jeudi 31 mai 2001, le comité fait une étude préliminaire des principales questions de défense et de sécurité qui touchent le Canada en vue de la préparation d'un plan de travail détaillé pour des études plus poussées. *(Voir fascicule nº 1 du lundi 18 juillet 2001 pour le texte complet de l'ordre de renvoi.)*

M. D'Avignon fait une déclaration puis, aux côtés d'autres témoins, répond aux questions.

À 10 h 15, le comité suspend la séance.

À 10 h 30, le comité reprend la séance.

Le surintendant Pilgrim fait une déclaration et répond aux questions.

À 12 h 05, le comité suspend ses travaux jusqu'à nouvelle convocation de la présidence.

ATTESTÉ:

OTTAWA, le jeudi 19 juillet 2001
(7)

[*Traduction*]

Le Comité sénatorial permanent de la défense et de la sécurité se réunit aujourd'hui à 14 h 15, dans la salle 705 de l'édifice Victoria, sous la présidence de l'honorable Colin Kenny.

Members of the committee present: The Honourable Senators Atkins, Banks, Cordy, Forrestall, Kenny, Pépin, Wiebe (7).

Other senator present: The Honourable Senator Stratton (1).

In attendance: From the Parliamentary Research Branch, Library of Parliament: Grant Purves, Research Officer.

WITNESSES:

From the Department of National Defence:

Mr. James Harlick, Assistant Deputy Minister, Office of Critical Infrastructure Protection and Emergency Preparedness;

Mr. Gary O'Bright, Director General, Operations, Office of Critical Infrastructure Protection and Emergency Preparedness; and

Mr. Alan Bartley, Director General, Policy Planning and Readiness, Office of Critical Infrastructure Protection and Emergency Preparedness.

Pursuant to the Order of Reference adopted by the Senate on Thursday, May 31, 2001, the committee proceeded to its introductory survey of the major security and defence issues facing Canada with a view to preparing a detailed work plan for future comprehensive studies. *(See Issue No. 1, Monday July 18, 2001, for the full text of the Order of Reference.)*

Mr. Harlick made an opening statement and answered questions.

At 3:45 p.m., the committee continued *in camera.*

It was moved — That the Subcommittee on Veterans Affairs be composed of the following members: the Honourable Senators Meighen (Chair), Wiebe (Deputy Chair), Atkins, Pépin, Kenny, ex-officio.

The question being put on motion, it was resolved in the affirmative.

At 3:53 p.m., the committee adjourned to the call of the Chair.

ATTEST:

Membres du comité présents: Les honorables sénateurs Atkins, Banks, Cordy, Forrestall, Kenny, Pépin et Wiebe (7).

Autre sénateur présent: L'honorable sénateur Stratton (1).

Présents: De la Direction générale de la recherche parlementaire, Bibliothèque du Parlement: Grant Purves, agent de recherche.

TÉMOINS:

Du ministère de la Défense nationale:

M. James Harlick, sous-ministre adjoint, Bureau de la protection des infrastructures essentielles et de la protection civile;

M. Gary O'Bright, directeur général, Opérations, Bureau de la protection des infrastructures essentielles et de la protection civile;

M. Alan Bartley, directeur général, Planification des politiques et disponibilité opérationnelle, Bureau de la protection des infrastructures essentielles et de la protection civile.

Conformément à l'ordre de renvoi adopté par le Sénat le jeudi 31 mars 2001, le Comité a procédé à une étude préliminaire des principales questions de défense et de sécurité qui touchent le Canada en vue de la préparation d'un plan de travail détaillé pour des études plus poussées. (*Voir fascicule nº 1, lundi 18 juillet 2001, pour le texte complet de l'ordre de renvoi.*)

M. Harlick fait une déclaration préliminaire et répond aux questions.

À 15 h 45, le comité poursuit ses travaux à huis clos.

Il est proposé — Que le Sous-comité des affaires des anciens combattants soit composé des membres suivants: les honorables sénateurs Meighen (président), Wiebe (vice-président), Atkins, Pépin, Kenny, ex-officio.

La question est mise aux voix et adoptée.

À 15 h 53, le comité s'ajourne à la convocation de la présidence.

ATTESTÉ:

La greffière du comité,

Barbara Reynolds

Clerk of the Committee

EVIDENCE

OTTAWA, Thursday, July 19, 2001

The Standing Senate Committee on Defence and Security met this day at 8:45 a.m. to conduct an introductory survey of the major security and defence issues facing Canada with a view to preparing a detailed work plan for future comprehensive studies.

Senator Colin Kenny (*Chairman*) in the Chair.

[*English*]

The Chairman: Good morning, ladies and gentlemen. Whether you are here in person or are watching the proceedings on television, welcome to a meeting of the Standing Senate Committee on Defence and Security.

Our committee is the first permanent Senate committee with a mandate to examine matters of security and defence. We are continuing our introductory overview of issues that relate to our mandate.

Today, our first witness is Mr. Michel D'Avignon, who has been a federal public servant for 29 years. He has occupied successively senior positions in a number of departments and agencies, including the Public Service Commission, the Privy Council Office, Indian and Northern Affairs, and the Canadian Security Intelligence Service. Mr. D'Avignon is currently Director General of the National Security Directorate at the Department of the Solicitor General.

Mr. D'Avignon will provide an overview of responsibilities in the federal government for national security. He is accompanied by two officials from the department of the Solicitor General, Ms Annie Leblanc, Acting Director, Technology and Lawful Access Division, and Mr. Mike Theilman, Acting Director, Counter-Terrorism Division.

Welcome to the Senate committee. The floor is yours, Mr. D'Avignon.

[*Translation*]

Mr. Michel D'Avignon, Director General, National Security, Policing and Security Branch: I am very pleased to be with you today to provide a brief overview of the portfolio, with a particular emphasis on the Department of the Solicitor General and its national security role/responsibilities and how it fits into the overall government security structure.

[*English*]

I will also provide a brief description of how we are working with the U.S. and other allies to both strengthen domestic national security and to bolster international efforts to combat international security threats such as terrorism.

I then will turn to the work that the Department of the Solicitor General is undertaking at the present time to improve national security.

TÉMOIGNAGES

OTTAWA, le jeudi 19 juillet 2001

Le Comité sénatorial permanent de la défense et de la sécurité se réunit ce jour à 8 h 45 dans le cadre de son étude préliminaire des principales questions de défense et de sécurité qui touchent le Canada en vue de la préparation d'un plan de travail détaillé pour des études plus poussées.

Le sénateur Colin Kenny (*président*) occupe la fauteuil.

[*Traduction*]

Le président: Bonjour, mesdames et messieurs. Que vous soyez ici en personne ou que vous soyez en train de nous suivre à la télévision, bienvenue à cette séance du Comité sénatorial permanent de la défense et de la sécurité.

Notre comité est le premier comité sénatorial permanent chargé d'examiner des questions de défense et de sécurité. Nous poursuivons notre étude préliminaire des dossiers qui relèvent de notre mandat.

Aujourd'hui, notre premier témoin est M. Michel D'Avignon, qui est à l'emploi de la fonction publique fédérale depuis 29 ans. Il a successivement occupé des postes supérieurs au sein d'un certain nombre de ministères et d'organismes, notamment la Commission de la fonction publique, le Bureau du Conseil privé, Affaires indiennes et du Nord, et le Service canadien du renseignement de sécurité. M. D'Avignon est actuellement directeur général, Direction générale de la sécurité nationale, ministère du Solliciteur général.

M. D'Avignon nous fera un survol des responsabilités du gouvernement fédéral en matière de sécurité nationale. Il est accompagné de deux fonctionnaires du ministère du Solliciteur général, Mme Annie Leblanc, directrice intérimaire, Division de la technologie et de l'accès légal, et M. Mike Theilman, directeur intérimaire, Division de la lutte contre le terrorisme.

Bienvenue devant le comité sénatorial. Vous avez la parole, M. D'Avignon.

[*Français*]

M. Michel D'Avignon, directeur général, Sécurité nationale, Secteur de la police et de la sécurité: Il me fait plaisir d'être des vôtres aujourd'hui afin de vous présenter un survol du portfolio du solliciteur général, en portant une attention particulière sur le ministère du solliciteur général, son rôle et ses responsabilités en matière de sécurité nationale, ainsi que la façon dont celle-ci s'inscrit dans le cadre général du gouvernement.

[*Traduction*]

Je vais également vous faire une brève description de la façon dont nous travaillons avec les États-Unis et d'autres alliés en vue et de renforcer la sécurité nationale à l'intérieur du pays et d'augmenter les efforts internationaux visant à combattre les menaces à la sécurité internationale, comme par exemple le terrorisme.

Je traiterai ensuite du travail qu'entreprend présentement le ministère du Solliciteur général dans le but d'améliorer la sécurité nationale.

[*Translation*]

And last, I want to say a few words on what we perceive to be the immediate challenges facing us from a national security perspective.

I would like to preface my remarks today by noting that the national security apparatus of the government is much larger than the Portfolio of the Solicitor General alone, although the Portfolio does play a central role.

[*English*]

The Departments of National Defence, Foreign Affairs and International Trade, Justice, Canada Customs and Revenue Agency, Citizenship and Immigration, Health Canada and Transport Canada all share with the portfolio responsibility for the protection of Canada's national security.

It should also be noted that the Privy Council Office, through the coordinator of security and intelligence, works to advise the Prime Minister and cabinet on all national security issues. In short, Canada's national security community is indeed something that is greater than the sum of its composite parts.

The Solicitor General of Canada is the lead minister for public safety in Canada and has statutory responsibility for national security, policing and law enforcement, including Aboriginal policing, and corrections and conditional release.

The Solicitor General is supported in his responsibilities by a portfolio that is comprised of the department itself, four agencies — Correctional Service of Canada, National Parole Board, Canadian Security Intelligence Service, and Royal Canadian Mounted Police — and three review bodies, the RCMP Public Complaints Commission, the RCMP External Review Committee, and the Office of the Correctional Investigator.

The central role of the Solicitor General in national security derives from his responsibility for coordinating Canada's response to terrorist incidents and for ensuring that our national response arrangements are effective.

During a terrorist incident or threat, the Solicitor General is also the lead government public spokesperson and is responsible for providing advice to the Prime Minister and cabinet colleagues. The minister, along with the Minister of National Defence, also plays a key role in authorizing, if necessary, military support to assist the police response to a terrorist incident. The Solicitor General's lead role for national security also reflects his responsibility for both the RCMP and the Canadian Security Intelligence Service, two agencies with a key national security mandate and responsibility. As both these organizations will be speaking with you later today, I will not go into any great detail about their roles and responsibilities.

[*Français*]

Enfin, je vous dirai quelques mots sur ce que nous percevons être les défis immédiats auxquels nous devons faire face selon la perspective de la sécurité nationale.

J'aimerais souligner que l'appareil gouvernemental en matière de sécurité nationale dépasse largement le portfolio du solliciteur général, nonobstant le rôle central que joue le portfolio.

[*Traduction*]

Les ministères de la Défense nationale, des Affaires étrangères et du Commerce international, de la Justice, l'Agence des douanes et du revenu du Canada, Citoyenneté et Immigration, Santé Canada et Transports Canada ont tous une part de responsabilité dans le portefeuille en vue de la protection de la sécurité nationale du Canada.

Il convient de souligner également que le Bureau du Conseil privé, par le biais du coordonnateur de la sécurité et du renseignement, conseille le premier ministre et le Cabinet relativement à toutes les questions de sécurité nationale. En bref, la communauté de la sécurité nationale du Canada est véritablement une chose qui est plus grande que l'ensemble des éléments qui la composent.

Le solliciteur général du Canada est le principal ministre responsable de la sécurité publique au Canada et il a pour mandat de veiller à la sécurité nationale, à la police et à l'application de la loi, dont la police des Autochtones, et au système correctionnel et à la mise en liberté sous condition.

Le solliciteur général est, dans le cadre de l'exécution de ses responsabilités, appuyé par un portefeuille composé du ministère lui-même, de quatre agences — le Service correctionnel du Canada, la Commission nationale des libérations conditionnelles, le Service canadien du renseignement de sécurité et la Gendarmerie royale du Canada — et trois organes de surveillance, la Commission des plaintes du public contre la GRC, le Comité externe d'examen de la GRC et le Bureau de l'enquêteur correctionnel.

Le rôle central du solliciteur général en matière de sécurité nationale découle de sa responsabilité de coordonner la réaction du Canada aux incidents terroristes et de veiller à ce que nos mesures nationales d'intervention soient efficaces.

Lors d'une menace ou d'un incident terroriste, le solliciteur général est par ailleurs le principal porte-parole public du gouvernement et le ministre responsable de donner des conseils au premier ministre et au Cabinet. Le solliciteur général, conjointement avec le ministre de la Défense nationale, joue également un rôle clé pour autoriser, au besoin, un soutien militaire à l'appui des services de police face à un incident terroriste. Le rôle de premier plan qui revient au solliciteur général en matière de sécurité nationale reflète par ailleurs le fait qu'il soit responsable et de la GRC et du SCRS, deux organismes qui ont des mandats et des responsabilités stratégiques en matière de sécurité nationale. Étant donné que des représentants de ces deux organismes vont vous entretenir plus tard aujourd'hui, je

[*Translation*]

The department supports the minister in his national security responsibilities by providing independent policy advice on national security issues. In this capacity, the department assumes a lead role in the planning, coordination and implementation of the government's national security policies. The bulk of this work falls to the National Security Directorate, for which I am responsible.

[*English*]

Often, our work is to act as a catalyst, either bringing the portfolio or the broader federal community together to address national security issues that need a horizontal approach. For example, we are involved in bringing the portfolio together to work with the new office of Critical Infrastructure Protection and Emergency Preparedness to identify areas where we can cooperate and forge partnerships.

The National Security Directorate is made up of three divisions. The Security Policy Division is responsible for independent advice and support to the minister on national security issues generally and support to him in his direction, control and accountability for CSIS. Another division is the Counter-Terrorism Division, which supports the minister in his lead responsibility for Canada's counterterrorism program. It includes maintaining the national counterterrorism plan and the complementary operation readiness program. The third division is the Lawful Access Division. As the title suggests, it is responsible for advising the minister on issues related to maintaining the lawful intercept and search and seizure capabilities of police and security agencies.

I would like to take a few moments to describe in more detail the role and responsibilities of these three divisions.

The Security Policy Division often represents departmental or portfolio interests on broad national security issues. For example, the division represents the portfolio interests in the review that is underway of the government security policy. The division's other chief responsibility is to support the Solicitor General and the Deputy Solicitor General in the exercise of their statutory responsibilities under the CSIS Act and the Security Offences Act.

The Counter-Terrorism Division is responsible for the national counterterrorism plan, which was approved by the government in 1989. The plan is the heart of our national counterterrorism arrangements. The overall aim of the plan is to ensure coordination of counterterrorism roles, responsibilities and resources of federal departments and agencies and other levels of government and law enforcement agencies in Canada. The plan is considered a living document and, as such, is subject to periodic

n'entrerai pas davantage dans le détail quant à leurs rôles et responsabilités.

[*Français*]

Le ministère appuie le ministre dans l'exercice de ses fonctions en lui prodigant des conseils sur des questions de politique et de sécurité nationale. Le ministère joue un rôle de première importance dans la planification, la coordination et la mise en place de politiques gouvernementales sur des questions de sécurité nationale. La majeure partie de ce travail revient à la direction générale de la Sécurité nationale, dont je suis responsable.

[*Traduction*]

Souvent, notre travail est de jouer le rôle de catalyseur, pour rassembler ou le portefeuille ou la communauté fédérale plus large afin de réagir à des questions de sécurité nationale qui exigent une approche horizontale. Par exemple, nous nous occupons de réorganiser le portefeuille dans le but d'oeuvrer aux côtés du nouveau Bureau de la protection des infrastructures essentielles et de la protection civile à la détermination de domaines dans lesquels nous pourrons collaborer et forger des partenariats.

La Direction générale de la sécurité nationale réunit trois divisions. La Division de la politique en matière de sécurité est chargée de fournir au ministre conseils et soutien indépendants pour l'ensemble des questions de sécurité nationale et de l'appuyer dans son travail de direction, de contrôle et de reddition de comptes à l'égard du SCRS. Une autre division est celle de la lutte contre le terrorisme. Celle-ci appuie le ministre relativement au programme canadien de lutte contre le terrorisme. Relève de lui le maintien du Plan national de lutte contre le terrorisme, et du programme de préparation opérationnelle complémentaire. La troisième division est celle de l'accès légal. Comme son nom l'indique, celle-ci a pour rôle de conseiller le ministre relativement aux questions touchant l'interception légale de communications et les fouilles et saisies menées par les forces policières et de sécurité.

J'aimerais maintenant prendre quelques instants pour vous faire une description plus détaillée du rôle et des responsabilités de ces trois divisions.

La Division de la politique en matière de sécurité défend souvent les intérêts du ministère ou du portefeuille dans le cadre de questions de sécurité nationale générale. Par exemple, la division représente les intérêts du portefeuille dans le contexte de l'examen en cours portant sur la politique du gouvernement en matière de sécurité. L'autre principale responsabilité de la division est d'appuyer le solliciteur général et le solliciteur général adjoint dans l'exécution des responsabilités statutaires qui leur reviennent en vertu de la Loi sur le Service canadien du renseignement de sécurité et de la Loi sur les infractions en matière de sécurité.

La Division de la lutte contre le terrorisme est responsable du Plan national de lutte contre le terrorisme qui a été approuvé par le gouvernement en 1989. Ce plan est au coeur de nos mesures nationales antiterrorisme. L'objet d'ensemble du plan est de veiller à la coordination des rôles, responsabilités et ressources en matière d'antiterrorisme des ministères et organismes fédéraux ainsi que des autres paliers de gouvernement et des organismes de maintien de l'ordre du pays. Le plan est considéré comme étant un

revisions that reflect lessons learned during exercises, changing roles and responsibilities and, perhaps most important, changing trends in terrorism.

A larger and more fundamental two-year review of the plan was completed in May 2000. This review included consultations with federal partners, the provinces and territories, all RCMP divisions and major municipal police forces. The end result is a much more user-friendly plan that, among other things, takes into account the threat of chemical, biological, radiological and nuclear terrorism.

When the plan was approved in 1989, the Department of the Solicitor General was also given responsibility for evaluating, amending and exercising the plan on an ongoing basis. In response, the department developed the operational readiness program, which consists of exercises, seminars and workshops, and other training vehicles.

[*Translation*]

The program has several objectives. First, to create awareness of national counter-terrorism arrangements and resources, particularly among first responders and other levels of government; second, to provide training opportunities where the integration of the policy and operational response to terrorist incidents can be practised; third, to promote the use of best practices in counter-terrorism response; and finally, to identify areas for improvement and ensure that our arrangements are in keeping with the threat environment.

[*English*]

The national counterterrorism plan and the operational readiness program are mutually reinforcing. The overall result is a continually evolving cycle that promotes improvement and hones our counterterrorism arrangements.

Lawful access consists of the court-authorized search and seizure of information and the lawful interception of communications. For federal and non-federal enforcement agencies, lawful access is an essential tool, especially in the investigation and prevention of organized crime and terrorism.

However, the agency's investigating capabilities is continually eroded by the illicit use of new technologies. Complex technologies such as those developed to maximize the speed, volume and security of communications are increasingly challenging conventional lawful access methods.

With globalization, networks are now connected worldwide. This presents complex technical and legal challenges. In this context, Canada must work with its allies to combat trans-border high-tech crime. Deregulation has resulted in a rapid increase in the number of equipment manufacturers and service providers. In order to maintain lawful access to communications, law enforcement agencies must now deal with a wide range of companies and, consequently, a more diversified combination of

document vivant et fait en tant que tel l'objet de révisions périodiques destinées à refléter les leçons apprises pendant les exercices menés, l'évolution des rôles et responsabilités et, ce qui est peut-être le plus important, les nouvelles tendances du terrorisme.

Un examen plus vaste et plus approfondi du plan, échelonné sur deux ans, a été terminé en mai 2000. Cet examen a comporté des consultations avec des partenaires fédéraux, les provinces et les territoires, toutes les divisions de la GRC et les principales forces de police municipales. Le résultat est un plan beaucoup plus convivial qui, entre autres choses, tient compte de la menace de terrorisme chimique, biologique, radiologique et nucléaire.

Lors de l'approbation du plan en 1989, le ministère du Solliciteur général s'était également vu chargé d'évaluer, de modifier et d'appliquer le plan de façon permanente. C'est ainsi que le ministère a élaboré son programme de préparation opérationnelle comportant exercices, conférences et ateliers et autres véhicules d'apprentissage et de formation.

[*Français*]

Le programme comporte plusieurs objectifs. Premièrement, offrir une plus grande connaissance des accords et des ressources antiterroristes en place, plus particulièrement auprès des premiers répondants et ensuite aux autres paliers de gouvernement. Deuxièmement, créer des occasions favorables de formation qui faciliteraient l'intégration de la politique et la riposte de force de la sécurité à la suite d'un incident terroriste. Troisièmement, promouvoir de meilleures pratiques dans la gestion d'un incident terroriste. Finalement, apporter des améliorations où il y a lieu afin de répondre efficacement aux menaces contre la sécurité.

[*Traduction*]

Le plan national de lutte contre le terrorisme et le programme de préparation opérationnelle se renforcent l'un l'autre. Le résultat d'ensemble est un cycle en évolution constante qui fait la promotion de l'amélioration et met au point nos mécanismes antiterrorisme.

L'accès légal recouvre les fouilles et les saisies d'information autorisées par un tribunal et l'interception légale de communications. Pour les organismes de maintien de l'ordre fédéraux et non fédéraux, l'accès légal est un outil utile, dans le cadre surtout des enquêtes et de la prévention de la criminalité organisée et du terrorisme.

Les capacités d'enquête de ces organismes sont cependant sans cesse entamées par l'utilisation illicite de nouvelles technologies. Des technologies complexes, comme celles mises au point en vue de maximiser la vitesse, la volume et la sécurité des communications, posent à l'égard des méthodes conventionnelles d'accès licite des défis de plus en plus importants.

Avec la mondialisation, les réseaux sont aujourd'hui raccordés les uns les autres à l'échelle planétaire, ce qui présente des défis techniques et juridiques complexes. Dans ce contexte, le Canada doit travailler aux côtés de ses alliés pour combattre la criminalité technologique transfrontalière. La déréglementation a débouché sur une augmentation rapide du nombre de fabricants de matériel et de fournisseurs de services. Afin de maintenir un accès légal aux communications, les forces de police doivent aujourd'hui

network infrastructure. Authorities need to retain their capability to lawfully access the information and communications essential to fulfil the mandate granted to them by Parliament.

The department continues to work either directly or in support of foreign affairs to strengthen security cooperation and coordination with the United States. The Ahmed Ressam investigation and trial illustrated that we have strong effective working relationships in both the government-to-government and operational levels. The same level of cooperation has been evident in the trial of Mokhtar Haouari that concluded in New York last week.

The department is a key member of the Canada-U.S. bilateral consultative group on counterterrorism. This is the primary Canada-U.S. forum for discussion of counterterrorism issues. It brings together departments and agencies from both governments to enhance counterterrorism collaboration, cooperation and information sharing.

The Department of the Solicitor General and the U.S. Department of Defense co-manage the Canada-U.S. bilateral agreement on counterterrorism research and development. Its shared objective is to develop new or adapt old technology to counterterrorism threats. The department has a lead in organizing the Canada-U.S. counterterrorism tabletop exercises.

The last such exercise was in February, 2000 and was the subject of a briefing to both the Solicitor General and the then Attorney General of the U.S., Janet Reno. Another exercise is planned for February 2002.

The Department of the Solicitor General and the U.S. Justice Department co-chair the Canada-U.S. cross-border crime forum. While the focus of this forum is on transnational crime, it also touches on emerging cross-border security issues. The recent crime forum meeting in June was attended by John Ashcroft, the new Attorney General of the United States, who said, at that time, that the Canada-U.S. relationship was a model for cooperation.

One of the fundamental principles of Canadian national security policy is that domestic security and global security are interdependent. To that end, the Department of the Solicitor General works in a range of international fora, usually in support of the Department of Foreign Affairs and International Trade to develop comprehensive global responses to security issues such as terrorism. This includes the G8, the UN and the Organization of American States, among others. In the case of the UN, Canada is a signatory to all 12 UN conventions on terrorism and has ratified 10 of them. The conventions and other agreements, to which Canada is a signatory, set standards for preventing or responding to terrorist activities.

traiter avec une vaste gamme d'entreprises et, partant, avec un ensemble d'infrastructures de réseaux plus diversifiées. Les autorités doivent maintenir leurs capacités d'accéder légalement aux données et aux communications dont elles ont besoin pour s'acquitter du mandat confié à elles par le Parlement.

Le ministère continue de travailler ou directement ou à l'appui des Affaires étrangères en vue de renforcer la collaboration et la coordination en matière de sécurité avec les États-Unis. L'enquête et le procès mettant en cause Ahmed Ressam ont montré que nous entretenons de très solides relations de travail effectives tant au niveau gouvernement à gouvernement qu'au niveau opérationnel. Ce même niveau de collaboration a été manifeste dans le procès de Mokhtar Haouari, procès qui a pris fin à New York la semaine dernière.

Le ministère est un membre clé du groupe bilatéral consultatif canado-américain sur l'antiterrorisme. Il s'agit là du principal forum canado-américain de discussion de questions portant sur l'antiterrorisme. Il réunit des ministères et des organismes des deux gouvernements, ce dans le but de favoriser la collaboration, la coopération et le partage d'information en matière de lutte contre le terrorisme.

Le ministère du Solliciteur général et le U.S. Department of Defense administrent conjointement l'entente bilatérale entre le Canada et les États-Unis sur la recherche et le développement en matière de lutte contre le terrorisme. Leur objet commun est d'élaborer de nouvelles technologies de lutte contre les menaces terroristes ou d'en adapter d'anciennes. Le ministère joue un rôle de premier plan dans l'organisation de simulations canado-américaines d'exercices antiterrorisme sur maquette.

Le denier exercice du genre a été mené en février 2000 et a fait l'objet d'un breffage devant et le solliciteur général et l'Attorney General américain d'alors, Janet Reno. Un autre exercice du genre est prévu pour février 2002.

Le ministère du Solliciteur général et le Justice Department américain coprésident le Forum canado-américain sur la criminalité transfrontalière. Bien que ce forum porte principalement sur le crime transnational, il aborde également les problèmes émergents en matière de sécurité transfrontalière. A assisté à la récente réunion du forum sur la criminalité, tenue en juin, John Ashcroft, le nouvel Attorney General américain, qui a déclaré à l'époque que la relation canado-américaine était un modèle de coopération.

L'un des principes fondamentaux de la politique nationale du Canada en matière de sécurité est que la sécurité nationale et la sécurité mondiale sont interdépendantes. Dans ce contexte, le ministère du Solliciteur général est actif dans une vaste gamme de tribunes internationales, en règle générale à l'appui du ministère des Affaires étrangères et du Commerce international, en vue de l'élaboration d'interventions mondiales globales face aux problèmes de sécurité comme le terrorisme. Je citerai à titre d'exemple le G8, les Nations Unies et l'Organisation des États américains. Dans le cas des Nations Unies, le Canada est signataire des 12 conventions des Nations Unies sur le terrorisme et il en ratifié dix. Les conventions et autres ententes dont le Canada est signataire fixent les normes en vue de la prévention d'activités terroristes ou de la lutte contre celles-ci.

The department also provides a Canadian chair for the Canada-U.S.-United Kingdom trilateral group on chemical biological terrorism. The main objective of this group is to coordinate efforts and exchange information to counter chemical and biological terrorism. Again, in support of foreign affairs, we have also participated in bilateral discussions to address security issues.

In response to the January 1999 Report of the Special Senate Committee on Security and Intelligence, the government made a commitment to develop options for a strategy to strengthen national counterterrorism response capability, particularly the capability to respond to the threat of chemical, biological, radiological and nuclear terrorism. This is a particularly complex and demanding area because a chemical or biological terrorist incident would demand a multi-jurisdictional and multi-agency response.

The provinces are key partners in this initiative, given their primary responsibility for first responders and consequence management. To ensure that their views are represented in the development of a national strategy, we will be conducting consultations with them this fall.

Bill C-16 in respect of the registration of charities and security information and the Income Tax Act would be an important tool in Canada's fight against terrorism. It is intended to stop those front organizations that have obtained charitable status in Canada from providing tax receipts for money that is intended by the donor to go to a charitable cause but which ultimately supports terrorist activity. This bill will maintain the integrity of the charitable registration system as well as maintain Canada's international commitment to stop the flow of funds that supports terrorist activity. The bill is currently before the Commons Finance Committee.

The drive towards worldwide knowledge-based economies has accelerated the development of sophisticated information and communication technologies. Technology is a tool for those who enforce laws, but it is also a weapon for those who may wish to undermine our security. With the growing challenges to lawful access, we need to work even harder to keep pace with new technologies. The Lawful Access Division is coordinating the work of the portfolio in this area and both CSIS and the RCMP have dedicated resources to develop technical solutions. These solutions will be shared with police services.

In addition, a sound, legal framework must be in place. The government needs to review current laws to ensure that they address new technologies.

For the immediate future, the Canada-U.S. security relationship and Canada's work in international fora will continue to be both a challenge and a priority for the government and the Department of the Solicitor General. In the case of the Canada-U.S. security

Le ministère désigne également un président canadien pour le Groupe trilatéral Canada-États-Unis-Royaume-Uni sur le terrorisme chimique et biologique. Le principal objet de ce groupe est de coordonner des efforts et d'échanger des renseignements en vue de contrer le terrorisme chimique et biologique. Toujours à l'appui des Affaires étrangères, nous avons également participé à des discussions bilatérales portant sur des questions de sécurité.

En réponse au rapport de janvier 1999 du Comité sénatorial spécial sur la sécurité et les services de renseignement, le gouvernement s'est engagé à élaborer des options en vue d'une stratégie destinée à renforcer la capacité d'intervention nationale face au terrorisme, et tout particulièrement au terrorisme chimique, biologique, radiologique et nucléaire. Il s'agit là d'un domaine particulièrement complexe et exigeant car un incident terroriste chimique ou biologique exigerait une action multijuridictionnelle et multiorganismes.

Les provinces sont des partenaires clés dans cette initiative, étant donné leur responsabilité de premiers agents d'intervention et de gestion des conséquences. Afin de veiller à ce que leurs opinions soient représentées dans le cadre de l'élaboration d'une stratégie nationale, nous allons mener des consultations auprès d'elles cet automne.

Le projet de loi C-16 portant sur l'enregistrement des organismes de bienfaisance, les renseignements de sécurité et la Loi de l'impôt sur le revenu est un outil important dans la lutte menée contre le terrorisme par le Canada. Il a pour objet d'empêcher les organismes de façade qui ont obtenu le statut d'organisme de bienfaisance au Canada de fournir des reçus d'impôt pour des fonds dont le donateur pensait qu'ils allaient servir une cause charitable mais qui viendront en définitive appuyer des activités terroristes. Le projet de loi maintiendra l'intégrité du système d'enregistrement des organismes de bienfaisance ainsi que l'engagement international du Canada à stopper les flux d'argent à l'appui d'activités terroristes. Le Comité des finances de la Chambre des communes est en train d'examiner le projet de loi.

La poussée vers des économies mondiales fondées sur le savoir a accéléré l'émergence de technologies sophistiquées d'information et de communications. La technologie est un outil pour ceux qui appliquent la loi mais elle est également une arme pour ceux désireux de miner notre sécurité. Face à la multiplication des obstacles à l'accès légal, il nous faut travailler encore plus fort pour suivre le rythme de l'émergence de nouvelles technologies. La Division de l'accès légal coordonne le travail du portefeuille dans ce domaine et le SCRS et la GRC ont tous deux des ressources réservées à la mise au point de solutions techniques. Ces solutions seront partagées avec les services de police.

Il importe par ailleurs d'avoir en place un solide cadre juridique. Le gouvernement doit par conséquent réexaminer les lois en vigueur pour veiller à ce qu'elles englobent les nouvelles technologies.

Quant à l'avenir immédiat, la relation de sécurité canado-américaine et le travail effectué par le Canada dans le cadre de tribunes internationales continueront d'être et un défi et une priorité pour le gouvernement et pour le ministère du Solliciteur

partnership, we already have extensive arrangements in place, both at the government-to-government and the operational levels. However, we will continue to work with our U.S. counterparts on a priority basis to enhance national security on both sides of the border.

As I mentioned earlier in my remarks, domestic security and global security are interdependent. With that in mind, the department will need to continue to work in bilateral and multilateral fora to develop a concerted approach to terrorism and other national security threats. This too will remain a priority.

This concludes my formal remarks. I would be happy to answer any questions the committee may have.

Senator Forrestall: You will appreciate that we are a little reluctant because of our lay background and the distance between your daily world and ours. Frankly, it scares us. Nevertheless, we appreciate your being here and, even more so, your role in our society. It is comforting to know that people are doing things that we do not really have to know all about.

You indicated that we had ratified only 10 of the 12 UN conventions. Which two remain? Could you give us an explanation of the conventions, briefly, with particular emphasis on the two that we have not signed and the reasons for that?

Mr. D'Avignon: The 10 that have been signed deal with a range of issues that include airplane hijackings. I do not have the list in front of me to give you the full explanation of the 10 that have been signed, but the two that we have not ratified deal with terrorist bombing and the suppression of terrorist financing. Suppression of terrorist financing was signed in February 2000, and terrorist bombing was signed a little sooner than that. Those are the two that have not been ratified, as yet.

The suppression of terrorist financing would involve, in all likelihood, modifications to legislation, possibly including the Criminal Code. The lead on the work with respect to that is with the Department of Justice.

Senator Forrestall: The reason I would presume that we have not ratified them is house time and the priority of other matters to be dealt with to let the debate proceed in its normal way.

Mr. D'Avignon: Exactly, and to examine in detail the implications and requirements that need to be met in order to be able to do so.

Senator Forrestall: I was not aware of that. I thought we had ratified pretty much as these events arose.

général. Dans le cas du partenariat de sécurité canado-américain, nous avons déjà en place des arrangements exhaustifs tant au niveau gouvernement à gouvernement qu'au niveau opérationnel. Nous continuerons cependant d'oeuvrer de façon prioritaire avec nos homologues américains en vue d'améliorer la sécurité nationale des deux côtés de la frontière.

Comme je l'ai mentionné plus tôt dans mes remarques, la sécurité nationale et la sécurité mondiale sont interdépendantes. Cela étant, le ministère devra continuer, dans le cadre de tribunes bilatérales et multilatérales, d'oeuvrer à l'élaboration d'une approche concertée face au terrorisme et aux autres menaces à la sécurité nationale. Cela aussi devra demeurer une priorité.

Voilà qui met fin à mes remarques liminaires. Je me ferai un plaisir de répondre à toutes les questions que voudront me poser les membres du comité.

Le sénateur Forrestall: Vous comprendrez que nous avons quelques hésitations du fait de nos antécédents de profanes et de l'écart qu'il y a entre votre monde quotidien et le nôtre. Bien franchement, cela nous fait peur. Quoi qu'il en soit, nous vous sommes reconnaissants de votre présence ici et, plus encore, du rôle que vous jouez dans notre société. Il est rassurant de savoir qu'il y a des gens qui font des choses dont nous ne devons pas forcément absolument tout savoir.

Vous avez indiqué que nous n'avons ratifié que dix des 12 conventions des Nations Unies. Quelles sont ces deux conventions restantes? Pourriez-vous nous expliquer brièvement ces conventions, en vous attardant tout particulièrement sur les deux que nous n'avons pas signées, en précisant pourquoi c'est le cas?

M. D'Avignon: Les dix qui ont été signées traitent de toute une gamme de questions, dont les détournements d'avion. Vu que je n'ai pas la liste devant les yeux, je ne peux pas vous donner une explication exhaustive quant aux dix conventions qui ont été signées, mais les deux que nous n'avons pas ratifiées traitent des attentats à la bombe terroristes et de la suppression du financement du terrorisme. La convention sur la suppression du financement de terrorisme a été signée en février 2000, et celle portant sur les attentats à la bombe a été signée un peu avant. Voilà quelles sont les deux qui n'ont pas encore été ratifiées.

La convention visant la suppression du financement du terrorisme exigerait vraisemblablement des modifications législatives y compris, peut-être, au Code criminel. C'est le ministère de la Justice qui est le premier responsable de ce dossier.

Le sénateur Forrestall: Je présume que si nous ne les avons pas ratifiées c'est à cause du calendrier des travaux à la Chambre et de la priorité accordée à d'autres questions devant être réglées afin que le débat se poursuive selon la façon habituelle.

M. D'Avignon: Précisément, ainsi que de façon à être en mesure d'examiner dans le détail les ramifications et les exigences que cela supposerait.

Le sénateur Forrestall: Je n'étais pas au courant de cela. Je pensais que nous avions plus ou moins ratifié ces choses au fil des événements.

Can you given us some information in respect of security in the air. The various forms, looks and faces of terrorism are interesting. In your assessment, what is the primary threat to us as we head into the new millennium?

Mr. D'Avignon: If you look at the issue in global terms, the primary threat is the changing nature of the phenomenon itself and how that nature and new technology allow terrorists to develop a versatility that challenges the forces of order. That ever-changing reality forces us to be constantly vigilant, to be fleet of foot, to keep abreast of how the threats are changing, how methods are changing, and how new developments, particularly in technology, help not only us but also help terrorists to accomplish their ends.

Senator Meighen: As Senator Forrestall said, this is a daunting area for amateurs. What concerns me as an ordinary citizen is whether we have the organizational coherence in Canada to deal with known threats and whether we have the tools to do the job without, of course, compromising human rights.

In terms of organizational coherence, the analysis and investigation of these matters is split between the RCMP and CSIS. We also have OCIPEP, the Office of Critical Infrastructure Protection and Emergency Preparedness, which, I am told, answers to the Department of National Defence. I am not necessarily being critical. I am just wondering whether the right hand knows what the left hand is doing all the time, without even mentioning what collaboration and cooperation arrangements you have entered into with provincial departments of the Solicitor General or Attorney General or whoever it might be. Is everyone tripping over everyone else? Or are you satisfied, Mr. D'Avignon, that you have a seamless organization that can react quickly and coherently anywhere in the country to a terrorist threat?

Mr. D'Avignon: I would say, yes, I am satisfied. There are a number of things in place that allow us to be agile and flexible in dealing with our universe. Committees exist to bring people together on a regular basis so that information is exchanged and people know where other people stand. The national counterterrorism plan, to which I alluded earlier in my remarks, is the key document that lays out the structure and the functioning of the government's response in the event of an incident occurring.

I mentioned earlier as well that we are engaged in discussions with OCIPEP to ensure that we have a good understanding of areas where we could partner. They are developing their mandate from the beginning and sorting out their new universe. Some of that is an old universe because Emergency Preparedness has been around for a long time. We have had relationships with them for a number of years. We are dealing now with a new component of Critical Infrastructure Protection. We are in the process of working with them to provide greater definition and ensure that we have a good symbiotic relationship.

Pourriez-vous nous renseigner au sujet de la sécurité dans les airs. Les différents visages, formes et images du terrorisme sont intéressants. Quelle est selon vous la principale menace à laquelle nous sommes exposés en ce début du nouveau millénaire?

M. D'Avignon: Si vous envisagez la question dans un contexte mondial, la principale menace est la nature changeante du phénomène lui-même et la façon dont cette nature et la nouvelle technologie offrent aux terroristes des possibilités d'adaptation qui constituent un réel défi pour les forces de l'ordre. Cette réalité sans cesse changeante nous impose d'être en tout temps vigilants et prompts à réagir, et toujours au courant de l'évolution des menaces et des méthodes et de la façon dont les nouveaux développements, dans le domaine de la technologie, surtout, non seulement nous aident nous, mais aident également les terroristes à réaliser leurs fins.

Le sénateur Meighen: Comme l'a dit le sénateur Forrestall, il s'agit ici d'un domaine intimidant pour nous autres amateurs. Ce qui me préoccupe en tant que simple citoyen est la question de savoir si nous avons au Canada la cohésion organisationnelle requise pour repousser les menaces connues et si nous disposons des outils nécessaires pour faire le travail, sans, bien sûr, compromettre les droits de la personne.

Pour ce qui est de la cohésion organisationnelle, le travail d'analyse et d'enquête est partagé entre la GRC et le SCRS. Il y a également le BPIEPC, Bureau de la protection des infrastructures essentielles et de la protection civile qui, me dit-on, relève du ministère de la Défense nationale. Mon but n'est pas forcément d'être critique. Je me demande tout simplement si la main droite sait en tout temps ce que fait la main gauche, sans même parler des arrangements de collaboration et de coopération que vous avez établis avec les ministères provinciaux du Solliciteur général ou du Procureur général ou autre. Est-ce que chacun est en train de trébucher sur l'autre ou bien êtes-vous convaincu, M. D'Avignon, d'avoir une organisation sans coutures capable de réagir rapidement et de façon cohérente face à une menace terroriste n'importe où au pays?

M. D'Avignon: Je dirais que oui, j'en suis convaincu. Il y a en place plusieurs choses qui nous permettent d'être agiles et flexibles face à notre univers. Il existe des comités qui ont pour objet de réunir des gens de façon régulière dans le but d'échanger des renseignements et d'expliquer où l'on en est. Le plan national de lutte contre le terrorisme, que j'ai évoqué tout à l'heure dans mes remarques liminaires, est le document clé établissant la structure et le fonctionnement de la réaction du gouvernement en cas d'incident.

J'ai également mentionné tout à l'heure que nous sommes engagés dans des discussions avec le BPIEPC dans le but de bien comprendre les domaines dans lesquels nous pourrions être partenaires avec d'autres. Ce bureau est en train d'élaborer son mandat et de faire le tri de son nouvel univers. L'ancien univers fait partie de l'ensemble, car la Protection civile existe depuis longtemps. Nous entretenons des relations avec ce groupe depuis plusieurs années. Nous traitons aujourd'hui avec une nouvelle composante, celle de la protection des infrastructures essentielles. Nous oeuvrons aujourd'hui à ses côtés en vue de mieux cerner les

The provinces have responsibilities as first responders in any event, be it a terrorist event or a hazardous-material incident. They can then engage Emergency Preparedness. Because of the provinces' primary roles, we maintain good contacts with them. We are engaged in a very extensive consultation process on the counterterrorism plan to ensure that they are in the fold, as it were. The Security Offences Act provides for police-to-police arrangements between RCMP and local police forces. All of the provinces, with the exception of Quebec, have arrangements. Discussions have started with Ontario and B.C. to examine the arrangements with those two provinces. There is a need to look at these again.

A whole structure is in place. It is a bit like an iceberg, with most of the structure under the water, but it is there and is functioning well. There is a reasonably good sense of how the various roles interact. We engage in exercises that bring the players together. That is one of our responsibilities under the operational readiness program. We propose a scenario and then work through the decisions on how the various agencies and departments would interact in response to the incident and how the information and policy advice would flow to the decision makers.

Senator Meighen: That is very encouraging. Can I conclude then — and I have no information to the contrary — that the incidents reported in the press recently and to which you have alluded in your presentation did not bring to light any major breakdown in communication between our various agencies?

Mr. D'Avignon: That is a fair statement. The response was not perfect. However, in this business, though we strive for perfection, I doubt we will ever attain it. There will always be some weird wrinkle that will catch us out. Things did work reasonably well and people were generally satisfied.

In keeping with the philosophy or the approach usually taken in this business, we are constantly assessing events to see what we did well and what we did less well. A process is underway at this time to decide what improvements we can make after our experience with the Ressam incident. Some departments have already made changes, and some of the more glaring errors that needed attention are already receiving attention. The nature of the work forces us to be in a continual improvement mode. We cannot afford not to learn from every incident to which we are exposed.

Senator Meighen: This may not be under your jurisdiction, but I would be interested in knowing what liaison exists. Before the fact, when a terrorist is coming to Canada, there have been

Les provinces ont des responsabilités en tant que premiers intervenants quel que soit l'événement concerné, qu'il s'agisse d'un incident terroriste ou d'un incident mettant en cause des matières dangereuses. Elles peuvent alors enclencher la Planification d'urgence. Étant donné le rôle de premier plan des provinces, nous maintenons avec elles de bonnes relations. Nous sommes engagés dans un processus de consultations très exhaustif portant sur le plan de lutte contre le terrorisme, ce afin de veiller à ce que les provinces soient pleinement intégrées, si vous voulez. La Loi sur les infractions en matière de sécurité prévoit des arrangements de force policière à force policière entre la GRC et les services de police locaux. Toutes les provinces à l'exception du Québec ont de tels arrangements. Des discussions ont été entreprises avec l'Ontario et la Colombie-Britannique en vue de l'examen des arrangements intéressant ces deux provinces. Il importe de les revoir.

Toute une structure est en place. C'est un petit peu comme un iceberg, le gros de la structure étant sous l'eau, mais elle est là et elle fonctionne bien. Il y a une assez bonne compréhension des interactions entre les différents rôles. Nous lançons des exercices pour rassembler les joueurs. C'est là l'une des responsabilités qui nous reviennent en vertu du programme de préparation opérationnelle. Nous proposons un scénario puis nous passons en revue les décisions quant à la manière dont les différents ministères et organismes réagiraient face à l'incident et quant à la façon dont les renseignements et les conseils politiques seraient communiqués aux décisionnaires.

Le sénateur Meighen: Cela est très encourageant. Puis-je en conclure — et je ne dispose d'aucun renseignement indiquant le contraire — que les incidents récemment rapportés dans la presse et que vous avez évoqués dans votre exposé ne témoignent d'aucune rupture de communications d'importance entre les divers organismes responsables?

M. D'Avignon: Ce que vous dites est juste. La réaction n'a pas été parfaite. Cependant, dans ce domaine, bien que nous visions la perfection, je doute qu'on y parvienne jamais. Il y aura toujours quelque part une aspérité qui nous accrochera. Les choses se sont néanmoins plutôt bien terminées et les gens étaient dans l'ensemble satisfaits.

Conformément à la philosophie ou à l'approche habituellement suivie dans notre domaine, nous évaluons constamment les événements pour déterminer ce que nous avons bien fait et ce que nous avons moins bien fait. Un processus est en cours à l'heure actuelle en vue de décider quelles améliorations nous pourrions apporter suite à l'expérience vécue dans le cadre de l'affaire Ressam. Certains ministères ont déjà apporté des changements et plusieurs des erreurs les plus flagrantes qui méritaient qu'on s'y penche sont déjà en train d'être examinées. La nature même du travail nous oblige à fonctionner dans un mode d'amélioration continue. Nous ne pouvons pas nous permettre de ne pas tirer des leçons de chaque incident auquel nous sommes exposés.

Le sénateur Meighen: Ceci n'est peut-être pas de votre ressort, mais cela m'intéresserait de savoir quelle liaison existe. Sans parler de cas précis de terroristes venant au Canada, il y a eu des

accusations in the press, raised both in Canada and elsewhere, that we are a haven for terrorists and that we are the gateway to the United States. Do you have any reassurance or any comment on that criticism? Is it a false criticism? Do you work closely with the Department of Citizenship and Immigration in examining these areas? I am wondering whether something can be done, if it needs to be done, to tighten up our security regarding this issue.

Mr. D'Avignon: There are a number of elements that connect with this. Yes, the primary responsibility is with the Department of Citizenship and Immigration. They have programs in place and work closely with the Canadian Security Intelligence Service in watching the borders and in identifying people who may want to come to Canada, or who do come to Canada, about whom we would have concerns. Citizenship and Immigration also work closely with the RCMP in instances where more direct action, if you will, is required, whether an arrest for purposes of deportation or whatever. Again, I would say that the system is not perfect, but it has a series of elements in it that work reasonably well that we could certainly improve. In fact, there is a bill before the House of Commons, Bill C-11, that proposes to bring more rigor, I believe, to the process that Citizenship and Immigration are responsible for and to deal with some of these concerns.

Senator Meighen: I would hope that in committee you might be called upon to support the bill, if you could or if you wish, to give evidence as to why it is necessary. I am old enough to remember that the killer of Martin Luther King used a Canadian passport to travel around Europe. It took that incident for Canada to come to the realization that passports should not be handed out like lottery tickets, that an individual must go through some process to get a passport. Canada has always bent over backwards to make sure that our protection measures were not ones that infringed upon human rights. It is a difficult balance, and I appreciate that; however, we must monitor the situation carefully, as you have said, to make sure we have the right combination.

Mr. D'Avignon: Yes. In fact, in the context of Ressam, the passport office now has a new automated system that allows them to improve their information exchanges and to verify with other federal government departments whether, for one reason or another, there is concern with a particular applicant. That is an instance where, in reaction to the Ressam incident, action is already being initiated to take us down that road.

Senator Atkins: I am not sure that my questions fall directly under your jurisdiction but I will ask them anyway.

In the wisdom of this government, they decided to eliminate the port police. What measures has the government taken to compensate for the dismissal of port police?

Mr. D'Avignon: Unfortunately, that is totally out of my area of competence. I am aware of the decision but I truly know nothing of that particular issue.

accusations dans la presse, tant au Canada qu'ailleurs, selon lesquelles notre pays serait un refuge pour terroristes et une porte d'accès aux États-Unis. Pourriez-vous nous fournir quelque assurance ou commentaire en réaction à cette accusation? Est-ce une fausse accusation? Travaillez-vous étroitement avec le ministère de la Citoyenneté et de l'Immigration à cet égard? Je me demande s'il n'y aurait pas moyen de faire quelque chose, s'il y a lieu, pour resserrer la sécurité sur ce plan.

M. D'Avignon: Il y a plusieurs éléments qui interviennent ici. Oui, la première responsabilité revient au ministère de la Citoyenneté et de l'Immigration. Celui-ci a des programmes en place et travaille étroitement avec le Service canadien du renseignement de sécurité dans la surveillance des frontières et l'identification de personnes désireuses de venir au Canada ou présentes sur notre territoire et au sujet desquelles nous nous posons certaines questions. Citoyenneté et Immigration travaille par ailleurs étroitement avec la GRC sur les cas qui exigent une action plus directe, si vous voulez, qu'il s'agisse d'une arrestation aux fins d'expulsion ou autre. Encore une fois, je dirais que le système n'est pas parfait mais qu'il comporte une série d'éléments qui fonctionnent relativement bien mais que nous pourrions certainement améliorer. Il y a en fait un projet de loi dont est saisi la Chambre des communes, le projet de loi C-11, qui a, je pense, pour objet d'apporter davantage de rigueur au processus dont est responsable Citoyenneté et Immigration et de traiter de certains de ces problèmes.

Le sénateur Meighen: J'ose espérer qu'on pourra faire appel à vous en comité pour appuyer le projet de loi, si vous le pouviez ou si vous le vouliez, en expliquant pourquoi il est nécessaire. Je suis suffisamment vieux pour me rappeler que le tueur de Martin Luther King avait utilisé un passeport canadien pour parcourir l'Europe. Il a fallu cet incident pour que le Canada se rende compte que les passeports ne devraient pas être distribués comme des billets de loterie et que tout demandeur de passeport doit suivre un certain processus. Le Canada s'est toujours fendu en quatre pour veiller à ce que nos mesures de protection n'empiètent pas sur les droits de la personne. C'est un équilibre qui est difficile à réaliser, je m'en rends compte. Il nous faut néanmoins surveiller de très près la situation, comme vous l'avez dit, afin d'être bien certain d'avoir la bonne combinaison.

M. D'Avignon: Oui. En fait, dans le contexte de l'affaire Ressam, le bureau des passeports s'est doté d'un nouveau système automatisé qui lui permet d'améliorer les échanges d'informations et de vérifier auprès d'autres ministères fédéraux si un demandeur pose des problèmes pour une raison ou une autre. Voilà donc un exemple de ce genre de situation: suite à l'affaire Ressam, des mesures ont déjà été prises pour nous faire avancer sur cette voie.

Le sénateur Atkins: Je ne suis pas certain que mes questions portent sur des aspects qui sont de votre compétence, mais je vais vous les poser quand même.

L'actuel gouvernement a, dans sa sagesse, décidé d'éliminer la police portuaire. Quelles mesures le gouvernement a-t-il prises pour compenser le renvoi de la police portuaire?

M. D'Avignon: Malheureusement, cela n'est pas du tout de mon ressort. Je suis au courant de la décision, mais je ne suis pas du tout au courant de ce dossier particulier.

Senator Atkins: Under your position, do you not see a certain vulnerability of the country through the admission of people who can come through our ports, including terrorists?

Mr. D'Avignon: I would not know how to respond to you because that is one issue that I know very little about. I would need to make some assumptions by saying that Transport Canada, in making whatever alternate arrangements they have made, would have taken into consideration the importance of security and of controlling, to the extent that they have a responsibility for doing so, access and verifying movement of people.

I must also assume that in doing that they would make sure that they had arrangements in place, either with police of local jurisdiction or with the RCMP, to ensure that in the event there was a requirement for assistance that the police and the RCMP were in a position to be able to assist.

I am speaking here just on the basis of supposition. Truly, I do not know anything about that particular area. If you wish, we could look into it and provide you with some additional information.

Senator Atkins: One of the reasons I raise it is because of issues of concern to the Canada-U.S. Parliamentary Association, of which I am a member. That association meets on an annual basis. The American politicians, senators and congressmen leave the impression that we are vulnerable through our ports and that they are vulnerable as a result of that. That is the reason. Then they get into this whole question of drugs. We had a meeting in May and I can tell you that one thing they were very concerned about is the examination that is underway on this whole question of the use of marijuana. Apart from energy, they spent more time on that than anything.

Mr. D'Avignon: I mentioned in my remarks the cross-border crime forum. I know that, in the context of that forum, some of these issues get discussed with a view to finding practical solutions to a number of these issues. I am not speaking specifically of port police, but the kinds of concerns about drug flow and so on. The Canada Customs and Revenue Agency also speaks with their American counterparts and maintains close contacts with them. At the operational level, at the working level, there are a number of measures that are in place and discussions to keep that information flowing and to mutually reinforce one another. The RCMP have IBETs — integrated border enforcement teams — that work with the American border patrol in specific areas of the country to focus on problems, whether it is drug smuggling or whatever might occur along the border.

There are a number of measures in place that involve both the Americans and us that are cooperative both in terms of the sharing of information and of taking enforcement action.

Senator Atkins: I should make the point that the Americans were cooperative in terms of the security matters. I am not being critical of this.

Le sénateur Atkins: Dans le contexte de vos fonctions, ne considérez-vous pas que le pays est rendu quelque peu vulnérable du fait de l'admission de personnes, dont des terroristes, à nos ports?

M. D'Avignon: Je ne sais trop quoi vous répondre car il s'agit d'une question dont je ne sais que peu de choses. Il me faudrait m'appuyer sur certaines hypothèses disant que Transports Canada, dans les arrangements de rechange qu'il a mis en place, a dû tenir compte de l'importance de la sécurité et du contrôle, dans la mesure où il a une responsabilité à cet égard, de l'accès des gens et de la vérification de leurs mouvements.

Il me faudrait également supposer que, ce faisant, il veillerait à mettre en place des dispositions, ou avec la police locale ou avec la GRC, afin d'être certain qu'en cas de besoin la police et la GRC soient en mesure de prêter main forte.

Ce que je vous dis là ne s'appuie que sur des hypothèses. Je ne sais en vérité rien de cette question particulière. Si vous voulez, nous pourrions nous renseigner et vous fournir des précisions supplémentaires.

Le sénateur Atkins: L'une des raisons pour lesquelles je vous en parle est que cette question figure parmi les sujets de préoccupation de l'Association parlementaire Canada-États-Unis, dont je suis membre. Cette association se réunit chaque année. Les politiciens, sénateurs et membres du Congrès américain ont l'impression que nous sommes vulnérables à cause de nos ports et qu'ils le sont par contrecoup. Voilà pourquoi je vous interroge là-dessus. Ils parlent également de toute la question des stupéfiants. Nous avons eu une réunion en mai et je peux vous dire qu'un sujet qui les préoccupe beaucoup est l'examen de toute la question de l'utilisation de marijuana qui est en cours. Exception faite de la question de l'énergie, les politiques américains consacrent plus de temps à cette question qu'à n'importe quelle autre.

M. D'Avignon: J'ai mentionné dans mes remarques le forum sur la criminalité transfrontalière. Je sais que dans le contexte de ce forum certaines de ces questions ont été examinées dans le but de trouver des solutions pratiques à plusieurs aspects. Je ne veux pas parler de la police portuaire en particulier, mais de questions comme les mouvements de drogue, etc. L'Agence des douanes et du revenu du Canada traite également avec son équivalent américain avec lequel elle entretient d'étroites relations. Au niveau opérationnel, au niveau travail, il y a plusieurs mesures qui sont en place ainsi qu'un dialogue permanent destiné à favoriser l'échange d'information et le soutien réciproque. La GRC a des équipes de contrôle intégrées à la frontière qui travaillent avec la patrouille frontalière américaine à certains endroits du pays pour traiter des problèmes qui y existent, qu'il s'agisse de trafic de stupéfiants ou d'autres activités le long de la frontière.

Il y a en place diverses mesures auxquelles les Américains et nous autres collaborons tant sur le plan du partage de renseignements que sur celui de la prise de mesures coercitives.

Le sénateur Atkins: Il me faut souligner que les Américains ont été très coopératifs pour ce qui est des questions de sécurité. Je ne leur adresse aucune critique à cet égard.

The final question I have for the moment is the following: Can you explain the statement that "terrorism runs on fundraising?"

Mr. D'Avignon: Yes. One of the realities of terrorism is how terrorist groups are organized to collect fund and to channel those funds to their causes. We are faced with reality that that is done through a number of vehicles. In countries where there are sizeable expatriate populations that come from countries where there are terrorist concerns operating, organizations that are front companies profess to have humanitarian ends and collect funds in other countries and then take those funds and divert them. It depends on how those companies are structured but a part of that money goes toward supporting terrorist actions, whether it is the procurement of weapons, allowing people to travel and so on. A range of support activities goes into ensuring that terrorist action on the ground occurs.

As in any other reality that we are faced with, money makes it go. Fundraising is one of the ways that terrorist groups are able to secure funds sometimes putting a very benign face on it. Other times, it is through more crass methods, such as levying taxes within ethnic communities, for example. It runs the gamut from very sophisticated through to more criminal, almost, activities. That source of funds is what allows them to operate in whatever area of the world that they are operating in to pursue their political ends.

Senator Atkins: Does this kind of fundraising reach down right into the grassroots, or is it more sophisticated?

Mr. D'Avignon: It is both. Some of it is very sophisticated and some of it is shaking people down on street corners.

Senator Atkins: How does the public know? How can they protect themselves from this?

Mr. D'Avignon: Again, in looking at this, you must think of expatriate communities of people who come from countries where they do not necessarily trust the forces of order. They view the police with fear and concern. They come to a new country to escape some of these realities. Unfortunately, these homeland conflicts follow with them in many cases. They tend to be a little more isolated from the mainstream and in the beginning do not quite understand how the culture functions, what kind of trust they can put in the police forces or the forces of order that exist. Essentially, they become victimized. This can go on for a period of time before they either decide that they will stop doing this and turn to the police forces to protect them or they continue to be victimized for a period of time.

Senator Atkins: Are we talking about big dollars?

Mr. D'Avignon: We are talking sizeable amounts of money, yes.

La dernière question que j'ai à vous poser pour l'instant est la suivante: Pouvez-vous nous expliquer l'expression «le terrorisme est alimenté par la collecte de fonds»?

M. D'Avignon: Oui. L'une des réalités du terrorisme est la façon dont les groupes terroristes sont organisés pour collecter des fonds et diriger ces fonds vers leurs causes. La réalité à laquelle nous nous trouvons confrontés est que cela est fait grâce à différents véhicules. Dans les pays qui comptent d'importants groupes d'expatriés originaires de pays dans lesquels fonctionnent des groupes terroristes, des organismes qui leur servent de façade se déclarent comme étant des organismes d'intervention humanitaire et ramassent des fonds dans d'autres pays pour ensuite les détourner. Tout dépend de la façon dont ces sociétés sont structurées, mais une partie de l'argent ramassé sert à appuyer des actions terroristes, qu'il s'agisse de l'achat d'armes, du financement de déplacements ou autres. Toute une gamme d'activités de soutien entrent en jeu pour veiller à ce que l'action terroriste se fasse sur le terrain.

Comme c'est le cas de toute autre réalité à laquelle l'on peut se trouver confronté, l'argent est le nerf de la guerre. La collecte de fonds est un des moyens qui permettent aux groupes terroristes d'obtenir des fonds en arborant un visage bénin. D'autres fois, ces groupes recourent à des méthodes plus sales, par exemple en percevant des impôts auprès de communautés ethniques. Cela couvre toute la gamme, allant de mesures très sophistiquées à des activités quasi riminelles. Ce sont ces sources de fonds qui leur permettent de mener leurs activités au service de leurs fins politiques où que ce soit dans le monde.

Le sénateur Atkins: Ces genres d'activités de collecte de fonds descendent-elles jusqu'à la base ou bien est-ce plus sophistiqué?

M. D'Avignon: Les deux. Certaines de ces activités sont très sophistiquées, mais dans d'autres cas, il s'agira d'intimider les gens au coin de la rue.

Le sénateur Atkins: Comment le public le sait-il? Comment les gens peuvent-ils se protéger contre ce genre de choses?

M. D'Avignon: Encore une fois, dans ce contexte particulier, il faut savoir qu'il s'agit de communautés d'expatriés originaires de pays où les gens ne font pas nécessairement confiance aux forces de l'ordre. Ces gens sont craintifs et méfiants face aux forces de police. Ils arrivent dans un nouveau pays pour échapper à certaines de ces réalités. Malheureusement, dans bien des cas, les conflits qui déchiraient leur pays les suivent. Ils ont tendance à s'isoler des courants généraux et, au début, ils ne comprennent pas très bien comment fonctionne la culture, quelle confiance ils peuvent faire aux forces policières ou aux forces de l'ordre qui existent. En gros, ces personnes deviennent victimes. Ces situations peuvent durer un certain temps avant que la personne décide qu'elle veut y mettre fin et demande la protection de la police ou alors continue pendant quelques temps encore de se faire avoir.

Le sénateur Atkins: S'agit-il de gros sous?

M. D'Avignon: Oui, de montants considérables.

Senator Wiebe: Going back to the port police, your answer left me with the impression that the right hand does not know what the left land is doing. Is that not your job, to protect the security of this country through our ports? Saying that the Department of Transport may have had a reason for not having the police there, what was the reason for the police in the first place and what is there now to replace it? This scares me, to be truthful with you.

If your response is that you do not know why the police were taken away and your do not know what the Department of Transport is doing, is our security so fragmented that we are different departments looking after different areas of the country? I hope you can reassure me.

Mr. D'Avignon: As I told Senator Atkins, I will look into this a little more closely. It is not something with which I am particularly familiar. I will be more than happy to get back to the committee with some answers.

Senator Cordy: You used the term "lawful access." As a citizen of Canada, I have wondered how you balance the acts of terrorism, the tactics that terrorists or criminals in general would use with the rights of the citizens? As Senator Meighen said earlier, in Canada we tend to bend over backwards to ensure that the rights of citizens are not trampled upon. How do you balance the two?

Mr. D'Avignon: The quick and easy answer to your question is that when police forces or security agencies want to use very intrusive techniques that come under the heading of "lawful access," they require warrants from the courts. The police must take the case to court, to a judge, present the case and seek judicial authorization. The police or security agency gets a warrant that has conditions attached to it, which they must respect, that allows them to undertake the interception or whatever else it could be, entry into a building, seizure or whatever it is that they are specifically asking for. They take it to a judge, they outline the case, the basis of the investigation and what it is that they are specifically looking for and the techniques that they wish to use. The judge decides whether their proposal is acceptable and whether they have a strong case for taking such action.

Senator Cordy: It would be done on a case-by-case basis; is that correct?

Mr. D'Avignon: That is exactly correct.

Senator Cordy: Perhaps not most, but certainly a significant amount of policing in our country is managed by municipalities and the provinces. You spoke earlier about the having made arrangements with these different policing agencies. Would this include training? What are the arrangements that you make with the local police forces?

Mr. D'Avignon: The arrangements are made under the Security Offences Act, in particular, section 6(2), which allows for police-to-police arrangements to be made.

Le sénateur Wiebe: Revenant à la question de la police portuaire, votre réponse m'a donné l'impression que la main droite ne sait pas ce que fait la main gauche. Votre rôle n'est-il pas d'assurer la sécurité du pays par l'intermédiaire de nos ports? Si l'on dit que le ministère des Transports a peut-être eu des raisons de ne pas y installer des policiers, pourquoi y a-t-il eu des policiers au départ et qu'y y a-t-il à l'heure actuelle en remplacement? Bien franchement, cela me fait peur.

Si votre réponse est que vous ne savez pas pourquoi la police a été enlevée et que vous ignorez ce que fait le ministère des Transports, notre sécurité est-elle si fragmentée qu'il y a différents ministères qui s'occupent de différentes régions du pays? J'espère que vous pourrez me rassurer.

M. D'Avignon: Comme je l'ai dit au sénateur Atkins, je vais regarder cela d'un petit peu plus près. Ce n'est pas un domaine qui m'est très familier. Je me ferai cependant un plaisir de revenir au comité avec des réponses.

Le sénateur Cordy: Vous avez utilisé l'expression «accès légal». En tant que citoyenne du Canada, je me demande comment vous assurez un équilibre entre les actes de terrorisme, les tactiques auxquelles recourent généralement terroristes et criminels, et les droits des citoyens. Comme l'a dit plus tôt le sénateur Meighen, au Canada nous avons tendance à nous fendre en quatre pour veiller à ce que les droits des citoyens ne soient pas bafoués. Comment faites-vous pour équilibrer les deux choses?

M. D'Avignon: La réponse simple et rapide à votre question est que lorsque les forces policières ou les agences de sécurité souhaitent employer des techniques très intrusives sous la rubrique «accès légal», il leur faut obtenir des mandats auprès des tribunaux. La police doit se présenter devant un tribunal, devant un juge, exposer l'affaire et demander une autorisation. La police ou l'agence de sécurité obtient un mandat assorti de conditions qui doivent être respectées et qui lui permettent d'entreprendre l'interception ou autre, de pénétrer dans un immeuble, de faire une saisie, et ainsi de suite, selon ce qui a été demandé. L'agence doit soumettre l'affaire à un juge, exposer le cas, justifier l'enquête, préciser ce qu'elle cherche et les techniques qu'elle souhaite employer. Le juge décide alors si la proposition est acceptable et si les mesures demandées sont justifiées.

Le sénateur Cordy: Ce serait donc fait au cas par cas, n'est-ce pas?

M. D'Avignon: Précisément.

Le sénateur Cordy: Ce n'est peut-être pas le cas de toutes les activités policières menées dans notre pays, mais une part importante en tout cas est assurée par les municipalités et les provinces. Vous avez parlé plus tôt de dispositions prises avec ces différentes agences de maintien de l'ordre. Ces arrangements engloberaient-ils la formation? Quels sont ces arrangements que vous prenez avec les forces de police locales?

M. D'Avignon: Les arrangements sont pris en vertu de la Loi sur les infractions en matière de sécurité, et plus particulièrement du paragraphe 6(2) qui permet la prise d'arrangements de force de police à force de police.

The arrangements are made between the RCMP and the municipal police forces. They deal, in particular, with terrorist incidents and how terrorist incidents will be managed. The Security Defences Act gives the RCMP the responsibility for terrorist incidents, but the RCMP has not interpreted their role as an exclusive role because, most often, if an incident occurs, the police force of jurisdiction will be the first on site and will start to deal with whatever is in front of them.

These arrangements allow the police, among themselves, to identify beforehand the types of events that they may be dealing with and how they will interact with one another, including the handover of responsibilities for the management of that particular incident. These arrangements are very operationally focused in relation to these kinds of incidents.

Mr. Mike Theilmann, Acting Director, Counter-Terrorism Division, Department of the Solicitor General Canada: Your point about training is very well taken, too. That is why we have the operational readiness program to support these arrangements, to ensure there is awareness at the local level and that police and incident commanders in particular know what arrangements are in place in their local jurisdiction. That is why we have been running seminars and tabletop exercises across the country for the last couple of years. We also run a component in the incident commanders course at the Canadian Police College. They are a primary target audience and we want to ensure they know what their responsibilities are in a terrorist incident and how they work with the RCMP. That backs up the arrangements with concrete training to ensure there is awareness at the local level.

Senator Cordy: In order that you have full cooperation by all levels in a specific incident.

Mr. Theilmann: Exactly. It is a multi-jurisdictional response and any terrorist incident engages the national interest, so that has to be there. That is why we put such an emphasis on training.

Senator Banks: I will be a bit more rude than my colleague Senator Wiebe was in reinforcing his point. If a reasonable person looked at the office of the Director General of National Security, Policing and Security Branch in a country with the longest coast line in the world, in which access to our country through the ports is and always has been an ongoing problem with regard to criminals and terrorists, it would be absurd, on the face of it, given the title of your office, that you do not have knowledge of, let alone control of, the policing of our ports. Perhaps you do in a different way, perhaps through the RCMP, CSIS or whatever, but it would seem to me that you really must know those things. I do hope that you will get back to us on that.

My question is addressed to Ms Leblanc. It follows up on what Senator Cordy said, something that Senator Atkins will remember well. We recently dealt with a bill dealing with CCRA and legal access to peoples' mail, particularly mail that was either leaving or coming into the country, sent by people of interest or addressed

Les arrangements sont pris entre la GRC et les forces de police municipales. Ils couvrent particulièrement les incidents terroristes et la façon d'y réagir. La Loi sur les infractions en matière de sécurité confère à la GRC la responsabilité relativement aux incidents terroristes, mais la GRC n'a pas interprété son rôle comme étant exclusif car, dans la plupart des cas, s'il y a incident, la force policière de l'endroit concerné sera le premier intervenant sur les lieux et traitera de ce à quoi elle sera confrontée.

Ces arrangements permettent aux forces de police de déterminer entre elles à l'avance les genres d'événements auxquels elles risquent d'être confrontées et l'interaction qu'elles voudront avoir entres elles, y compris le transfert de responsabilités en ce qui a trait à la gestion de tel ou tel incident. Ces arrangements, visant ce type d'incidents, sont de nature très opérationnelle.

M. Mike Theilmann, directeur intérimaire, Division de lutte contre le terrorisme, ministère du Solliciteur général du Canada: Vos propos au sujet de la formation sont eux aussi très justes. C'est pourquoi nous avons le programme de préparation opérationnelle, pour appuyer ces arrangements, pour veiller à ce qu'il y ait sensibilisation au niveau local et à ce que la police et les commandants sur place sachent quels arrangements sont prévus dans leur secteur. C'est pourquoi nous organisons depuis quelques années à l'échelle du pays séminaires et simulations d'exercices sur maquette. Nous nous occupons également d'un volet du cours pour commandants sur le terrain offert au Collège canadien de police. Il s'agit là d'un auditoire cible de première importance et nous tenons à ce qu'il connaisse ses responsabilités en cas d'incidents terroristes et sache comment travailler avec la GRC. Cela vient appuyer la formation concrète afin d'assurer qu'il y ait sensibilisation au niveau local.

Le sénateur Cordy: Afin de vous assurer l'entière collaboration de tous les paliers en cas d'incident.

M. Theilmann: Précisément. Il s'agit d'une réaction multijuridictionnelle et tout incident terroriste engage l'intérêt national, d'où l'importance que tout cela soit bien en place. C'est pourquoi nous mettons tant l'accent sur la formation.

Le sénateur Banks: Je vais être un petit peu plus impoli que ne l'a été mon collègue le sénateur Wiebe pour appuyer ses arguments. Si une personne raisonnable regardait le bureau du directeur général de la sécurité nationale, Secteur de la police et de la sécurité, dans un pays qui a la plus longue côte nationale au monde, et où l'accès à notre pays par les ports est et a toujours été un problème pour ce qui est des criminels et terroristes, il serait de prime abord absurde, étant donné le titre de votre bureau, que vous ne connaissiez ni ne contrôliez la surveillance policière de nos ports. Peut-être que vous le faites d'une façon différente, possiblement par le biais de la GRC, du SCRS ou autre, mais il me semble qu'il vous faudrait vraiment connaître ces choses. J'espère vraiment que vous nous reviendrez là-dessus.

Ma question s'adresse à Mme Leblanc et découle de ce qu'a dit le sénateur Cordy, ce dont le sénateur Atkins se souviendra très bien. Nous avons récemment traité d'un projet de loi portant sur la Loi sur le système correctionnel et la mise en liberté sous condition et sur l'accès légal au courrier des particuliers, surtout le

to people of interest — which is a nice way of saying people who are under suspicion of something.

I do not want to speak for either the committee, which recommended the bill's passage, or for the Senate, which did pass it. I will speak only for myself when I say that I held my nose when I voted for that aspect of the bill in committee, and in the Senate as well. We each had to make a decision as to the benefit as opposed to the disadvantage of allowing the Canada Customs and Revenue Agency to open peoples' mail, all the while claiming that they do not read it, they only open it to see if there is something in it. I understand why. One can put a computer chip or a dot in a piece of mail that could contain who knows what. We do need to do that. On the basis of opposite benefit, I, and I think all of us, decided to vote for the bill and it was passed.

However, we heard some horror stories, Ms Leblanc. One in particular that I recall vividly was that if they had to get a court order for every time they opened peoples' mail, the courts would be jammed. They do it with such frequency and in such large volume that they could not possibly get court orders to open all the mail they open. They are permitted to open mail without a court order depending upon its size and weight. There was a case, however, in which a piece of mail that exceeded the limit was opened. It was addressed to a person of interest outside the country. It turned out to be entirely innocent, but it contained confidential information having to do with a court case, I believe. In any case, the document contained in that piece of mail ended up in the dossier of the prosecutor in the case, which it clearly ought not to have. There is no way on earth that it should have got there because, of course, they do not read the mail.

My question to you is the same one that we asked at the time: Who is minding the store? Who makes the judgment? How far must we trust lawful authority and its exercise? How open do we need to have that gate? Can you give us some confidence that the circumstances that I described to you do not happen a lot and that there is a reasonable and acceptable balance between the cost in terms of access to private information, on the one hand, and the security of all of us on the other?

Ms Annie Leblanc, Acting Director, Technology and Lawful Access Division, Department of the Solicitor General Canada: Perhaps I can ask for clarification. You mentioned that mail opened was from people of interest to people of interest. Do you recall how that was defined by CCRA?

Senator Banks: Yes. The person in Canada to whom the mail was addressed was a person of interest.

Ms Leblanc: That was not defined further?

courrier à destination ou en partance du Canada envoyé par des personnes d'intérêt ou adressé à des personnes d'intérêt — ce qui est une appellation gentille pour les personnes que l'on soupçonne de quelque chose.

Je n'entends pas parler au nom ni du comité, qui a recommandé l'adoption du projet de loi, ni du Sénat, qui l'a bel et bien adopté. Je ne parle qu'en mon nom propre lorsque je dis que je me suis pincé le nez lorsque j'ai voté pour cet aspect du projet de loi en comité ainsi qu'au Sénat. Il nous a chacun fallu prendre une décision quant à l'opportunité du pouvoir de l'Agence des douanes et du revenu du Canada d'ouvrir le courrier des gens, qui prétend qu'elle ne le lit pas, qu'elle l'ouvre tout simplement pour voir s'il s'y trouve quelque chose. Je comprends pourquoi. L'on pourrait mettre dans un courrier une puce d'ordinateur ou autre chose contenant l'on ne sait quoi. Il nous faut prendre ces mesures. C'est à cause de cet avantage que moi-même et, je pense, nous tous, avons décidé de nous prononcer en faveur du projet de loi et de l'adopter.

Nous avons néanmoins entendu des histoires d'horreur, madame Leblanc. Je me souviens notamment très bien qu'on nous a dit que s'il leur fallait obtenir une ordonnance de la cour chaque fois qu'ils ouvraient le courrier des gens, les tribunaux seraient paralysés. Ils le font si souvent et pour des volumes si importants qu'il ne leur serait tout simplement pas possible d'obtenir des ordonnances de la cour les autorisant à ouvrir tout le courrier qu'ils ouvrent. Ils sont autorisés à ouvrir du courrier sans ordonnance de la cour selon la taille et le poids de l'envoi. Il y a cependant eu un cas d'ouverture d'un article qui dépassait la limite. Il était adressé à une personne d'intérêt à l'extérieur du pays. L'envoi s'est avéré être parfaitement innocent, mais il renfermait, je pense, des renseignements confidentiels se rapportant à une affaire judiciaire. Quoi qu'il en soit, le document renfermé dans l'enveloppe s'est retrouvé dans le dossier du procureur, ce qui, clairement, n'aurait jamais dû arriver. Cela n'aurait jamais dû se faire car, bien sûr, ils ne sont pas censés lire le courrier.

La question que je vous pose est la même que celle que nous avons posée à l'époque: qui surveille la boutique? Qui prend la décision? Jusqu'où doit aller notre confiance à l'égard de l'autorité légale et de l'exercice de son pouvoir? Jusqu'où doit-on ouvrir la grille? Pouvez-vous nous donner quelque assurance que les circonstances que je viens de vous décrire ne surviennent pas souvent et qu'il existe un équilibre raisonnable et acceptable entre le coût de l'accès à l'information privée d'un côté et la sécurité de nous tous de l'autre?

Mme Annie Leblanc, directrice intérimaire, Division de la technologie et de l'accès légal, ministère du Solliciteur général du Canada: Je peux peut-être demander un éclaircissement. Vous avez mentionné que le courrier ouvert était adressé à des personnes d'intérêt par des personnes d'intérêt. Vous souvenez-vous de la définition donnée dans la Loi sur le système correctionnel et la mise en liberté sous condition?

Le sénateur Banks: Oui. La personne au Canada à laquelle le courrier était adressé était une personne d'intérêt.

Mme Leblanc: Cela n'a pas été défini de façon plus précise?

Senator Banks: Yes. We asked. A person of interest was someone toward whom a security organization, CSIS, the RCMP or some other, had expressed an interest because the individual was under suspicion of criminal activity.

Ms Leblanc: So they did have information from a law enforcement or national security agency?

Senator Banks: Yes, and they were looking for the mail. This is almost a perfect example of the cost-benefit analysis. Here is a person of interest, under suspicion of having nefarious dealings, although not yet convicted of any crime. A piece of mail to that person was intercepted. It was an innocent piece of mail, not an illegal piece of mail. It was not contraband, it was not anything that ought not to have been sent through the mail, but it ended up in the wrong place. That is a risk, and I understand that we take it, but who is minding the store?

Ms. Leblanc: These types of situations are not the norm. There are exceptional circumstances in which some action needs to be taken before the judicial authority may be sought. The realm in which I work, lawful access, is based on the premise that there is a court authorization, either under the Criminal Code or the CSIS Act.

Senator Banks: I am sorry to interrupt, but we do have lawful access for packages over a certain size, and a court order is not required to open a package or a large envelope. If I understand it correctly, no such authority is needed. The post office can simply do it, and they do.

Ms Leblanc: In those circumstances, all facets were weighed very carefully. It was deemed that this was an appropriate measure to be taken. Obviously, it is not one that is taken lightly.

In the situation where a judge waives an individual's privacy rights, the decision is not taken easily; it is taken for the public good.

Senator Banks: I have no problem when court authority is requested, whether obtained or not. My problem is that the law now permits the opening of mail above a certain size and weight without a court authority. Who is minding that?

Ms Leblanc: I do not have much more information than what you have provided to me, and I appreciate that. I would venture to say that if the agencies are involved, and they are, then there is a basis for all the information to be compiled on these people of interest. If the process were approved, and it was, and the bill has passed, then these measures were deemed to be appropriate in exceptional circumstances.

Le sénateur Banks: Oui. Nous avons posé la question. Une personne d'intérêt est une personne à l'égard de laquelle un organisme de sécurité, le SCRS, la GRC ou autre, a exprimé de l'intérêt du fait qu'elle soit soupçonnée de s'être adonnée à des activités criminelles.

Mme Leblanc: Ils ont donc obtenu des renseignements auprès de forces de l'ordre ou d'une agence de sécurité nationale?

Le sénateur Banks: Oui, et ils cherchaient le courrier. C'est une illustration presque parfaite de l'analyse coûts-avantages. Voici une personne d'intérêt soupçonnée de s'être adonnée à de viles activités mais qui n'a encore été jugée coupable d'aucun crime. Un courrier destiné à cette personne a été intercepté. C'était un courrier innocent et non illégal. Ce n'était pas de la contrebande ni autre chose qui n'aurait pas dû être envoyé par courrier, mais cela s'est retrouvé au mauvais endroit. C'est là un risque, et je comprends qu'on le prenne, mais qui surveille la boutique?

Mme Leblanc: Ces types de situations ne sont pas la norme. Il se présente des circonstances exceptionnelles dans lesquelles des mesures doivent être prises avant que l'on ne puisse demander une autorisation aux tribunaux. Le domaine dans lequel j'oeuvre, soit l'accès légal, s'appuie sur la prémisse qu'il y a une autorisation des tribunaux, en vertu du Code criminel ou de la Loi sur le SCRS.

Le sénateur Banks: Excusez-moi de vous interrompre, mais l'accès légal est reconnu pour les paquets supérieurs à une certaine taille, et un mandat judiciaire n'est pas requise pour ouvrir un paquet ou une grosse enveloppe. Si j'ai bien compris, aucune autorisation du genre n'est requise dans de tels cas. Les Postes peuvent tout simplement le faire, et c'est ce qui se passe.

Mme Leblanc: Dans ces circonstances, tous les éléments ont été soigneusement évalués. L'on a considéré que c'était une mesure appropriée. Il est certain que ce n'est pas une chose qui est prise à la légère.

Dans les cas où le juge balaie les droits à la vie privée de l'intéressé, cette décision n'est pas prise à la légère, elle est prise dans l'intérêt du bien public.

Le sénateur Banks: Je n'ai aucun problème lorsque l'autorisation des tribunaux est demandée, qu'elle soit ou non obtenue. Mon problème est que la loi autorise à l'heure actuelle l'ouverture d'envois postaux supérieurs à une certaine taille et à un certain poids sans autorisation accordée par un tribunal. Qui surveille les choses?

Mme Leblanc: Je ne dispose pas de beaucoup plus de renseignements que ceux que vous m'avez fournis, et je comprends la situation. Je dirais que si les agences interviennent, et c'est bien le cas, alors il est normal que l'on compile tous ces renseignements au sujet de ces personnes d'intérêt. Si le processus était approuvé, et cela a été le cas ici, et le projet de loi a été adopté, alors ces mesures ont été jugées appropriées dans les cas de circonstances exceptionnelles.

Again, I would say that confidential information such as a letter, which is probably solicitor-client privilege, should have not surfaced. I would say that this would be exceptional circumstance.

Senator Banks: One more question, if I may. It has to do with points raised previously. My question is with respect to the passport. You will forgive my, if not our, cynicism.

Senator Meighen mentioned that he remembers the kind of passport that the accused assassin of Martin Luther King carried. It was a Canadian one. People said that they would tighten this up. However, it now appears that Mr. Ressam received his passport without even having gone to pick it up. Someone else picked it up for him.

It turns out that although Mr. Ressam was a person of interest to our security forces, United States officers arrested him as he crossed the border into the United States with a bomb in his car. On the face of it, that would make us look dumb.

Perhaps I should not address the question to you but rather to the Minister of Citizenship and Immigration, but you must surely have an interest in whether or not people can pick up Canadian passports by sending a messenger. This is not a new situation. This is a situation that, as Senator Meighen pointed out, has been in place for years and years. Are you confident that something will be done about it?

Mr. D'Avignon: As I said earlier, senator, there is a review underway of that entire case and the various dimensions of it, including access to passports. That is being examined.

The passport office has already introduced measures to offset the use of baptismal certificates and to increase exchange of information to better identify who the people are. I am not totally familiar with all the technicalities but, suffice it to say, yes, it is a concern.

The entire case is being examined to identify weaknesses in the system and how to correct them. Particular to passports, there is some work that is already underway to deal with those vulnerabilities.

We are learning. We will continue to learn, and we will be taking measures to stopgap those cases where there has been some vulnerability, which has been exploited.

[*Translation*]

Senator Pépin: I would like to come back to one aspect of our security cooperation with other countries, and specifically the Echelon network which the United States, Canada, New Zealand and Australia are part of. That network was created some years ago and was originally conceived as a communication intelligence system capable of intercepting communications originating in East Block countries. According to several articles that appeared in mainly European newspapers, the Echelon system is now used for other purposes. Indeed, faxes, phone conversations and E-mail are now apparently used for the purposes of economic espionage. Without necessarily attributing too much credibility to this

Encore une fois, je dirais que des communications confidentielles, comme par exemple une lettre, qui relèvent sans doute du secret professionnel, n'auraient jamais dû apparaître. Je dirais qu'il s'agirait là de circonstances exceptionnelles.

Le sénateur Banks: Encore une question, si vous permettez. Elle concerne des points soulevés précédemment. Ma question porte sur les passeports. Vous me pardonnerez mon, voire notre, cynisme.

Le sénateur Meighen a mentionné qu'il se souvient du genre de passeport dont était munie la personne accusée du meurtre de Martin Luther King. C'était un passeport canadien. Les gens avaient dit qu'ils resserreraient tout cela. Or, il appert aujourd'hui que M. Ressam a obtenu son passeport sans même être allé le chercher. C'est quelqu'un d'autre qui est allé le récupérer pour lui.

Il s'avère que, bien que M. Ressam ait été une personne d'intérêt pour nos forces de sécurité, ce sont des agents américains qui l'ont arrêté alors qu'il traversait la frontière pour aller aux États-Unis avec une bombe dans sa voiture. Nous avons l'air, à première vue, un peu bêtes.

Je devrais peut-être poser la question non pas à vous mais au ministre de la Citoyenneté et de l'Immigration, mais cela doit certainement vous intéresser de savoir si des gens peuvent faire ramasser un passeport canadien par un messager. Il ne s'agit pas d'une situation nouvelle. Il s'agit d'une situation qui, comme l'a souligné le sénateur Meighen, existe depuis des années. Êtes-vous convaincu qu'on y fera quelque chose?

M. D'Avignon: Comme je l'ai dit plus tôt, sénateur, toute cette affaire, avec toutes ses dimensions, y compris l'accès aux passeports, est en train d'être réexaminée. On s'y penche.

Le bureau des passeports a déjà mis en place des mesures eu égard à l'utilisation de certificats de baptême et pour augmenter l'échange d'informations afin de mieux cerner l'identité des demandeurs. Je ne suis pas au courant de tous les aspects techniques mais qu'il suffise de dire que oui, c'est un grand sujet de préoccupation.

Toute l'affaire est en train d'être examinée pour déterminer quelles sont les faiblesses du système et comment les corriger. Pour ce qui est des passeports en particulier, du travail est déjà en cours en vue d'éliminer les failles.

Nous apprenons. Nous continuerons d'apprendre et nous prendrons des mesures pour colmater les brèches là où elles ont été exploitées.

[*Français*]

Le sénateur Pépin: J'aimerais revenir sur un aspect de notre partenariat avec d'autres pays en matière de sécurité, plus précisément sur le réseau Échelon qui réunit les États-Unis, le Canada, la Nouvelle-Zélande et l'Australie. Ce réseau a été créé il y a plusieurs années et il était, à l'origine, un système d'écoute qui devait intercepter les communications du Bloc de l'Est. Selon un bon nombre d'articles de journaux, dont la plupart sont européens, le système Échelon est maintenant utilisé à d'autres fins. En fait, on utiliserait les télécopies, les conversations téléphoniques et les courriels pour des fins d'espionnage économique. Sans prêter trop de crédibilité à ces informations, quelle est la nature exacte du

information, I would like to know what the exact nature of that network is. What are its actual capabilities and what is Canada's role within that network? And finally, in what way does it benefit our country?

Mr. D'Avignon: Unfortunately, that is not an area I am particularly familiar with. I would have to do some research and provide that information at a later date. I am afraid I am not able to give an intelligent answer to that question.

Senator Pépin: Earlier, you referred to the security work and training you carry out in cooperation with all the provinces with the exception of Quebec. Would it be indiscreet to enquire as to why Quebec is not part of that agreement?

Mr. D'Avignon: Quebec prefers not to sign formal agreements involving police force cooperation. However, that does not mean that there is no cooperation. On the contrary, relations between our Department and the Ministry of Public Security in Quebec are excellent. The Sûreté du Québec and the Royal Canadian Mounted Police work very well together. I could cite the example of the Summit of the Americas held in Quebec City, where the RCMP, Sûreté du Québec, and the Ste-Foy and Quebec City Police Forces worked together to divide up roles and responsibilities. Together, they worked out an agreement that all parties abided by throughout the event and which allowed them to maintain control during the Summit.

Quebec's official position, however, is that it does not wish to be a party to any formal agreement. Notwithstanding the reality in terms of the police forces and officials involved, we maintain very good relations as regards information sharing and cooperation.

Senator Pépin: In Montreal, a ceremony is held every year in November where the RCMP and Quebec police officers distribute awards to police officers who distinguished themselves in the performance of their duties. So, I was wondering why Quebec was not a signatory to the agreement.

Mr. D'Avignon: On the ground, there is excellent cooperation.

[*English*]

The Chairman: Mr. D'Avignon, what relationship, if any, is there between the Solicitor General and the Department of Defence in defining threats or risks to the country?

Mr. D'Avignon: There is a fairly tight relationship, if you will. There are a number of areas in which we intersect. In the context of the national counterterrorism plan, National Defence has a role at the table in the work that we do in putting the plan together.

Within the counterterrorism plan, there is the interdepartmental policy advisory group, which I chair, and on which National Defence sits. In fact, Cmdre. Forcier, who was here yesterday, and some of his staff sit on that committee.

We have a relationship with them for training and involvement in exercises. All of the exercises we have done engage the Department of National Defence and bring them to the table to participate in those exercises.

réseau? Quelles sont ses capacités réelles et quel est le rôle du Canada dans ce réseau? Enfin, quels avantages apporte-t-il à notre pays?

M. D'Avignon: Malheureusement, ce n'est pas un domaine que je connais particulièrement bien. Il faudrait que je fasse une recherche de renseignements pour ensuite vous les fournir. Je ne suis vraiment pas en mesure de parler de façon intelligente.

Le sénateur Pépin: Tout à l'heure, vous nous avez parlé du travail que vous faites au point du vue sécurité et entraînement en collaboration avec toutes les provinces, sauf le Québec. Serait-il trop indiscret de vous demander quelle est la raison pour laquelle le Québec ne fait pas partie de cette entente?

M. D'Avignon: Le Québec préfère ne pas parapher des ententes formelles dans le domaine des forces policières. Toutefois, cela ne veut pas dire qu'il n'y a pas de collaboration. Au contraire, la relation entre notre ministère et le ministère de la Sécurité publique au Québec est très bonne. La Sûreté du Québec et la Gendarmerie royale du Canada travaillent très bien ensemble. Je peux vous donner l'exemple du Sommet des Amériques tenu à Québec où la GRC, la Sûreté du Québec, le corps policier de Sainte-Foy et celui de la ville de Québec se sont tous entendus pour répartir les rôles et les responsabilités. Ils ont, entre eux, établi un accord qu'ils ont respecté tout au long de l'événement et qui leur a permis de contrôler la situation lors du Sommet.

Du point de vue officiel, le Québec ne veut pas s'engager dans une entente formelle. Nonobstant la réalité au niveau des corps policiers et des fonctionnaires, il y a une très bonne relation de partage et de collaboration.

Le sénateur Pépin: Chaque année en novembre, à Montréal, il y a une cérémonie où la GRC et les policiers du Québec remettent des prix aux policiers qui se sont démarqués lors d'un événement quelconque. Je me demandais alors pourquoi le Québec ne signait pas l'entente.

M. D'Avignon: Sur le terrain, il y a une très bonne collaboration.

[*Traduction*]

Le président: M. D'Avignon, quelle relation, s'il y en a une, existe entre le solliciteur général et le ministre de la Défense quant à la définition de menace ou de risque pour le pays?

M. D'Avignon: Il existe, si vous voulez, une relation plutôt étroite. Il y a plusieurs domaines dans lesquels nos activités s'entrecroisent. Dans le contexte du plan national de lutte contre le terrorisme, la Défense nationale a un rôle à la table dans le travail que nous abattons dans le cadre de l'élaboration du plan.

Existe à l'intérieur du plan de lutte contre le terrorisme un groupe consultatif sur la politique interministérielle que je préside et auquel siège la Défense nationale. En fait, le commodore Forcier, qui était ici hier, et certains membres de son équipe siègent à ce comité.

Nous entretenons avec eux une relation en vue de la formation et de la participation aux exercices. Tous les exercices que nous avons menés ont engagé le ministère de la Défense nationale de sorte que celui-ci vienne à la table pour y participer.

As well, we organize training with them for first responders and for provincial police forces, particularly in the area of chemical, biological and radiological threats. There is a required training component coordinated with National Defence for first responders and police forces.

At a broader level, the Department of National Defence is involved in a series of committees operating at a senior level to discuss national security matters. They sit on the interdepartmental policy committee, which is chaired by the Privy Council Office, that brings together assistant deputy ministers to discuss policy issues related to national security engaged at that level. The interdepartmental committee on security and intelligence, which is chaired at the deputy minister level, involves National Defence as well. DND is part and parcel of the fabric of everything that is done.

They also provide assessments to various departments. Their primary focus on threat from a military point of view, and it is usually most focused offshore in respect of areas where the Canadian Armed Forces are actually engaged. However, they receive information from other agencies and share information with the other agencies to round out the threat analyses during the everyday course of business.

The Chairman: You commented earlier on Quebec and the fact that they had not signed an accord with the federal government. Do contract provinces function differently than non-contract provinces? Do Quebec and Ontario, with their own provincial police forces, have a different sort of arrangement?

Mr. D'Avignon: I do not think so, no. The arrangements are made between the RCMP and the Ontario Provincial Police or the Sûreté. In the case where the RCMP are the police of local jurisdiction, such as in some of the provinces, then that facilitates the whole relationship because they are dealing with themselves at different levels, obviously. I have not seen anything that would indicate that there is any substantive or qualitative difference in terms of the functioning of the relationships. They tend to cooperate well with one another to exchange information and work together in those cases where they are brought together by operational need.

The Chairman: There is legislation in place that provides for the federal authorities to take control of a terrorist incident. Is that correct?

Mr. D'Avignon: Yes. The Security Offences Act gives the RCMP the authority to take charge of those cases that involve a terrorist incident.

The Chairman: Has that authority ever been exercised?

Mr. Theilmann: I do not believe it has ever actually been used.

The Chairman: How does it work when you train with other police forces? Do they accept the arrangement and are they comfortable with the idea that a federal officer can arrive on the scene and declare that, under the act, they are in charge?

Nous organisons par ailleurs avec eux de la formation destinée aux premiers intervenants et aux forces de police provinciales, dans le contexte surtout de menaces chimiques, biologiques et radiologiques. Il y a un volet de formation obligatoire qui est coordonné avec la Défense nationale et qui est destiné aux premiers intervenants et aux forces de police.

À un niveau plus large, le ministère de la Défense nationale participe à une série de comités de niveau supérieur qui discutent de questions de sécurité nationale. Il siège au comité politique interministériel que préside le bureau du Conseil privé et qui réunit des sous-ministres adjoints dans le but de discuter des questions de politique liées à la sécurité nationale à ce niveau. Le comité interministériel sur la sécurité et le renseignement, qui est présidé au niveau sous-ministre, compte lui aussi sur la participation de la Défense nationale. Le MDN fait partie intégrante de tout ce qui est entrepris.

Il fournit également des évaluations à différents ministères. Il s'intéresse au premier chef aux menaces de type militaire surtout celles se dessinant à l'étranger dans des secteurs où les Forces armées canadiennes sont véritablement engagées. Il reçoit cependant des renseignements d'autres agences et en communique à son tour à certaines agences dans le but de parachever les analyses de menaces faisant partie de son quotidien.

Le président: Vous avez parlé plus tôt du Québec et du fait qu'il n'ait pas signé d'accord avec le gouvernement fédéral. Les provinces liées par un contrat fonctionnent-elles différemment des provinces qui n'en ont pas signé? Le Québec et l'Ontario, qui sont dotés de leur propre force de police provinciale, ont-ils des arrangements différents?

M. D'Avignon: Non, je ne le pense pas. Les arrangements sont pris par la GRC et par la police provinciale de l'Ontario ou par la Sûreté. Dans les cas où la GRC est la force policière locale, comme c'est le cas dans certaines provinces, alors cela facilite toute la relation car elles traitent avec elles-mêmes à différents niveaux, bien évidemment. Je n'ai rien vu qui indique qu'il y ait de différences qualitatives ou fondamentales du côté du fonctionnement des relations. Il semble qu'il y ait une bonne collaboration et de bons échanges d'informations entre les différentes forces et qu'elles travaillent bien ensemble lorsque le besoin opérationnel les met ensemble.

Le président: Il existe une loi en vertu de laquelle les autorités fédérales doivent prendre le contrôle en cas d'incident terroriste, n'est-ce pas?

M. D'Avignon: Oui. La Loi sur les infractions en matière de sécurité autorise la GRC à prendre le contrôle de la situation en cas d'incident terroriste.

Le président: Ce pouvoir a-t-il jamais été exercé?

M. Theilmann: Je ne pense pas qu'il ait jamais été véritablement exercé.

Le président: Comment cela fonctionne-t-il lorsque la formation se fait avec d'autres forces policières? Les participants acceptent-ils l'arrangement et sont-ils confortables avec l'idée qu'un agent fédéral puisse se présenter et déclarer qu'en vertu de la loi c'est lui le responsable?

Mr. Theilmann: In our training exercises, one of the objectives is to exercise whatever agreement is in place between the RCMP and the local police force of the jurisdiction. That agreement is in place to lay out the roles and responsibilities during a terrorist incident. It is laid out in black and white already. In an exercise, we are practising the provisions of that agreement, such as calling for a handover.

The RCMP say they always interpreted it to mean that they have primary jurisdiction but not exclusive jurisdiction. They realize that in some areas of Canada there will be a police force on the ground, such as in Toronto. They work out exactly who does what in responding to a terrorist incident.

For example, if the Toronto police force wanted access to federal resources, such as Joint Task Force 2 or the RCMP-DND biological defence response team, that would always be done through the RCMP chain of command. Thus, the RCMP are always important players; and that is in these agreements.

The Chairman: The legislation provides for the RCMP to decide on their own that they will assume authority. They do not have to consult with the municipal officials because they have authority under the act to say, "This is our baby."

Mr. Theilmann: We work it out beforehand to ensure that there is a legislative authority to respond to terrorist incidents. In an operational context where there are jurisdictional people on the ground, the RCMP could give you more information about the arrangements they have in specific provinces.

The Chairman: Are agreements in place with each municipal police force?

Mr. Theilmann: Yes, they are.

The Chairman: In respect of government computer systems, have we experienced unauthorized access?

Mr. D'Avignon: I am not quite sure what the answer to that question is. I think that representatives from the Office of Critical Infrastructure Protection and Emergency Preparedness, OCIPEP, would be in a better position to speak to that particular issue. There have been studies, as well as some review, of these kinds of intrusions, and they would have a better sense of what has happened on that front.

Senator Forrestall: I have a question concerning a current problem. The United States has issued a second terrorist attack warning, concentrating primarily on the Arabian Peninsula and within the Persian Gulf, generally. That warning is for both the military and civilian population in the area. A few weeks ago, a Canadian frigate in the gulf put to sea to lessen her vulnerability to attack. Of course, this relates quite directly, but not solely, to the attack on the USS *Cole.*

Are you aware of the American warning that I understand was reported yesterday but perhaps issued somewhat earlier? Is this warning attributed, or related, to Usama Bin Laden? Has Canada taken any steps to issue a caution to our civilians and military personnel who are in the Persian Gulf or the Arabian Peninsula area?

M. Theilmann: Dans le cadre de nos exercices de formation, l'un de nos objectifs est de mettre à l'épreuve toute entente en place entre la GRC et la police locale. Ces ententes ont pour objet d'établir les rôles et les responsabilités en cas d'incident terroriste. Tout est déjà écrit noir sur blanc. Dans le cadre d'un exercice, nous mettons en application les dispositions de l'entente, comme par exemple la cession de pouvoirs.

La GRC dit avoir toujours interprété cela comme signifiant qu'elle détient la principale juridiction, mais que celle-ci n'est pas exclusive. Elle sait que dans certaines parties du pays, comme par exemple dans la ville de Toronto, il y aura déjà sur le terrain une force policière. Il s'agit donc de déterminer très exactement qui fait quoi face à un incident terroriste.

Par exemple, si la police torontoise voulait accéder à des ressources fédérales, comme par exemple la Force opérationnelle II ou l'Équipe de défense biologique GRC-MDN, cela passerait toujours par la chaîne de commandement de la GRC. Ainsi, la GRC demeure un joueur important, et cela fait partie de ces ententes.

Le président: La loi prévoit que la GRC décide par elle-même si elle veut assumer le contrôle d'une situation. Elle n'a pas à consulter les fonctionnaires municipaux car elle est, en vertu de la loi, autorisée à dire que c'est son affaire.

M. Theilmann: Nous établissons tout à l'avance afin d'être certain qu'il existe un pouvoir législatif de réagir à des incidents terroristes. Dans un contexte opérationnel où il y a des responsables sur le terrain, la GRC pourrait mieux vous renseigner au sujet des arrangements qu'elle a pris dans diverses provinces.

Le président: Des arrangements sont-ils en place avec chaque force de police municipale?

M. Theilmann: Oui.

Le président: Pour ce qui est des systèmes informatiques du gouvernement, y a-t-il eu des cas d'accès non autorisé?

M. D'Avignon: Je ne sais trop quelle est la réponse à cette question. Je pense que les représentants du Bureau de la protection des infrastructures essentielles et de la protection civile ou BPIEPC, seraient mieux en mesure de vous entretenir de cette question précise. Il y a eu des études, ainsi qu'un réexamen, de ces types d'intrusion, et les gens du Bureau auraient une meilleure idée de ce qui s'est passé à cet égard.

Le sénateur Forrestall: J'ai une question au sujet d'un problème actuel. Les États-Unis ont émis une deuxième alerte en cas d'attaque terroriste, visant principalement la péninsule arabe et la région du golfe Persique. Cette alerte est destinée et aux militaires et à la population civile dans la zone. Il y a quelques semaines, une frégate canadienne dans le Golfe a pris le large pour être moins vulnérable aux attaques. Cela découle bien sûr directement, mais pas seulement, de l'attaque contre le USS *Cole.*

Étiez-vous au courant de l'avertissement américain qui, si j'ai bien compris, a été rapporté hier mais a peut-être été émis un petit peu plus tôt? Cet avertissement est-il attribué ou lié à Usama Bin Laden? Le Canada a-t-il pris des mesures pour avertir nos civils et notre personnel militaire se trouvant dans le golfe Persique ou dans la région de la péninsule arabe?

Mr. D'Avignon: Like you, I read this morning in the newspaper that a warning had been issued to American forces in the Persian Gulf.

As you know, threat assessments are conducted on a daily basis based on information that is shared between the various intelligence agencies. That is done on an international level; they talk to one another.

As to whether the Department of External Affairs or the Department of National Defence have issued warnings to Canadian citizens overseas in that area, I quite honestly do not have the answer to that.

Normally, the Department of External Affairs does put out warnings to Canadians who are overseas in areas where a problem is brewing or is occurring. Canadian travellers may be asked to leave or to go to the consulates. I do not know in this particular case whether External Affairs has done so.

Senator Forrestall: This would not then normally come across your desk?

Mr. D'Avignon: No. That would be dealt with either by Department of National Defence in its own right or by the Department of External Affairs. We are not responsible for that.

Senator Forrestall: You will appreciate the concern?

Mr. D'Avignon: Absolutely.

Senator Forrestall: The concern has been heightened somewhat. I thought perhaps there was a coordinating effect whereby a warning went across your desk before going any further.

Mr. D'Avignon: No, it does not.

Ms Leblanc: Mr. D'Avignon, Alberta has as one pride and joy a province-wide public radio network, the CKO radio network, which has 17 radio stations throughout the province. At the flick of a switch, that network can interrupt all other radio stations and broadcast emergency preparedness notices, warning of any kind of disaster. The federal government contributes on the basis of emergency preparedness. I do not know how familiar you are with that, but do you know if any such instant radio-based warning systems exist in other provinces?

Mr. Theilmann: I honestly do not know. I worked at Emergency Preparedness Canada many years ago and much work was being done then on emergency broadcast systems. I do not know where it stands right now. You might want to direct that question to the Office of Critical Infrastructure Protection and Critical Preparedness this afternoon. They may have more knowledge.

The Chairman: Thank you for appearing before us. We appreciate receiving the information you have provided us and we hope to receive still more from you regarding ports. We will look forward to receiving that.

M. D'Avignon: J'ai tout comme vous appris ce matin en lisant le journal qu'une alerte avait été émise aux forces américaines dans le golfe Persique.

Comme vous le savez, il se fait chaque jour des évaluations de menaces sur la base de renseignements échangés par les différentes agences de renseignements. Cela se fait au niveau international; les différentes agences se parlent entre elles.

Quant à la question de savoir si le ministère des Affaires étrangères ou si celui de la Défense nationale ont émis des avertissements aux citoyens canadiens présents dans la région, je vous dis bien franchement que je ne connais pas la réponse.

En règle générale, le ministère des Affaires étrangères met en garde les Canadiens en pays étranger se trouvant dans des zones où un problème couve ou éclate. Il arrive que l'on demande aux touristes canadiens de partir ou de se rendre à un consulat. J'ignore si le ministère des Affaires étrangères a fait cela dans ce cas-ci.

Le sénateur Forrestall: Ce genre de chose ne vous serait donc pas normalement communiqué dans le cadre de votre travail?

M. D'Avignon: Non. Cela serait l'affaire ou du ministère de la Défense nationale ou de celui des Affaires étrangères. Nous ne sommes pas responsables de cela.

Le sénateur Forrestall: Vous comprenez cependant la préoccupation?

M. D'Avignon: Absolument.

Le sénateur Forrestall: Cette préoccupation a été quelque peu rehaussée. Je pensais qu'il y avait peut-être un certain travail de coordination en vertu duquel un avertissement passait par votre bureau avant d'aller plus loin.

M. D'Avignon: Non, ce n'est pas le cas.

Mme Leblanc: Monsieur D'Avignon, l'Alberta est très heureuse et très fière de son réseau provincial de radio public, le réseau CKO, qui compte 17 stations de radio dans la province. Au moyen d'une simple touche, le réseau peut interrompre les émissions de toutes les autres stations de radio et diffuser des avis de préparation à une situation d'urgence pour avertir les citoyens de tout désastre possible. Le gouvernement fédéral contribue à la planification d'urgence. J'ignore si vous êtes au courant, mais savez-vous s'il existe de tels systèmes d'avertissement radio instantané dans d'autres provinces?

M. Theilmann: Bien franchement, je ne le sais pas. J'ai travaillé à Protection civile Canada il y a de nombreuses années et beaucoup de travail de systèmes de radiodiffusion en cas de situation d'urgence se faisait à l'époque. J'ignore où en sont les choses aujourd'hui. Vous voudrez peut-être poser votre question aux représentants du Bureau de la protection des infrastructures essentielles et de la protection civile qui doivent vous rencontrer cet après-midi. Ils seront peut-être plus au courant.

Le président: Merci d'être venus comparaître devant nous. Nous vous sommes reconnaissants des renseignements que vous nous avez fournis et nous comptons en recevoir encore davantage de vous relativement aux ports. Nous attendons ces précisions supplémentaires avec impatience.

Mr. D'Avignon: I will make sure you get it.

The Chairman: Honourable senators, our next witness this morning is Superintendent Pilgrim. Supt. Pilgrim has been a member of the RCMP for 31 years. Much of his career was spent in New Brunswick, where his duties included general policing, drug enforcement and national security enforcement. After receiving his commission to the rank of inspector, he was posted to Nova Scotia, where he was responsible for planning and management services, federal enforcement branch, in the Cole Harbour detachment. After promotion to superintendent, he served as Director, Counterterrorism Division, at the Department of Solicitor General. Last September, he transferred to his present position as Officer in Charge, National Security Investigations Branch, Criminal Intelligence Directorate at RCMP headquarters. He will speak to us about the national security mandate of the RCMP.

Welcome, Supt. Pilgrim. The floor is yours.

Superintendent J. Wayne Pilgrim, Officer in Charge, National Security Investigations Branch, Criminal Intelligence Directorate: On behalf of the RCMP, it is a pleasure to be here today to provide an overview of the national security program and to identify some of the challenges that face law enforcement as it relates to national security.

I wish to draw your attention to two organization charts that were provided for you. One is entitled "Headquarters Organization"; the second is entitled "Criminal Intelligence Directorate." To put things in perspective as to where I sit in the scheme of things, in the "Headquarters Organization" chart you will note that the Commissioner is at the top. The highlighted area indicates the Deputy Commissioner of Operations. Follow that down to the Criminal Intelligence Directorate or the Assistant Commissioner Criminal Intelligence, my immediate boss, Assistant Commissioner Richard Proulx. The second chart provides the organization of the Criminal Intelligence Directorate and the highlighted areas show where the National Security Investigation branch fits into that process.

To begin, I would like to provide a brief overview of the RCMP mandate to investigate national security offences under the Security Offences Act.

With the separation of the security service in 1984, the RCMP maintained its responsibility to conduct criminal investigations of national security offences. The act did not create any new offences. It did, however, confirm, for the first time in legislation, that, for specific offences having a national security dimension, the RCMP had primary peace officer responsibility.

While the responsibility of CSIS is to collect and advise the government on threats to the security of Canada, we both have the responsibility to prevent, deter and investigate potential threats. The RCMP has the primary responsibility to conduct criminal

M. D'Avignon: Je veillerai à ce que vous receviez cela.

Le président: Honorables sénateurs, le témoin suivant ce matin est le surintendant Pilgrim. Le surintendant Pilgrim travaille à la GRC depuis 31 ans. Il a travaillé pendant une grosse partie de sa carrière au Nouveau-Brunswick, où il a été affecté à divers services dont la police générale, la lutte antidrogue et la sécurité nationale. Après avoir été promu au grade d'inspecteur, il a été affecté en Nouvelle-Écosse où il a exercé des tâches de gestion en tant que responsable des services de gestion et de planification, du service divisionnaire de l'exécution des lois fédérales et du détachement de Cole Harbour. Après sa promotion au grade de surintendant, il a été nommé à la tête de la Division de l'antiterrorisme au ministère du Solliciteur général du Canada. En septembre dernier, il a été muté au poste qu'il occupe actuellement à titre d'officier responsable de la Sous-direction des enquêtes relatives à la sécurité nationale de la Direction des renseignements criminels à la DG de la GRC. Il va nous entretenir du mandat en matière de sécurité nationale de la GRC.

Bienvenue, surintendant Pilgrim. Vous avez la parole.

Le surintendant J. Wayne Pilgrim, officier responsable de la Sous-direction des enquêtes relatives à la sécurité nationale, Direction des renseignements criminels: C'est un plaisir pour moi d'être ici devant vous aujourd'hui au nom de la GRC pour vous faire un survol du programme de sécurité nationale et cerner certains des défis auxquels se trouvent confrontées les forces de maintien de l'ordre dans le contexte de la sécurité nationale.

Je souhaite porter à votre attention deux organigrammes qui vous ont été fournis. L'un s'intitule «Headquarters Organization» et le deuxième «Direction des renseignements criminels». Pour vous situer un petit peu mon rôle dans tout cela, vous constaterez que dans l'organigramme intitulé «Headquarters Organization» le commissaire se trouve tout à fait en haut. La case hachurée correspond au sous-commissaire responsable des opérations. Suivez la ligne vers le bas jusqu'à la Direction des renseignements criminels ou au commissaire adjoint aux renseignements criminels et vous y trouverez mon supérieur immédiat, le commissaire adjoint Richard Proulx. Le deuxième organigramme représente la Direction des renseignements criminels et on y voit bien où s'inscrit dans tout le processus la Sous-direction des enquêtes relatives à la sécurité nationale.

J'aimerais, pour commencer, vous donner un bref aperçu du mandat de la GRC d'enquêter sur les infractions relatives à la sécurité nationale en vertu de la Loi sur les infractions en matière de sécurité.

Suite à la séparation du service de sécurité en 1984, la GRC a maintenu sa responsabilité de mener des enquêtes criminelles pour les infractions relatives à la sécurité nationale. La loi n'a pas créé de nouveaux délits. Elle a cependant confirmé, pour la toute première fois en droit, que pour certains délits particuliers ayant une dimension sécurité nationale, la GRC avait la responsabilité première d'exercer le rôle d'agent de la paix.

Bien que la responsabilité du SCRS soit d'enquêter et de conseiller le gouvernement relativement aux menaces à la sécurité du Canada, nous avons tous deux pour responsabilité de prévenir et de décourager les menaces potentielles et d'enquêter sur

investigations into national security offences, which has been defined to include threats to the security of Canada, as defined under the CSIS Act, and threats against internationally protected persons, or IPPs, within the meaning of the Criminal Code of Canada. Criminality must be present for RCMP involvement.

RCMP headquarters monitors all national security-related investigations. We ensure liaison and dissemination of information between field units and various international agencies. In order to carry out our duties, we have 169 established positions within the program nationally.

The RCMP provides subject-matter expertise in various areas of responsibility, for example, criminal investigators of national security offences, collecting and reviewing threat-related information and intelligence pertaining to persons and property of specific Canadian and foreign dignitaries, diplomatic and consular officials, performing a liaison function with CSIS and agencies, and managing a threat assessment program in support of our protective operations. Threat assessments are used to assign appropriate level of physical security.

In 1996, the RCMP enhanced its national security investigation capability at international airports. This initiative coincided with the termination of the RCMP's protective and security mandate at designated airports. It is important to note that the RCMP continues to provide protective and security functions under contract to airport authorities where we are the police of jurisdiction. Airport national security investigation sections are located at Vancouver, Edmonton, Calgary, Winnipeg, Toronto, Ottawa, Dorval and Halifax. Mirabel and Gander, because of their change in status, no longer have a national security investigation present. The airport units are satellites of the divisional national security investigation sections to ensure there is a cohesion and direction with respect to national security priorities.

Pursuant to section 6(1) of the Security Offences Act, the RCMP has primary responsibility. We have interpreted this to mean that this responsibility is not exclusive. As you heard from the previous witness in this regard, it takes into reality the jurisdictional makeup of the country, federal, provincial and municipal. At present, there are approximately 65 police to police agreements nationally between the RCMP and other police of jurisdiction. These agreements are designed to set out the role of the RCMP vis-à-vis the police force of jurisdiction in the event of a national security incident.

Section 6(2) of the Security Offences Act provides the federal government with authority to enter into an arrangement with provinces and territories for the policing of an offence outlined under the act. The Solicitor General, as you heard earlier, is presently undertaking a review of the government-to-government arrangements. This will be followed by a re-examination of the

celles-ci. La GRC a pour principale responsabilité de mener des enquêtes criminelles sur les infractions relatives à la sécurité nationale, définies comme englobant les menaces à la sécurité du Canada, au sens de la Loi sur le SCRS, et les menaces contre les personnes jouissant d'une protection internationale, au sens du Code criminel du Canada. Il doit y avoir criminalité pour qu'intervienne la GRC.

La Direction générale de la GRC surveille toutes les enquêtes relatives à la sécurité nationale. Nous veillons à la liaison et à la diffusion de renseignements entre les unités divisionnaires et divers organismes internationaux. Afin d'être en mesure de nous acquitter de nos responsabilités, nous avons 169 postes établis à l'intérieur du programme à l'échelle nationale.

La GRC assure des services d'expert dans différents domaines de responsabilité, par exemple, enquêtes criminelles sur des infractions en matière de sécurité nationale, cueillette et examen de renseignements au sujet de menaces et de personnes et de biens de dignitaires canadiens et étrangers, de diplomates et d'employés consulaires, travail de liaison avec le SCRS et d'autres organes et administration d'un programme d'évaluation des menaces à l'appui de nos opérations de protection. Les évaluations de menaces servent à la détermination du niveau de sécurité physique approprié requis.

En 1996, la GRC a amélioré sa capacité d'enquête en matière de sécurité nationale aux aéroports internationaux. Cette initiative a coïncidé avec la suppression du mandat de protection et de sécurité de la GRC à certains aéroports désignés. Il importe de souligner que la GRC continue d'assurer des fonctions de protection et de sécurité sous contrat aux administrations aéroportuaires où nous sommes le service de police local. Il existe des sections d'enquête en matière de sécurité nationale aux aéroports de Vancouver, Edmonton, Calgary, Winnipeg, Toronto, Ottawa, Dorval et Halifax. Les aéroports de Mirabel et de Gander, étant donné leur nouveau statut, n'ont plus de section d'enquêtes en matière de sécurité nationale. Les unités aéroportuaires sont des satellites des sections divisionnaires d'enquêtes relatives à la sécurité nationale ayant pour objet d'assurer cohésion et direction par rapport aux priorités en matière de sécurité nationale.

En vertu du paragraphe 6(1) de la Loi sur les infractions en matière de sécurité, c'est la GRC qui a la responsabilité première. Nous avons interprété cela comme voulant dire que cette responsabilité n'est pas exclusive. Comme vous l'auront dit les témoins qui nous ont précédés, cela tient compte de la composition juridictionnelle du pays et du partage des pouvoirs entre les gouvernements fédéral, provinciaux et municipaux. Il existe à l'heure actuelle dans le pays environ 65 accords de force policière à force policière entre la GRC et d'autres services de police. Ces ententes ont pour objet de préciser le rôle respectif de la GRC et des forces de police locales en cas d'incident mettant en cause la sécurité nationale.

Le paragraphe 6(2) de la Loi sur les infractions en matière de sécurité autorise le gouvernement fédéral à négocier des ententes avec les provinces et les territoires à l'égard d'une infraction visée par la loi. Comme vous l'avez déjà entendu, le solliciteur général a entrepris un examen des arrangements de gouvernement à gouvernement. Cela sera suivi par un réexamen des ententes de

police-to-police agreements. Any new or revised police-to-police agreements will continue to be consistent with the spirit and the intent of the Security Offences Act.

On the issue of international cooperation, terrorism, as everyone is aware, is a globalized phenomenon. It is a challenge that requires global solutions. Conspiracies are often hatched in one country, logistical and material support amassed in another, with the objective of carrying out an attack in a third country.

The exchange and the cementing of relationships through formal arrangements are enhanced through the RCMP's participation in various international fora and working groups. In addition, we have created several bilateral arrangements with international partners in the U.S. and the U.K., just to name a few. To facilitate our relationships internationally, we are a full participating member of Interpol. As well, we have foreign liaison officers posted to Canadian embassies and high commissions in various locations around the world, for example, London, Paris, Hong Kong, Washington, Istanbul. In fact, we have 29 liaison officers in 20 foreign postings. Our liaison officers perform a support function to Canadian police services, not just the RCMP, in criminal investigations abroad, and they facilitate the sharing of information between law enforcement agencies.

Being the neighbour of the number one target of terrorism — that is, the U.S — it creates an added responsibility to ensure that our level of readiness is adequate and to ensure an effective response to a terrorist incident. Although there has always been a high degree of cooperation between our two countries, the recent Ressam investigation highlighted the need to ensure continued cooperation. With that in mind, we have been participating in a variety of bilateral arrangements with American agencies for several years, for example, the Bilateral Consultative Group on Counterterrorism, the North East Border Regional Terrorism Taskforce, Project Northstar, Integrated Border Enforcement Teams and the Canada-U.S. Cross-border Crime Forum, just to name a few. In addition, we participate in a number of other international fora or organizations, for example, the International Association of Chiefs of Police, Counterterrorism Committees of the G8 and the Organization of American States.

From a domestic national security perspective, we are faced with several challenges. For example, the terrorist immigrant. A serious threat continues from individuals who choose to pursue homeland conflicts and use Canada as a staging ground to further criminal conspiracies to carry out terrorist acts. We are mindful of the potential for developing links between organized crime groups and terrorist organizations. However, at this time, there is no direct evidence of a symbiotic relationship between terrorists and organized crime groups in this country. There has been some evidence that organized street gangs with links to criminal extremists have provided money that is intended to support the extremist cause.

services policiers à services policiers. Toute entente de police à police nouvelle ou révisée devra continuer de cadrer avec l'esprit et l'objet de la Loi sur les infractions en matière de sécurité.

En ce qui concerne la question de la collaboration internationale, comme chacun sait, le terrorisme est un phénomène mondial. Il s'agit d'un problème qui exige des solutions mondiales. Souvent, les conspirations naîtront dans un pays, le soutien logistique et matériel sera organisé dans un autre, et l'attaque elle-même sera menée dans un troisième pays.

L'échange de données et le raffermissement de relations dans le cadre d'arrangements formels sont favorisés par la participation de la GRC à divers forums et groupes de travail internationaux. Nous avons par ailleurs négocié plusieurs arrangements bilatéraux avec des partenaires internationaux aux États-Unis et au Royaume-Uni, pour ne nommer que deux exemples. En vue de faciliter nos relations à l'échelle internationale, nous sommes un membre participant à part entière d'Interpol. Nous avons par ailleurs des officiers de liaison avec l'étranger en poste dans des ambassades canadiennes et des hauts commissariats dans divers endroits du monde, notamment à Londres, à Paris, à Hong Kong, à Washington et à Istanbul. Nous avons en fait 29 officiers de liaison en poste dans 20 missions étrangères. Nos officiers de liaison assurent un rôle de soutien aux services de police canadiens dans l'ensemble, et pas seulement à la GRC, lors d'enquêtes criminelles à l'étranger, et il facilitent l'échange de renseignements entre organismes d'application de la loi.

En tant que voisin de la première cible mondiale du terrorisme — je veux parler des États-Unis — nous avons une responsabilité accrue de veiller à ce que notre état de préparation soit adéquat et à ce que nous soyons en mesure de contrer de façon effective un incident terroriste. Même s'il y a toujours eu un degré élevé de collaboration entre nos deux pays, la récente enquête entourant l'affaire Ressam a fait ressortir la nécessité d'assurer une collaboration continue. Cela étant, nous participons depuis plusieurs années à divers arrangements bilatéraux avec des agences américaines, notamment le Groupe consultatif bilatéral de lutte contre le terrorisme, le North East Border Regional Terrorism Taskforce, le projet Northstar, les équipes intégrées de la police des frontières et le Forum canado-américain sur la criminalité transfrontalière, pour n'en citer que quelques exemples. Nous participons par ailleurs à un certain nombre de forums ou d'organisations internationales, comme par exemple l'Association internationale des chefs de police, les comités de lutte contre le terrorisme du G8 et l'Organisation des États américains.

Du point de vue de la sécurité nationale intérieure, nous sommes confrontés à plusieurs défis. Il y a, par exemple, l'immigrant terroriste: celui-ci choisit de poursuivre son action dans le cadre de conflits dans son pays d'origine et utilise le Canada comme lieu d'organisation de conspirations criminelles dans le but de mener des actions terroristes. Cette catégorie d'immigrants pose au pays de sérieuses menaces. Nous sommes sensibles à la possibilité de l'établissement de liens entre les groupes de crime organisé et les organisations terroristes. Cependant, à l'heure actuelle, il n'existe aucune preuve directe de l'existence dans ce pays d'une relation symbiotique entre terroristes et groupes du crime organisé. Il existe certaines preuves

We are cognizant that funding is the lifeblood of terrorism. In Canada, funding by and large, from our assessment, is conducted by legal means. We would become involved when criminal acts are committed or suspected in conjunction with fundraising.

There is evidence to show that criminal extremists are using technology to thwart police investigations. The use of firewalls in computer systems makes it difficult, if not impossible, to search systems to obtain evidence of criminal activity. The threat posed by chemical, biological, radiological and nuclear or CBRN weapons or, to use the American term, "weapons of mass destruction," is new and emerging. The capacity or intention by terrorist organizations to use weapons of mass destruction is presently assessed as low. However, the impact of any attack could have devastating consequences. The most notable example of such an act is the Aum Shinrikyo attack with sarin gas on the Tokyo subway system. This incident highlighted to the world that there is a new terrorist threat.

The recent example of the suspicious package received at the Department of Citizenship and Immigration office here in Ottawa clearly illustrated the challenges posed by this type of threat, even if it is eventually determined to be a hoax. Vigilance and close cooperation within a diverse group of responders are key.

Finally, with respect to challenges facing law enforcement, is the ability to protect sensitive sources of information in judicial proceedings. Section 38 of the Canada Evidence Act provides for some protection of sensitive information involving international relations, national defence, or national security. There is a reluctance to use the Canada Evidence Act where sensitive information may form a critical element of the criminal case, and if the information is withheld the case may not stand on its own. There is new legislation being proposed in the near future that will address some of the concerns by law enforcement.

Within the national security program, we have developed enforcement priorities in two categories of criminal extremism: threats that are homegrown or domestic in nature; and foreign-based or influenced. Earlier I briefly mentioned chemical, biological, radiological, nuclear or CBRN and weapons of mass destruction as one of the challenges facing enforcement. As part of the RCMP's response capability, we recognize that other agencies have developed expertise to respond to specific aspects of chemical and biological threat or incident. Therefore, we have developed partnerships that will strengthen our overall response capabilities.

que des gangs de rue organisés ayant des liens avec des extrémistes criminels ont versé de l'argent destiné à appuyer la cause extrémiste.

Nous savons que le financement est le moteur du terrorisme. Au Canada, selon nous, le financement est dans l'ensemble obtenu de façon légale. Nous intervenons lorsqu'il y a commission ou suspicion de commission d'actes criminels conjointement avec des activités de levée de fonds.

Il existe des preuves montrant que des extrémistes criminels sont en train d'utiliser la technologie pour contrecarrer les enquêtes policières. L'utilisation de pare-feu dans les systèmes informatiques rend difficile voire impossible le furetage dans les systèmes en vue d'obtenir des preuves d'activités criminelles. La menace posée par les armes chimiques, biologiques, radiologiques et nucléaires, ou armes CBRN, ou, pour emprunter l'expression américaine, «les armes de destruction massive», est nouvelle et en expansion. La capacité ou l'intention des organisations terroristes d'utiliser des armes de destruction massive sont à l'heure actuelle considérées comme faibles. Cependant, l'incidence de toute attaque pourrait avoir des conséquences dévastatrices. L'exemple le plus notable d'un tel acte est l'attaque au sarin d'Aum Shinrikyo dans le métro de Tokyo. Cet incident a mis en relief partout dans le monde l'existence d'une nouvelle menace terroriste.

Le récent exemple du colis suspect reçu au bureau du ministère de la Citoyenneté et de l'Immigration ici à Ottawa a fait clairement ressortir les défis posés par ce genre de menace, même si l'on a découvert par la suite qu'il ne s'agissait que d'une plaisanterie. La vigilance et une collaboration étroite au sein d'un groupe d'intervenants diversifié sont essentielles.

Enfin, en ce qui concerne les défis auxquels se trouvent confrontées les forces de maintien de l'ordre, il importe d'être en mesure de protéger les sources sensibles de données dans le cadre de procédures judiciaires. L'article 38 de la Loi sur la preuve au Canada offre une certaine protection aux renseignements sensibles mettant en cause des relations internationales, la défense nationale ou la sécurité nationale. L'on hésite à recourir à la Loi sur la preuve au Canada lorsque des informations sensibles peuvent constituer un élément critique d'une affaire pénale, et si les renseignements sont dissimulés, l'affaire n'aboutira peut-être pas. Une nouvelle loi traitant de certaines des préoccupations des forces de l'ordre devrait être proposée dans un proche avenir.

Dans le cadre du programme de sécurité nationale, nous avons élaboré des priorités d'exécution pour deux catégories d'extrémistes criminels: les menaces qui sont de nature intérieure ou interne, et les menaces de souche ou d'origine étrangère. J'ai mentionné un petit peu plus tôt que les armes chimiques, biologiques, radiologiques ou nucléaires ou armes CBRN et les armes de destruction massive sont l'un des défis auxquels se trouvent confrontées les forces de maintien de l'ordre. Dans le cadre de la capacité de réaction de la GRC, nous reconnaissons que d'autres organismes se sont dotés des compétences requises pour réagir à certains aspects particuliers de menaces ou d'incidents de nature chimique ou biologique. C'est ainsi que nous avons élaboré des partenariats qui viendront renforcer nos capacités d'intervention globales.

For example, we have created a criminal incident team of explosive disposal technicians and forensic identification specialists who have been trained in the area of explosive detection, mitigation and crime-scene examination. This team is part of the joint biological and chemical response team with the Department of National Defence from Canadian Forces Base Borden. In addition, we utilize the services provided by the Defence Research Establishment Suffield, Alberta, or DRES, which provides a scientific assistance in the form of research, advice and laboratory analysis.

In other areas throughout the country, our explosive disposal technicians have partnered with local hazardous material teams normally attached to local fire departments. Such is the case in the National Capital Region, where excellent efforts have been made toward enhancing the overall response capabilities to a chemical and/or biological incident. The National Capital Region first responders committee may very well be the model for the rest of the country.

To improve our first response capability, bomb technicians at a number of strategic locations have been trained in device recognition and site safeguarding. They have not been trained in threat mitigation. Also, we have provided training to our national incident commanders with respect to crisis or incident management involving chemical and biological threats.

There was some discussion earlier from the previous witnesses with respect to lawful access. In 1974, Parliament saw the need to provide law enforcement with an important tool in the prevention, investigation and prosecution of criminal offences. In amendments to the Criminal Code, law enforcement was given the authority to intercept private communications providing that strict conditions were met. For example, a judge must be satisfied that it would be in the best interests of the administration of justice to do so and that other investigative procedures have been tried and failed or are unlikely to proceed. It was necessary to show that the matter is urgent and that other means of investigation would not be practical. The conditions provided a time frame — a period not to exceed 60 days — in which law enforcement had to operate. The age of technology has increased the challenge of maintaining a lawful access capability or the ability to intercept private communications. An added challenge and a key element of lawful access is the ability to search and seize information or computer files.

New technologies are increasingly overwhelming conventional lawful access methods. It is enabling criminals to shield their activities from detection. New features create new challenges. For example, local number portability permits individuals to retain phone numbers when they change addresses. Personal communication systems, such as cellphones, paging devices or palm pilots, feature digital technology that provides an increased level of security. Communications via satellite provide the

Par exemple, nous avons créé une équipe d'intervention en cas d'incident criminel composée de spécialistes de l'enlèvement d'explosifs et de l'identité judiciaire et qui ont reçu une formation en détection d'explosifs, en atténuation des impacts et en fouille du lieu du crime. Cette équipe fait partie de l'équipe d'intervention d'urgence biologique et chimique du ministère de la Défense nationale établie à la Base des Forces canadiennes Borden. Nous recourons par ailleurs aux services assurés par le Centre de recherches pour la défense Suffield (Alberta), ou CRDS, qui offre un soutien scientifique sous forme de recherche, de conseils et d'analyses de laboratoire.

Ailleurs au pays, nos techniciens de l'enlèvement d'explosifs ont forgé des partenariats avec les équipes locales d'intervention en cas de déversement de matières dangereuses, qui sont normalement rattachées aux services de pompiers locaux. C'est le cas dans la Région de la capitale nationale, où d'excellents efforts ont été déployés en vue d'améliorer les capacités d'intervention d'ensemble en cas d'incident chimique et(ou) biologique. Le comité de première intervention de la Région de la capitale nationale pourrait fort bien servir de modèle pour le reste du pays.

Dans le but d'améliorer notre capacité d'intervention initiale, des techniciens de l'enlèvement de bombes à plusieurs endroits stratégiques ont reçu une formation en reconnaissance des dispositifs et en protection de sites. Il n'ont pas reçu de formation en matière d'atténuation des menaces. Nous avons également offert à nos commandants sur place nationaux une formation en gestion de crise ou d'incident lié à des menaces chimiques ou biologiques.

Les témoins précédents ont discuté tout à l'heure de la question de l'accès légal. En 1974, le Parlement a jugé nécessaire de fournir aux forces de maintien de l'ordre un outil important dans la prévention, la conduite des enquêtes et les poursuites liées aux infractions criminelles. Grâce à des modifications apportées au Code criminel, les forces de l'ordre se sont vues autoriser à intercepter les communications privées à condition de satisfaire à certaines conditions strictes. Par exemple, un juge doit être convaincu que ce sera dans le meilleur intérêt de l'administration de la justice et que d'autres techniques d'enquête ont été tentées, ont échoué ou seraient vouées à l'échec. Il était important de prouver que l'affaire était urgente et que d'autres moyens d'enquête ne seraient pas pratiques. Les conditions établissaient un cadre temporel — ne devant pas dépasser 60 jours — à l'intérieur duquel les forces de l'ordre devaient s'exécuter. L'âge de la technologie a augmenté le défi du maintien d'une capacité d'accès légal ou de la capacité d'intercepter des communications privées. Un défi supplémentaire, qui est un élément clé de l'accès légal, est la capacité de mener des fouilles ou des saisies de données ou fichiers informatiques.

De nouvelles technologies viennent sans cesse contrecarrer les méthodes conventionnelles d'accès légal. Elles permettent aux criminels de mettre leurs activités à l'abri de toute détection. Toutes les nouveautés créent de nouveaux défis. Par exemple, la portabilité de son numéro local permet à une personne de conserver son numéro de téléphone lorsqu'elle change d'adresse. Les systèmes de communications personnels tels les téléphones cellulaires, les téléavertisseurs et les Palm Pilot utilisent une

versatility to conduct business anywhere and the capability for systems to connect through various gateways throughout the world. As well, there is the Internet, which is being increasingly used by criminals as a means of communication in conducting criminal activity. The challenge is for law enforcement to maintain its ability to detect, prevent and prosecute those who utilize the Internet to further their criminal objectives.

To contribute to the challenge is the use of cryptography by the criminal element. Cryptography is basically a means to change text or voice into unbreakable codes. Technology has enhanced the ability to encrypt to the point where it has surpassed the ability to decrypt messages. As technologies improve, encryption products will also increasingly be used to encrypt voice conversations. There is increasing potential for cryptography to become an effective tool for criminals intent on shielding their criminal activities, such as drug trafficking, money laundering, child pornography and terrorism.

As was pointed out when we discussed CBRN as an emerging threat, the same applies to cyber-terrorism. We see it as an emerging threat. While the tactics used may very well be the same, cyber-terrorism is not the same as information warfare or high-tech cyber-crime. The factor that distinguishes one from the other is motive. An essential element of terrorism is that the actions taken against the target are intended to influence decision-makers and the decisions they take.

The impact of a threat, whether actual or real, against an electronic information system should not be restricted to the loss of life or serious damage to property. We should also consider the pressures felt by the loss of confidence in the system and in the organization's whose systems were disrupted or destroyed. Also, consideration must be given to the loss of confidence in the ability of government to effectively prevent or respond to such incidents. The disruption, corruption or unauthorized access to a system can add the same, if not greater, impact than physical damage and may have more influence on decision-makers.

Such activity can be dealt with as a crime in Canada under the Criminal Code of Canada, notwithstanding the national security dimension.

Further challenges for law enforcement in this respect, from an investigative standpoint, include cyber-crime and cyber-terrorism. These present enormous and unique challenges. As indicated, attacks can be masked in a number of ways. In the absence of a claim of responsibility in the early stages, it would be difficult to determine the nature or source of the attack. Good intelligence is critical with respect to an organization's capability and modus operandi. Given that such attacks can be conducted from relatively obscure and safe locations, prosecutions can present an even greater challenge.

technologie numérique qui assure un niveau de sécurité accru. Les communications via satellite offrent la possibilité de mener ses affaires n'importe où et la capacité de branchement de systèmes par le biais de divers portails partout dans le monde. Il y a également l'Internet, qui est de plus en plus utilisé par les criminels comme moyen de communication dans la conduite de leurs activités criminelles. Le défi pour les forces d'exécution de la loi est de maintenir leur capacité de détecter, de prévenir et de poursuivre ceux qui utilisent l'Internet à des fins criminelles.

Le défi présenté par l'utilisation de la cryptographie par l'élément criminel vient compliquer encore la situation. La cryptographie permet en gros de transformer un message écrit ou verbal en un code indéchiffrable. La technologie de l'encodage s'est perfectionnée à un point tel qu'elle l'emporte aujourd'hui sur la capacité de décrypter des messages. Au fur et à mesure de l'amélioration de la technologie, des produits d'encodage seront de plus en plus utilisés pour encoder des conversations. La cryptographie est ainsi destinée à devenir un outil efficace pour les criminels désireux de dissimuler leurs activités criminelles, comme par exemple le trafic de stupéfiants, le blanchiment d'argent, la pédopornographie et le terrorisme.

Le cyberterrorisme est, tout comme l'utilisation d'armes CBRN, une nouvelle menace. Même si les tactiques employées peuvent être les mêmes, le cyberterrorisme n'est pas la même chose que l'info-guerre ou le cybercrime de haute volée. Le facteur qui les distingue est le motif. Un élément essentiel du terrorisme est que les mesures prises contre la cible visée ont pour objet d'influencer les décisionnaires et leurs décisions.

Dans le cas d'un système d'information électronique, le concept de menace, que celle-ci soit réelle ou pas, ne devrait pas être limité à la perte de vie ou à des dommages matériels graves. Il importe également de tenir compte des pressions amenées par la perte de confiance à l'égard du système et de l'organisation dont les systèmes ont été atteints ou détruits. Il convient également d'accorder du poids à la perte de confiance à l'égard de la capacité du gouvernement de prévenir ou de contenir efficacement de tels incidents. Le démantèlement ou la corruption ou l'accès non autorisé à un système peut avoir une incidence équivalente, voire même supérieure, à celle des dommages physiques et pourrait même exercer une plus grande influence sur les décisionnaires.

De telles activités doivent être traitées comme étant des crimes au Canada en vertu du Code criminel, nonobstant la dimension sécurité nationale.

D'autres défis pour les forces de l'ordre, du point de vue enquête, sont le cybercrime et le cyberterrorisme. Il s'agit là de défis énormes et uniques. Comme je l'ai dit, les attaques peuvent être masquées de diverses façons. En absence d'une revendication de responsabilité aux premières étapes, il est difficile de déterminer la nature ou la source de l'attaque. L'accès à des renseignements fiables est essentiel en ce qui concerne la capacité et le modus operandi d'une organisation. Étant donné que de telles attaques peuvent être menées à partir d'endroits relativement obscurs et sûrs, la poursuite des responsables peut poser un défi encore plus grand.

The RCMP has developed a critical incident program that was approved by our senior executive to ensure that the RCMP was continually in a proper state of readiness to deal with critical incidents. We recognize that training is a key component to developing an effective response capability. Subsequently, we have trained to a high level a select group of national commanders who would be given command responsibility in the event of a critical incident in Canada. Their training has given them extensive exposure to the national counterterrorism plan, Canadian forces directives, the Security Offences Act and subsequent police-to-police agreements.

One of the primary forms of training is scenario-based exercises. As you heard earlier from a previous witness with respect to the operational readiness program, the RCMP participates actively in that program. The incident commanders also participate as observers in serious incidents, both nationally and internationally. We have expanded the critical incident program to include commanders from other police forces and agencies.

In conclusion, the RCMP takes its responsibility for national security very seriously. We are committed to ensuring that we fulfil our mandate. However, it is essential to understand that the protection of our national security is a multi-agency responsibility. We can only accomplish our objectives through a cooperative approach in areas such as the sharing of information, intelligence and training. As you have seen from my presentation, this occurs both nationally and internationally.

That concludes my formal presentation. I would be pleased to respond to any questions.

Senator Banks: My first question is somewhat rhetorical: Why did we not catch Mr. Ressam? The RCMP had knowledge of him. The security people had been watching him, and here he is driving around our country with a bomb in his car. The Americans caught him. Is that okay? Did we slip up? Should we have or could we have stopped him? Did he not do anything actually illegal until he got to the border? Obviously, he did, he was driving around with a bomb in his car. As I said, it is a rhetorical question, but I am sure you understand the thrust of it because I am getting at the whole question: Can we catch people like that? Are we doing okay? At times are we looking like fools, as I think we might have in that case at least to the uninformed who do not know the circumstances? Are we happy with that situation?

Supt. Pilgrim: Whenever we have a situation such as the Ressam incident, and there are individuals who are planning or staging criminal activity in Canada, of course we are not happy with that. There is a reluctance to get into the specifics of the investigation, but Mr. Ressam was active and lived in Montreal. We are talking about a large population base, with many places to conduct business undetected.

La GRC a élaboré un programme d'intervention lors d'un incident critique, programme qui a été approuvé par nos cadres supérieurs afin de veiller à ce que la GRC soit en permanence en mesure d'intervenir lors d'incidents majeurs. Nous reconnaissons que la formation est un élément clé d'établissement d'une capacité d'intervention efficace. En conséquence, nous avons formé à un très haut niveau un groupe sélect de commandants nationaux qui seraient chargés de la responsabilité sur place en cas d'incident grave au Canada. Leur formation les a exposés au plan national de lutte contre le terrorisme, aux directives des Forces canadiennes, à la Loi sur les infractions en matière de sécurité et aux ententes entre services de police élaborés en conséquence.

L'un des principaux outils de formation est la tenue d'exercices fondés sur des scénarios. Comme un témoin précédent vous l'a déjà dit, la GRC participe activement au programme de préparation opérationnelle. Les commandants sur place participent en tant qu'observateurs lors d'incidents graves, tant à l'échelle nationale qu'à l'échelle internationale. Nous avons élargi le programme d'intervention lors d'un incident critique pour englober les commandants d'autres forces policières et organismes d'intervention.

En conclusion, la GRC prend très au sérieux sa responsabilité à l'égard de la sécurité nationale. Nous nous sommes engagés à exécuter notre mandat. Il est cependant essentiel de comprendre que la protection de la sécurité nationale est une responsabilité partagée. Nous ne pourrons réaliser nos objectifs que s'il y a collaboration sur divers plans, notamment échange d'informations, renseignements et formation. Comme vous l'aurez constaté, cette collaboration doit se faire à l'échelle et nationale et internationale.

Voilà qui met fin à mon exposé formel. Je me ferai maintenant un plaisir de répondre à vos questions.

Le sénateur Banks: Ma première question est quelque peu rhétorique: pourquoi n'a-t-on pas mis le grappin sur M. Ressam? La GRC le connaissait. Les gens du service de sécurité le surveillaient et voilà qu'il sillonnait le pays avec une bombe dans sa voiture. Les Américains l'ont arrêté. Est-ce bien? Nous sommes-nous trompés? Aurions-nous dû ou aurions-nous pu l'arrêter? Le problème était-il qu'il n'avait en vérité pas commis d'acte illégal avant d'arriver à la frontière? Mais si, puisqu'il se promenait avec une bombe dans sa voiture. Comme je le disais, c'est une question rhétorique, mais je suis certain que vous comprenez à quoi je veux en venir: Pouvons-nous arrêter des gens comme cela? Faisons-nous correctement notre travail? Nous avons parfois l'air idiot, et je pense que c'était peut-être le cas cette fois-ci, en tout cas aux yeux des profanes qui n'étaient pas au courant des circonstances? Sommes-nous heureux de la situation?

Le surintendant Pilgrim: Chaque fois qu'il y a une situation comme l'affaire Ressam et qu'il y a des personnes qui planifient ou qui organisent des activités criminelles au Canada, il est évident que nous n'en sommes pas heureux. Il y a une hésitation à aborder le détail de l'enquête, mais M. Ressam était actif et vivait à Montréal. Nous parlons d'un gros bassin de population avec quantité d'endroits où mener des activités sans être repéré.

There is some evidence that the authorities were aware of his presence in Canada, but obviously, from the chain of events, there was no evidence to indicate what his particular plans were at that time. We are fortunate that the American authorities apprehended him as he was crossing into the U.S.

More generally, procedures are in place to work with the other law enforcement agencies. The Canadian Security Intelligence Service is charged with identifying individuals who may pose a threat to Canada and our national security or to other areas, and the exchange of information and intelligence is in place to ensure that those agencies that have a requirement to be aware of certain activities are made aware of those activities in a timely fashion.

You will be hearing from my CSIS counterparts that there are a number of individuals who have been identified by the service and where the RCMP has become, in some cases, involved at various stages and to varying degrees, resulting in the apprehension or the disruption of activities. In some cases, through the immigration process, they have been deported from Canada.

Senator Banks: Was Mr. Ressam an unusual case? Are we being assiduous enough? Are there impediments in the way of your apprehending persons such as Mr. Ressam? I am only using his example because it is such a glaring one.

Must we assume that there are fairly large numbers of people in the country, like Mr. Ressam, about whom we know little or who have not raised their profile enough, who are engaged in activities about which we can do nothing, because they do not have a high enough profile? Are we not sure they have bought materials to make the bombs with; is that the case?

Supt. Pilgrim: First of all, for the RCMP involvement, we must have a criminal activity or suspicion of a criminal activity to become involved.

Senator Banks: Such as a bomb?

Supt. Pilgrim: We must have the information or intelligence that that is the activity. Short of that information, in many cases it is difficult for us to determine what is happening.

Senator Banks: In that particular case, do you know or can you disclose whether we had any such information?

Supt. Pilgrim: I can tell you that we were not aware of the conspiracy to develop a bomb prior to the arrest.

Senator Banks: I think you were in the room when we were talking about the lawful access to mail. You have referred to that in your presentation, also. I commend your attention to the fact that mail, over a certain size and weight, is opened apparently with great frequency at the request of various security services,

Il existe certaines preuves que les autorités étaient au courant de sa présence au Canada, mais il ressort clairement de la chaîne d'événements qu'il n'y avait aucun élément de preuve quant au plan particulier qu'il échafaudait à l'époque. Nous avons eu de la chance que les autorités américaines aient pu l'arrêter alors qu'il traversait la frontière pour se rendre aux États-Unis.

De façon plus générale, il y a en place des procédures en vue de travailler avec les autres agences d'exécution de la loi. Le Service canadien du renseignement de sécurité est chargé d'identifier les personnes susceptibles de poser une menace pour le Canada et pour notre sécurité nationale ou pour d'autres endroits du globe, et le mécanisme d'échange d'informations et de renseignements sont en place pour veiller à ce que ces agences qui ont pour obligation d'être au courant de certaines activités y soient sensibilisées rapidement.

Mes homologues au SCRS, que vous allez recevoir, vont vous expliquer qu'il y a un certain nombre de personnes qui ont été identifiées par le service, ensuite de quoi la GRC est dans certains cas intervenue à différentes étapes et à différents degrés, le tout débouchant sur l'arrestation des intéressés ou sur le démantèlement de leurs activités. Dans certains cas, grâce au processus d'immigration, ces éléments ont été expulsés du Canada.

Le sénateur Banks: Le cas de M. Ressam était-il très différent? Sommes-nous suffisamment assidus? Y a-t-il des entraves quant à la façon dont vous pouvez appréhender des personnes comme M. Ressam? Je le cite en tant qu'exemple tout simplement parce que son cas est flagrant.

Doit-on penser qu'il y a au pays un nombre important de personnes comme M. Ressam, dont nous ne savons que peu de choses ou qui ne se sont pas suffisamment connaître et qui s'adonnent à des activités auxquelles nous ne pouvons rien parce que nous ne sommes pas suffisamment au courant? Est-ce parce que nous n'avons pas la certitude qu'elles ont apporté avec elles le matériel nécessaire à la fabrication de bombes?

Le surintendant Pilgrim: Premièrement, en ce qui concerne la participation de la GRC, il faut qu'il y ait activité criminelle ou suspicion d'activité criminelle pour que nous intervenions.

Le sénateur Banks: Comme par exemple une bombe?

Le surintendant Pilgrim: Il nous faut disposer d'informations ou de renseignements selon lesquels il y a une telle activité. Faute de cela, dans bien des cas il est difficile pour nous de déterminer ce qui se passe.

Le sénateur Banks: Dans le cas précis que j'ai évoqué, savez-vous ou pouvez-vous nous dire si l'on disposait de pareils renseignements?

Le surintendant Pilgrim: Je peux vous dire que nous n'étions pas au courant de la conspiration visant la construction d'une bombe avant l'arrestation.

Le sénateur Banks: Je pense que vous étiez dans la salle lorsque nous avons parlé de l'accès légal au courrier. Vous avez vous aussi fait état de cela dans votre exposé. J'aimerais porter à votre attention le fait que tout envoi postal supérieur à une certaine taille et un certain poids est apparemment souvent ouvert

the RCMP being one, without court authority. Pieces of mail above a certain weight and/or size can be opened when and if CSIS, Canadian Customs and Revenue Agency or the RCMP thinks that there might be something that ought to be seen.

Are you comfortable that when that is done at your behest it is only done when you have really solid reasons? Bear in mind that I am only asking you now about those instances in which a court's acquiescence is not required, where you can do this without asking a judge. Are you confident that we are being careful? I am asking this question for two reasons: first, regarding the protection of privacy; and, second, as you know better than I, if we are not careful, then an otherwise successful prosecution against a person who is unquestionably guilty of a crime or of contemplating one might fail because of an improper procedure before the fact.

Are we sufficiently careful in that regard?

Supt. Pilgrim: My immediate response is yes, and for the reasons that you outlined. When we either conduct a search ourselves or request another agency to do so, we have to do so based on the principle of reasonable and probable grounds, and also knowing that it will have to stand up to the scrutiny of the court systems at some point in time. It is important that we do not jeopardize the eventual prosecution of a particular case for a fishing trip, for example.

Senator Banks: That is precisely the reason I am asking the question. You have to have reasonable or probable cause in order to ask a judge to open an ordinary envelope that could contain a letter. However, the test is less stringent for a package. Without an x-ray which shows something illegal, if it just contains paper — although that could be a part of a criminal activity — you have no way of having reasonable or probable cause to think that a package might contain something illegal. The only indication is that it is from or addressed to a person of interest. The test for when it is proper to open larger mail is less stringent, as I am sure you know better than I, than for opening an ordinary letter, which can only be done with the approval of a judge, and in the presence of either the recipient or the sender. That test does not apply to a package, and it is in that circumstance that I ask you the question.

Supt. Pilgrim: From a police perspective, the size of the package is immaterial. In order for us to open any package, we require a court order. We have to have a warrant.

Senator Banks: That is not so.

Supt. Pilgrim: The RCMP must. I understand that Canada Customs, Canada Post and courier companies have authority to inspect packages that are suspicious in nature, or with regard to which there is information to indicate that they may pose a threat. Canada Customs works on a set of guidelines with which I am not

à la demande de divers services de sécurité, dont la GRC, sans qu'il y ait eu au préalable obtention d'une autorisation de la cour. Les articles de courrier qui dépassent un certain poids et(ou) une certaine taille peuvent être ouverts si et quand le SCRS, l'Agence des douanes et du revenu du Canada ou la GRC pense qu'il y aurait peut-être lieu de jeter un coup d'oeil sur le contenu.

Cela vous satisfait-il que ce ne soit fait que sur votre ordre lorsque vous avez des motifs vraiment solides? N'oubliez pas que je ne m'intéresse ici qu'aux cas pour lesquels l'autorisation de la cour n'est pas requise, lorsque vous pouvez aller de l'avant sans faire appel à un juge. Êtes-vous convaincu que nous sommes suffisamment prudents? Je vous pose la question pour deux raisons: premièrement, dans le contexte de la protection de la vie privée; deuxièmement, et vous le savez mieux que moi, si nous ne sommes pas prudents, alors le procès d'une personne qui est indéniablement coupable d'avoir commis un crime ou de l'avoir envisagé pourrait échoué, faute d'avoir suivi la procédure établie.

Sommes-nous suffisamment prudents à cet égard?

Le surintendant Pilgrim: Ma réponse immédiate serait que oui, et ce pour les raisons que vous évoquez. Lorsque nous menons nous-mêmes une perquisition ou demandons à une autre agence de le faire, nous le faisons sur la base de motifs raisonnables et probables, et avec la conviction que cela devra résister à l'examen minutieux qui en sera fait à un moment donné dans le cadre du système judiciaire. Il est important que nous ne compromettions pas la poursuite éventuelle d'une affaire donnée pour une expédition de pêche, par exemple.

Le sénateur Banks: C'est précisément ce pour quoi je pose la question. Il vous faut avoir une cause raisonnable ou probable pour pouvoir demander à un juge l'autorisation d'ouvrir une simple enveloppe qui pourrait contenir une lettre. Cependant, le critère est moins exigeant en ce qui concerne les colis. Sans une radio qui vous montre quelque chose d'illégal, si le paquet ne renferme que des papiers — même si cela pourrait relever d'une activité criminelle — vous ne disposez d'aucun moyen d'avoir un motif raisonnable ou probable de penser que le paquet pourrait contenir quelque chose d'illégal. Votre seul indice est qu'il a été envoyé par ou à une personne d'intérêt. Le critère quant à l'ouverture d'envois postaux plus gros est moins exigeant, comme vous le savez, j'en suis sûr, mieux que moi, que pour les simples lettres, qui ne peuvent être ouvertes qu'avec l'autorisation d'un juge et en la présence ou du destinataire ou de l'expéditeur. Ce même critère ne s'applique pas aux colis, et c'est sur cette catégorie d'envois postaux que porte ma question.

Le surintendant Pilgrim: Du point de vue de la police, peu importe la taille du paquet. Il nous faut, pour pouvoir ouvrir un envoi, quel qu'il soit, une ordonnance de la cour. Il nous faut avoir un mandat.

Le sénateur Banks: Ce n'est pas vrai.

Le surintendant Pilgrim: C'est le cas pour la GRC. Si j'ai bien compris, Douanes Canada, Postes Canada et les services de messagerie sont autorisés à inspecter les paquets d'apparence suspecte ou pour lesquels il y a des renseignements indiquant qu'ils pourraient poser une menace. Douanes Canada doit se

totally familiar. However, they have specific authority to inspect goods and items coming into the country.

From a policing perspective, we require a search warrant to open packages that are going through the mail or are seized in other circumstances.

Senator Banks: I believe I recall the Canadian Customs and Revenue Agency having told us that they sometimes open packages without a court order at the request of the RCMP. Would you check on that and let us know, please?

Supt. Pilgrim: Yes, I definitely will.

Senator Cordy: Welcome to our meeting. In my other life, I was a teacher in Cole Harbour, so I know the area well.

Could you clarify the term "cyber-terrorism"?

Supt. Pilgrim: That is a difficult one. I have participated in various discussions, nationally and internationally, where defining cyber-terrorism has been on the table.There is reluctance to define terrorism, per se, and even more to define specific aspects such as cyber-terrorism.

Situations in which information systems or critical infrastructures are threatened through the use of computer systems is probably the best definition I could give you. Again, let us not forget the motive, which is to change policy or influence decision-makers. It is not traditional a criminal activity for which greed is usually the underlying motive. It is committed more with the intent of changing policy decisions and influencing decision-makers.

Senator Cordy: With regard to influencing decision-makers, the previous speaker this morning talked about terrorist fundraising and laundering the funds raised so that they would appear legitimate. Does the criminal element, in an organized way, try to legitimize affecting decision-makers or lawmakers?

Supt. Pilgrim: Are you talking about traditional criminal organized groups at present?

Senator Cordy: Yes, organized crime groups.

Supt. Pilgrim: Organized crime groups use different methods to cover the means by which those proceeds were obtained. We have proceeds of crime legislation that helps us deal with some of those issues.

With respect to using those proceeds to influence decision-makers, there is always the potential that organized crime groups may attempt to influence decision-makers to be more relaxed with respect to certain legislation with regard to criminal organizations so that they are freer to carry on business as they choose.

conformer à un ensemble de lignes directrices que je ne connais pas à fond. Le service des douanes est en tout cas autorisé à inspecter les produits et les articles qui arrivent au pays.

En ce qui concerne la police, il nous faut un mandat de perquisition pour pouvoir ouvrir un paquet qui passe par le courrier ou qui a été saisi dans d'autres circonstances.

Le sénateur Banks: Je pense me souvenir que l'Agence des douanes et du revenu du Canada nous a dit qu'il lui arrive d'ouvrir des paquets sans ordonnance de la cour à la demande de la GRC. Pourriez-vous s'il vous plaît vérifier et nous communiquer la réponse?

Le surintendant Pilgrim: Oui, absolument.

Le sénateur Cordy: Bienvenue à notre réunion. Dans mon autre vie, j'étais enseignante à Cole Harbour, alors je connais bien la région.

Pourriez-vous expliquer ce que vous entendez par «cyberterrorisme»?

Le surintendant Pilgrim: C'est là une question difficile. J'ai participé à diverses discussions, nationales et internationales, au cours desquelles il a été question de définir ce qu'est le cyberterrorisme. Il y a une certaine hésitation à définir le terrorisme tout court, sans parler de variantes précises comme le cyberterrorisme.

La meilleure définition que je peux sans doute vous donner est qu'il s'agit de situations dans lesquelles des systèmes d'information ou des infrastructures essentielles sont menacés par l'utilisation de systèmes informatiques. Encore une fois, n'oublions pas le motif, qui est de faire changer des politiques ou d'influencer les décideurs. Il ne s'agit pas d'une activité criminelle traditionnelle dont le motif sous-jacent est en règle générale l'argent. L'intention ici sera plutôt de faire changer des décisions politiques et d'exercer une influence auprès des décideurs politiques.

Le sénateur Cordy: Pour ce qui est de l'idée d'influencer les décideurs, le témoin qui vous a précédé ce matin a parlé de levées de fonds organisées par des mouvements terroristes et de blanchiment de l'argent ainsi ramassé dans le but de présenter un visage légitime. L'élément criminel s'efforce-t-il de façon organisée à légitimiser l'influence qu'il tente d'exercer auprès des décideurs et des législateurs?

Le surintendant Pilgrim: Voulez-vous parler des groupes traditionnels du crime organisé?

Le sénateur Cordy: Oui, des groupes du crime organisé.

Le surintendant Pilgrim: Les groupes du crime organisé utilisent différentes méthodes pour couvrir les moyens grâce auxquels leurs fonds ont été obtenus. Nous avons des lois sur le produit de la criminalité qui nous aident à traiter de certaines de ces questions.

Quant à l'utilisation du produit de la criminalité pour influencer des décideurs, il existe toujours la possibilité que des groupes du crime organisé tentent d'inciter des décideurs à relâcher certaines contraintes législatives afin que les organisations criminelles soient plus libres de mener leurs affaires comme elles l'entendent.

Senator Cordy: Unbeknownst to the lawmakers, would they try to affect them in terms of political goals of terrorist groups?

Supt. Pilgrim: For the most part, criminal organizations are considered exactly that — criminal organizations, with an objective of obtaining proceeds through criminal activity. Although I have no specific details, there have been some public discussions with respect to some organized crime groups attempting to influence various Canadian establishments.

Senator Cordy: If the RCMP were aware of an organized attempt by a group to affect lawmakers, would the lawmakers be notified that this was happening?

Supt. Pilgrim: Yes, there is a process in place to advise and inform lawmakers and other officials when there is a potential for threat, influence, corruption or intimidation.

Senator Wiebe: Superintendent Pilgrim, I appreciated very much your presentation this morning. Throughout it you talked to us about the challenges that are facing the force throughout Canada. I just want to emphasize the word "resources." Given the resources at the disposal of the RCMP, I think that you are doing an outstanding job on behalf of the people of Canada.

However, I do have a very serious concern, especially when it comes to organized crime. Money is not a problem as far as they are concerned. They have the wealth. They are moving into legal enterprises. They are able to afford the technical expertise to hire the individuals through these legal companies. Some of these individuals may not even know that they are using that technology for organized crime. That technology is changing rapidly each and every day, even as we speak.

I am very much afraid that we are not, as a government or as a society, providing our police forces with the resources and the tools to be able to combat that kind of wealth. Is there anything that you could tell me to reassure me that those financial resources are there?

Second, I am a strong believer in a visible presence for the force throughout Canada. Are we sometimes sacrificing manpower in order to be able to afford the technology that is required to combat organized crime?

Supt. Pilgrim: The issue with resources, of course, as you very well know, is a never-ending story. With respect, there has been a need for more resources identified to government. The government, through the integrity funding process, has recognized this need. Last year there was $15 million allocated, and this year there is an additional $25 million allocated with respect to integrity funding. That is in the area of organized crime.

We are constantly assessing the degree of the threat and resetting our priorities with respect to organized crime. There is

Le sénateur Cordy: Est-ce que ces groupes terroristes essaieraient, à l'insu du législateur, de l'influencer dans le sens de leurs propres objectifs politiques?

Le surintendant Pilgrim: Les organisations criminelles sont pour la plupart exactement cela, soit des organisations criminelles dont le but est d'obtenir de l'argent au moyen d'activités criminelles. Je n'en ai pas de détails précis, mais il y a eu certaines discussions publiques au sujet de groupes du crime organisé ayant tenté d'exercer une influence auprès de différents milieux dirigeants canadiens.

Le sénateur Cordy: Si la GRC était au courant d'une tentative d'un groupe criminel organisé d'influencer le législateur, ce dernier en serait-il averti?

Le surintendant Pilgrim: Oui, il y a en place un processus destiné à conseiller et à avertir les législateurs et autres décideurs lorsqu'il y a risque de menace, de trafic d'influence, de corruption ou d'intimidation.

Le sénateur Wiebe: Surintendant Pilgrim, j'ai beaucoup apprécié votre exposé ce matin. Vous nous avez longuement entretenu des défis auxquels se trouve confrontée la GRC partout au pays. J'aimerais insister sur le mot «ressources». Étant donné les ressources à la disposition de la GRC, je pense que vous faites un travail remarquable pour le compte des Canadiens.

J'ai cependant une très grave préoccupation, surtout en ce qui concerne le crime organisé. L'argent n'est pas un problème pour les gens du milieu. Ils sont riches. Ils s'installent dans des entreprises légales. Ils ont les moyens, grâce à ces entreprises légales, d'embaucher les personnes qui ont les compétences techniques requises. Certains de ces employés ne savent peut-être même pas que leur patron utilise ces technologies pour le crime organisé. La technologie est en évolution constante, jour après jour; elle est en ce moment même en train de changer.

Ma grande crainte est que nous, c'est-à-dire le gouvernement et la société, ne donnions pas à nos forces de police les ressources et les outils dont elles ont besoin pour pouvoir combattre ce degré de richesse. Êtes-vous en mesure de me rassurer et de me dire que ces ressources financières sont là?

Deuxièmement, je crois fermement dans l'importance d'une présence visible de la force partout au pays. Arrive-t-il que l'on sacrifie la main-d'oeuvre afin de pouvoir nous doter de la technologie qui est requise pour combattre le crime organisé?

Le surintendant Pilgrim: La question des ressources est, bien sûr, comme vous le savez très bien, une histoire sans fin. Sauf le respect que je vous dois, le gouvernement a été saisi de notre besoin de disposer de plus de ressources. Le gouvernement, par le biais du processus de financement de la lutte contre la corruption, a reconnu ce besoin. L'an dernier, il y a eu une allocation de 15 millions de dollars, et cette année 25 millions de dollars supplémentaires ont été réservés à cette fin. Voilà ce qui a été fait relativement au crime organisé.

Nous réévaluons constamment le degré de la menace et réagençons nos priorités relativement au crime organisé en

always the option to deploy or re-deploy resources and/or return to government and request additional resources.

The threat is not the traditional national security threat. It is an area that is somewhat outside of my particular area of responsibility as it now stands. However, there are some linkages between my area from a national security perspective and the organized crime side of things because, as I stated earlier, some of the groups that are involved in some criminal activity, whether it is credit card fraud or fraudulent documents, impact the national security side. When we get into some of these issues, there is a potential danger to affect the economic security as well.

With respect to the technical requirements, with the advance of technology and with the new means for criminals to carry out their activity, the added challenges and the added demands are on the police to detect, disrupt, apprehend and prosecute. Without the equivalent technical means to perform those duties, the task is increasingly more difficult.

The short answer is yes, we always need resources. Coupled with that, we need to ensure that the resources that we have are effectively deployed commensurate with the threat and with the challenges that the criminal activity or the organized crime are posing to Canada.

Senator Wiebe: This is a problem in our society, and in all societies throughout the world, that we have never had to face previously. There is a completely new kind of speed in the ability to finalize the criminal act as far as the criminal is concerned. It makes it that much more difficult to try to detect that something may be going on. It may require that governments must provide the resources to address this threat.

As you know, I sit on the government side of the Senate and have always felt strongly that we are not providing the tools that are required to do the job. If we are not careful, we could lose that battle.

Supt. Pilgrim: The issue of globalization of technology was mentioned earlier this morning. Technology breaks down those traditional borders and jurisdictions that we depend on to contain some of these activities and provide us with a little more advantage. However, as I pointed out, one could conduct criminal activity sitting in a basement or office in any part of the world.

Senator Wiebe: You could commit a criminal activity while in a boat in the middle of a lake while you are fishing.

Supt. Pilgrim: That is right.

Senator Forrestall: I will follow up on Senator Wiebe's observations. Additional funds in the amount of $15 million last year and $25 million this year were provided. What amount do you expect next year?

conséquence. Il y a toujours la possibilité de déployer ou de redéployer des ressources et(ou) de retourner voir le gouvernement pour demander des ressources supplémentaires.

La menace dont on parle n'est pas une menace traditionnelle à la sécurité nationale. Il s'agit d'un volet qui s'inscrit quelque peu à l'extérieur de mes responsabilités actuelles. Il y a cependant certains liens entre mon secteur, du point de vue sécurité nationale et l'aspect crime organisé car, comme je l'ai dit tout à l'heure, certains des groupes qui s'adonnent à des activités criminelles, qu'il s'agisse de cartes de crédit ou d'autres documents frauduleux, ont une incidence sur le volet sécurité nationale. Et lorsqu'on se lance dans certaines de ces questions, il y a toujours un risque potentiel pour la sécurité économique également.

En ce qui concerne les besoins techniques, avec l'évolution technologique et les nouveaux moyens dont disposent les criminels pour mener leurs activités, la police est assujettie à de nouveaux défis et à de nouvelles exigences en vue de détecter, de démanteler, d'arrêter et de poursuivre. En l'absence de moyens techniques équivalents lui permettant de mener à bien ces responsabilités, la tâche est de plus en plus ardue.

La courte réponse, donc, est que oui, nous avons toujours besoin de ressources. Il nous faut également veiller à ce que les ressources dont nous disposons soient déployées de façon effective dans le contexte de la menace et des défis posés par l'activité criminelle ou par le crime organisé au Canada.

Le sénateur Wiebe: C'est un problème auquel notre société et toutes les sociétés du monde n'avaient jamais auparavant été confrontées. Aujourd'hui, le criminel peut finaliser son acte criminel à une vitesse jusqu'ici jamais vue. Il est ainsi de plus en plus difficile de détecter le fait qu'il se passe peut-être quelque chose. Les gouvernements devront peut-être fournir les ressources nécessaires pour contrer cette menace.

Comme vous le savez, je siège au Sénat du côté du parti au pouvoir et j'ai toujours eu la ferme conviction que nous ne fournissions pas les outils requis pour faire le travail. Si nous ne faisons pas attention, nous pourrions perdre la bataille.

Le surintendant Pilgrim: La question de la mondialisation de la technologie a été mentionnée plus tôt ce matin. La technologie abat les frontières traditionnelles sur lesquelles nous comptons pour contenir certaines de ces activités et nous assurer un certain avantage. Cependant, comme je l'ai souligné, une personne peut mener des activités criminelles à partir d'un sous-sol ou d'un bureau n'importe où dans le monde.

Le sénateur Wiebe: Vous pourriez commettre une activité criminelle pendant que vous pêchez à bord d'un bateau au beau milieu d'un lac.

Le surintendant Pilgrim: C'est exact.

Le sénateur Forrestall: J'aimerais enchaîner sur les observations du sénateur Wiebe. Des fonds supplémentaires de 15 millions de dollars l'an dernier et de 25 millions de dollars cette année ont été versés. À quel montant d'argent vous attendez-vous pour l'an prochain?

Does lack of knowledge of the exact amount of money that will be forthcoming lead to proper long term planning? Would it not be better if the amount were set somewhere, so that it was a natural annual increment that you could plan on?

Supt. Pilgrim: There is a process of which you are aware. There is a traditional budgetary process to identify needs for the upcoming fiscal period. In addition to that, there are usually ongoing discussions with respect to specific projects, initiatives and priorities of government, whether it is organized crime or another matter, to address those more on a case-by-case or on an individual basis. I do not have the specifics of that process. However, traditionally it is part of an ongoing strategy. We look at it in more of a long term time frame, especially when the priorities are identified. It is part of that annual strategic planning cycle in which the RCMP, like other agencies of government, are actively involved.

Senator Forrestall: I have been concerned particularly about comments from the United States and other jurisdictions that Canada is the back door to the United States for terrorists. I love tourism promotion. I love when people come to beautiful Nova Scotia. We want all the good publicity we can get. It is a form of disservice to suggest, internationally or globally, that a terrorist wanting to enter the U.S. should try Canada because it is the easiest door. That simply promotes Canada as an easy entryway to the United States. I do not want that kind of trans-traffic.

Does it bother the RCMP to have to live with this kind of comment? Does it bother you that we have this kind of inappropriate promotion?

Supt. Pilgrim: It goes to the question that was asked earlier about Canada being perceived as a safe haven. We have always maintained, within the community, that Canada is not a safe haven. I think you will hear that same comment from our CSIS colleagues when they appear before the committee. There have been numerous occasions when, as I mentioned earlier, individuals have been apprehended and deported; they have been dealt with by the legal process, whether immigration or the courts, and deported from the country.

Again, I do not have the numbers, but those examples demonstrate that we are not necessarily a safe haven; there is always the chance that such individuals would be detected and apprehended. We are a democratic society, and so we provide certain opportunities that many people in other parts of the world do not enjoy. With our system of society, we have an immigration process that invites people into the country.

At the same time it is hoped that, through the necessary screening process, we can balance the process so that we do not experience large numbers of undesirables entering Canada. When

Le fait que vous ne connaissiez pas le montant d'argent exact qui vous sera versé entrave-t-il votre planification à long terme? Ne serait-il pas préférable que le montant soit fixé quelque part afin que vous puissiez compter sur une augmentation annuelle régulière?

Le surintendant Pilgrim: Il y a en place un processus dont vous êtes au courant. Il existe un processus budgétaire traditionnel destiné à déterminer les besoins pour l'exercice financier à venir. Il y a par ailleurs en règle générale des discussions permanentes quant aux projets, initiatives et priorités particulières du gouvernement, qu'il s'agisse de la lutte contre le crime organisé ou d'autres choses, ce dans le but d'examiner les différentes rubriques davantage au cas par cas. Je n'ai pas le détail du processus. Cependant, traditionnellement, cela s'inscrit dans une stratégie permanente. Nous envisageons nos activités dans un contexte à plus long terme, surtout en ce qui concerne les priorités. Cela fait partie d'un cycle de planification stratégique annuelle auquel participe activement la GRC, comme tous les autres organes du gouvernement.

Le sénateur Forrestall: Je suis particulièrement préoccupé par des observations faites par les États-Unis et par d'autres pays et selon lesquelles le Canada serait la porte d'entrée arrière aux États-Unis pour les terroristes. J'adore la promotion du tourisme. J'adore cela lorsque les gens viennent dans notre belle province de la Nouvelle-Écosse. Nous voulons toute la bonne publicité que nous pouvons avoir. Mais cela nous nuit lorsqu'il est dit dans le monde qu'un terroriste désireux d'entrer aux États-Unis devrait s'essayer au Canada parce que c'est la porte la plus facile par laquelle pénétrer. C'est ainsi que l'on fait la promotion du Canada comme porte d'accès facile aux États-Unis. Ce genre de trafic transitoire ne m'intéresse pas.

Cela ennuie-t-il la GRC d'entendre ce genre de commentaires? Cela vous ennuie-t-il que le pays fasse l'objet de ce genre de promotion malencontreuse?

Le surintendant Pilgrim: Cela nous ramène à la question posée tout à l'heure relativement à la perception qu'ont certains que le Canada est un lieu de refuge sûr. Nous avons toujours maintenu, au sein de la communauté, que le Canada n'est pas un refuge sûr. Je pense que nos collègues du SCRS vous diront la même chose lorsqu'ils comparaîtront devant le comité. Il y a eu de nombreux cas, comme je l'ai mentionné tout à l'heure, de personnes qui ont été arrêtées et expulsées; on les a assujetties au processus juridique, en passant soit par les services de l'immigration soit par les tribunaux, et on les expulsées du pays.

Encore une fois, je n'ai pas les chiffres, mais ces exemples sont la preuve que nous ne sommes pas forcément un refuge sûr; il y a toujours la possibilité que ces personnes soient repérées et arrêtées. Nous sommes une société démocratique et nous offrons donc certaines possibilités dont les habitants d'autres parties du monde ne jouissent pas. Avec notre système de société, nous avons un processus d'immigration qui invite les gens à venir au pays.

En même temps, on espère, grâce au processus de sélection obligatoire, équilibrer le processus de façon à ne pas accueillir au Canada de nombres importants d'éléments indésirables. Lorsque

I say "undesirables" I am speaking strictly from a criminal perspective of those who enter the country and conduct criminal activities. However, the potential always exists for these things to happen with the current system and process that are in place.

Senator Forrestall: I appreciate your response. It is my understanding that, in recent years in particular, there has been growing evidence of surveillance of your side of this constant war by the criminal element — from biker gangs to the Russian mafia — anywhere you look. To what extent is this happening? Are you confident that you have a bit of a handle on it? Are you able to protect yourselves? The cyber-problems that we have are almost insurmountable. I do not know what we will do about it. It is the major problem that transcends rogue missiles from dissident states, in my mind, because it corrupts completely when you are denied the type of intelligence you need to serve the populace.

To what degree is surveillance of CSIS, and the particular elements in the force who are responsible for this type of work, being conducted?

Supt. Pilgrim: I cannot give you any details in respect of the degree of the surveillance, but I can speak about the RCMP. When we conduct criminal investigations, or projects in respect of criminal activity, on any individual in Canada, we do so with the understanding that there is always the potential for counter-surveillance being conducted on us and on our methods of doing business.

There is some protection under the law to protect sources of information and the methods of operation. We utilize those means whenever possible. Again, we are cognizant of the fact that the potential is there, and we attempt to develop our operations in a manner that will prevent counter-surveillance and the disclosure of our activities as they relate to sources, techniques and overall means of doing business.

Senator Forrestall: Are you successful in recruiting the experts needed to deal with this level of computer technology?

Supt. Pilgrim: It appears that we are successful. From the information that I have, it appears that when we are seeking a particular expertise that we do not have in-house, then we obtain that expertise outside, either through direct recruiting or on a contract basis, whatever the case may be.

However, we have a computer crimes area within the RCMP, and we also have an area called "Infomatics" that looks at the RCMP systems. These areas also provide a pool of expertise when we deal with technology.

Senator Forrestall: Do you prefer to have in-house expertise or do you prefer to have it on a contract basis? If it is necessary, can you search as far as the U.K., for example, to find the appropriate expertise? Do you do that from time to time?

je dis «indésirables» je parle strictement de l'aspect criminalité pour ceux qui entrent au pays et y mènent des activités criminelles. Il existe cependant toujours la possibilité que ces choses arrivent dans le cadre du système et des processus en place à l'heure actuelle.

Le sénateur Forrestall: J'apprécie votre réponse. D'après ce que j'ai compris, surtout au cours des dernières années, il y a eu des preuves croissantes de surveillance de votre côté de cette guerre permanente par l'élément criminel — allant des bandes de motards à la mafia russe — et ce où que l'on regarde. Dans quelle mesure est-ce le cas? Êtes-vous convaincu que vous contrôlez un peu la chose? Êtes-vous en mesure de vous protéger? Les cyberproblèmes que nous avons sont quasi insurmontables. J'ignore ce que nous pourrons y faire. À mon sens, il s'agit là d'un problème énorme qui l'emporte sur celui des missiles d'États renégats, car il y a à mon sens une corruption totale si vous vous voyez refuser le genre de renseignements qu'il vous faut pour servir la population.

Dans quelle mesure le SCRS et les éléments particuliers de la force qui sont responsables de ce genre de travail sont-ils surveillés?

Le surintendant Pilgrim: Je ne peux pas vous donner de détails quant au degré de surveillance, mais je peux vous parler de la GRC. Lorsque nous menons des enquêtes criminelles ou des projets portant sur l'activité criminelle ou sur une personne se trouvant sur le territoire canadien, nous le faisons en connaissance de cause, c'est-à-dire en sachant qu'il est possible que nous-mêmes et nos méthodes soyons visés par des mesures de contre-surveillance.

Il existe en vertu de la loi une certaine protection des sources d'information et des méthodes de travail employées. Nous y recourons partout où cela est possible. Encore une fois, nous savons que le risque est là et nous tentons de mener nos opérations de façon à empêcher la contre-surveillance et la divulgation de nos activités en ce qui a trait à nos sources, à nos techniques et à nos méthodes de travail.

Le sénateur Forrestall: Réussissez-vous à recruter les experts dont vous avez besoin étant donné le niveau de sophistication de la technologie informatique?

Le surintendant Pilgrim: Il semble que nous réussissions. D'après les renseignements dont je dispose, il semble que lorsque nous cherchons une compétence bien précise que nous n'avons pas à l'interne, nous obtenons cette compétence à l'extérieur, soit par voie de recrutement direct soit par voie contractuelle, selon le cas.

Nous avons cependant au sein de la GRC une section spécialisée dans le crime informatique, et nous avons également un service d'informatique qui s'occupe des systèmes de la GRC. Ces services nous offrent un bassin d'experts en technologie.

Le sénateur Forrestall: Préférez-vous avoir des experts à l'interne ou passer contrat pour obtenir ces services? Si cela était nécessaire, pourriez-vous aller jusqu'au Royaume-Uni, par exemple, pour y trouver les compétences que vous recherchez? Faites-vous cela de temps en temps?

Supt. Pilgrim: Yes, there has always to be a balance of what capabilities we have internally, and economically it is not always feasible to maintain a capability internally that may not be required or called upon on a regular basis. Subsequently, there are means whereby we are involved in exchange or secondment programs as a means of exchanging information and doing business. We form part of a variety of arrangements internationally where much of this expertise is at the table; and we are able to draw upon it as required.

Senator Forrestall: Do you have enough authority to do transborder chase and pursuit of information or conduct such a surveillance? Do you feel free or hindered?

Supt. Pilgrim: There is sufficient authority to do that. It is important, in that respect, that the relationships and the protocols are in place between the RCMP and other agencies, whether domestically or internationally. Of course, when we talk about Canada and her border, the U.S. is the first country to come to mind.

It is important that we have a relationship on both sides of the border and an understanding of the respective legal requirements and issues. In that way, instead of an RCMP officer running across the border, there is a degree of confidence and trust in the counterpart on the other side of the border to ensure that the task is dealt with as required.

Senator Forrestall: On the need-to-know basis, then, is that a reciprocal arrangement?

Supt. Pilgrim: Yes.

Senator Forrestall: When you need to know something, how cooperative are our neighbours to the south? Are they good or are they indifferent?

Supt. Pilgrim: No, I would definitely not say it was indifference. Through the Ressam investigation, we saw that we have a very good level of cooperation between ourselves and our counterparts in the FBI. We also have a very good relationship with other policing agencies. Whether it is state, federal, the Drug Enforcement Agency or the Alcohol, Tobacco, Firearms Agency, we have an excellent rapport. As I mentioned earlier, we are also part of Interpol and of the International Association of Chiefs of Police. That brings to the table, of course, the opportunity to create more partnerships and to strengthen the existing ones.

Senator Forrestall: In other words, you are pretty happy with the need-to-know level under which we operate with our neighbours to the south. What about the United Kingdom and Europe?

Supt. Pilgrim: Yes. With respect to our liaison officers, we have 29 in 20 posts around the world. They add greatly to the development of our relationships with various agencies

Le surintendant Pilgrim: Oui, il y a toujours eu un équilibre dans les capacités que nous avons à l'interne, et sur le plan financier, il n'est pas toujours faisable de maintenir une capacité à l'interne qui ne sera peut-être pas requise ni utilisée de façon régulière. C'est pourquoi nous participons à des programmes d'échanges ou de détachements comme moyen d'échanger des informations et de faire affaires. Nous participons à toute une gamme de formations internationales où beaucoup de ces compétences se trouvent réunies autour de la table et nous pouvons y puiser selon nos besoins.

Le sénateur Forrestall: Avez-vous suffisamment de pouvoir pour entreprendre des poursuites, des recherches d'information et du travail de surveillance transfrontaliers? Vous sentez-vous libres ou entravés?

Le surintendant Pilgrim: Nous disposons de suffisamment de pouvoir pour faire cela. Il est important, à cet égard, que soient en place les relations et les protocoles entre la GRC et les autres agences, qu'elles soient nationales ou internationales. Bien sûr, lorsque nous parlons du Canada et de sa frontière, le premier pays qui nous vient à l'esprit est les États-Unis.

Il est important qu'il y ait de part et d'autre de la frontière une bonne relation et une compréhension des exigences et des questions juridiques respectives. Ainsi, au lieu qu'un agent de la GRC traverse le frontière en courant, il y a de l'autre côté de la frontière un degré de confiance dans la façon dont le travail va être mené.

Le sénateur Forrestall: Pour ce qui est du principe de la nécessité d'accès, donc, il existe un arrangement de réciprocité, n'est-ce pas?

Le surintendant Pilgrim: Oui.

Le sénateur Forrestall: Lorsque vous devez savoir quelque chose, dans quelle mesure nos voisins du Sud sont-ils coopératifs? Sont-ils accommodants ou bien indifférents?

Le surintendant Pilgrim: Non, je ne dirais certainement pas qu'ils sont indifférents. Grâce à l'enquête entourant l'affaire Ressam, nous avons constaté un très bon niveau de collaboration entre nous-mêmes et nos homologues de la FBI. Nous avons également eu de très bons rapports avec d'autres agences policières. Qu'il s'agisse d'agences d'État, fédérales, de la Drug Enforcement Agency ou de l'Alcohol, Tobacco, Firearms Agency, nous avons toujours eu d'excellents rapports. Comme je l'ai mentionné tout à l'heure, nous faisons également partie d'Interpol et de l'Association internationale des chefs de police. Cela nous offre bien sûr l'occasion de créer d'autres partenariats et de renforcer ceux qui existent déjà.

Le sénateur Forrestall: En d'autres termes, vous êtes plutôt heureux du niveau d'accès sélectif avec lequel nous fonctionnons avec nos voisins du Sud. Qu'en est-il du Royaume-Uni et de l'Europe?

Le surintendant Pilgrim: Oui. En ce qui concerne nos agents de liaison, nous en avons 29 en place dans 20 missions dans le monde. Ces agents contribuent grandement au développement de

internationally. That goes a long way to strengthening the partnerships that are in place.

Senator Atkins: Superintendent Pilgrim, my first question goes back to our first witness' testimony and this whole question of port security. Does the RCMP work closely with the local authorities to satisfy their concerns with regard to port activities?

Supt. Pilgrim: Yes. Depending on the nature of the activity that we are interested in, we will work hand in hand with the authority that has jurisdiction. In addition, we have other programs targeting the broader context of border integrity at our ports, be they airports, land or sea ports. We work closely, sometimes daily, with the municipal or local police, provincial police, federal agencies, according to the jurisdiction. In addition, we conduct our own criminal investigations as they relate to activities at specific locations. The short answer is yes, we have a very good working relationship with the police.

Senator Atkins: Why do we get the feeling that there are not enough resources to deal with the level of activity? For example, in the port of Montreal, there is a sense that the level of security is insufficient to protect the interests of Canadians. To what extent can our authorities investigate containers to know what is going out of this country or coming into it?

Supt. Pilgrim: I am not sure any number of resources would be able to deal with the container situation at our ports. As you can well appreciate, container shipping is a major business. Thousands and thousands of containers go through a port on any given day.

It is difficult to say that we need additional resources to deal with the problem as a whole. However, resourcing is definitely one issue with respect to policing all of our ports, air, land or sea. Port security has been identified as one of our national priorities. Strategies are being examined on the best way to address the situation. It is to be hoped that the appropriate level of resources will be dedicated to that particular challenge.

Senator Atkins: If you find a Z71 red truck, let me know, license plate "Norman."

On industrial espionage, do you have any comment on whether it is taking off or whether you feel it is under control?

Supt. Pilgrim: It is in an area on which I do not have a great deal of information. That area is being monitored and assessed on a regular basis. You may want to approach that question with our CSIS counterparts when they appear before the committee.

Senator Atkins: Yesterday we heard about the military having a difficult time keeping their numbers in terms of recruitment. Is that a problem with the RCMP or not?

nos relations avec diverses agences à l'échelle mondiale. Cela contribue énormément à renforcer les partenariats qui sont en place.

Le sénateur Atkins: Surintendant Pilgrim, ma première question nous ramène au témoignage de notre premier témoin et à toute la question de la sécurité portuaire. La GRC travaille-t-elle étroitement avec les autorités locales quant aux préoccupations de ces dernières relatives aux activités portuaires?

Le surintendant Pilgrim: Oui. Selon la nature de l'activité à laquelle nous nous intéressons, nous travaillons main dans la main avec l'autorité responsable. Nous avons par ailleurs d'autres programmes visant la question plus vaste de l'intégrité de la frontière à nos ports, qu'il s'agisse d'aéroports, de postes frontière ou de ports maritimes. Nous travaillons étroitement, parfois quotidiennement, avec la police municipale ou locale, la police provinciale et les agences fédérales, en fonction des compétences de chacun. Nous menons par ailleurs nos propres enquêtes criminelles relativement à certaines activités survenant dans divers endroits. En sommes, donc, oui, nous entretenons de très bonnes relations de travail avec la police.

Le sénateur Atkins: Pourquoi avons-nous l'impression qu'il n'y a pas suffisamment de ressources compte tenu du niveau d'activité à maintenir? Par exemple, dans le port de Montréal, on a l'impression que le niveau de sécurité est insuffisant pour protéger les intérêts des Canadiens. Dans quelle mesure nos autorités sont-elles en mesure d'examiner les conteneurs pour savoir ce qui sort du pays et ce qui y entre?

Le surintendant Pilgrim: Je ne suis pas convaincu, quelles que soient les ressources qui y seraient consacrées, qu'il soit possible de régler toute la question des conteneurs dans nos ports. Comme vous le savez, le transport maritime est une activité très importante. Chaque jour un port verra passer des milliers et des milliers de conteneurs.

Il est difficile de dire qu'il nous faut des ressources supplémentaires pour traiter du problème dans son ensemble. Cependant, les ressources sont définitivement un élément dans toute la question de la surveillance de nos ports, qu'ils soient aériens, terrestres ou maritimes. La sécurité portuaire a été identifiée comme étant l'une de nos priorités nationales. L'on est en train de se pencher sur des stratégies quant à la meilleure façon d'aborder la situation. L'on espère qu'un niveau approprié de ressources sera consacré à ce défi.

Le sénateur Atkins: Si vous trouvez un camion rouge Z71, plaque d'immatriculation «Norman», faites-le moi savoir.

En ce qui concerne l'espionnage industriel, pourriez-vous nous dire si cela prend de l'ampleur ou bien si vous jugez que la situation est sous contrôle?

Le surintendant Pilgrim: C'est un sujet sur lequel je ne dispose pas de beaucoup de renseignements. La chose est surveillée et évaluée de façon régulière. Vous voudrez peut-être aborder cette question avec nos homologues du SCRS lorsqu'ils comparaîtront devant le comité.

Le sénateur Atkins: Hier, on nous a dit que les militaires éprouvaient de la difficulté à maintenir leur niveau de recrutement. Est-ce un problème du côté de la GRC?

Supt. Pilgrim: Recruiting within the RCMP is an ongoing process, not unlike the military, I am sure. Our human resource area within the RCMP is constantly looking at the formula to ensure the right balance of people leaving and coming in.

We do not have problems with attracting applicants for the RCMP. The difficulty is determining the numbers that we can accommodate given budget restraints and the established positions that we have. The balance is important. Recruiting and developing of expertise in police officers or peace officers does not appear to be a problem for us.

Senator Atkins: The new challenges in policing require new levels of qualifications. Over the last few years we have heard the challenges of ethnic balance and recruiting women. Would you care to comment on those two areas?

Supt. Pilgrim: The RCMP, in its recruiting process, takes these issues into consideration. I do not have the exact percentages right now. However, I do know that the percentage of women as regular members in the RCMP has significantly increased over the past number of years. Female members are in senior ranking positions in the RCMP at the present time.

We also take into consideration the other requirements from a policing perspective with respect to other communities within the country, communities such as Cole Harbour or our black communities in and around Halifax. It is one of the issues that we dealt with on a regular basis to ensure that we had sufficient numbers of black candidates being recruited, meeting the requirements and being engaged in the force.

It is always a challenge, because in many of these communities, as was pointed out earlier, depending on the cultural issues and some of the background, the police are not always seen as I would like to think the police in Canada are seen, which is in more of a positive light. In some of the other cultures that we may need to deal with, the police are not necessarily seen in that same light.

Senator Atkins: In regard to the comments made by Senator Forrestall, I gather that where you need the expertise in certain areas you are recruiting civilians into senior roles in the establishment?

Supt. Pilgrim: That is correct. There are some capabilities that we need outside of the traditional police function, so the trend is to recruit within that particular requirement as opposed to taking an individual and bringing him in as a police officer and then developing that capability at a later stage. Sometimes there is a difference in what you require there, and sometimes there is a need to have a combination of both. We are also meeting that requirement.

Senator Atkins: How do you change the slogan that the RCMP always get their man?

Supt. Pilgrim: In the generic sense?

[*Translation*]

Le surintendant Pilgrim: Le recrutement au sein de la GRC est un processus continu qui, j'en suis certain, n'est pas dissemblable de celui suivi par les militaires. Le service des ressources humaines de la GRC est sans cesse en train d'examiner la formule pour veiller au bon équilibre entre les personnes qui entrent et celles qui partent.

Nous n'avons pas de mal à attirer des candidats à la GRC. La difficulté réside dans la détermination des nombres que nous pouvons accueillir, compte tenu des compressions budgétaires et des postes établis que nous avons. L'équilibre est important. Le recrutement et l'acquisition de compétences par les agents de police ou gardiens de la paix ne semblent pas être un problème pour nous.

Le sénateur Atkins: Les nouveaux défis dans le travail de la police exigent de nouveaux niveaux de compétence. Au cours des dernières années, nous avons entendu parler des défis posés par l'équilibre ethnique et le recrutement de femmes. Auriez-vous quelque commentaire à faire au sujet de ces deux questions?

Le surintendant Pilgrim: Dans le cadre de son processus de recrutement, la GRC tient compte de ces aspects. Je n'ai pas les pourcentage exact en tête. Cependant, je sais que le pourcentage de femmes membres régulières de la GRC a sensiblement augmenté au cours des dernières années. L'on compte à l'heure actuelle des femmes parmi les rangs supérieurs de la GRC.

Nous tenons également compte d'autres exigences dans le cas de certaines localités du pays, comme par exemple Cole Harbour ou les communautés noires dans les environs de Halifax. Il s'agit là d'un aspect dont nous nous occupons de façon régulière, afin d'être certains d'avoir suffisamment de candidats noirs qui satisfassent les exigences et qui soient recrutés.

C'est un défi permanent, car dans nombre de ces localités, comme cela a été souligné plus tôt, selon le contexte culturel et historique, la police n'est pas toujours perçue comme je souhaiterais qu'elle le soit au Canada, c'est-à-dire dans une lumière positive. Dans certaines des autres cultures avec lesquelles nous pouvons être amenés à traiter, la police n'est pas toujours vue dans la même lumière.

Le sénateur Atkins: Pour en revenir aux commentaires faits par le sénateur Forrestall, je suppose que là où vous avez besoin de compétences dans certains domaines, vous recrutez des civils pour occuper des postes supérieurs à l'interne.

Le surintendant Pilgrim: C'est exact. Il y a certaines compétences dont nous avons besoin à l'extérieur de la fonction policière traditionnelle, alors la tendance est de recruter à l'intérieur de ce cadre au lieu d'aller chercher une personne, de la recruter en tant qu'agent de police puis de la former à un stade ultérieur. Il y a parfois une différence dans ce dont vous avez besoin et il faut parfois une combinaison des deux. Nous satisfaisons donc ces besoins-là également.

Le sénateur Atkins: Comment changer le slogan voulant que la GRC attrape toujours son homme?

Le surintendant Pilgrim: Dans le sens générique?

[*Français*]

Senator Pépin: You mentioned in your presentation that if information held in files is not kept confidential, Canadians will have less confidence in the government. On the one hand, I fully agree that the government needs to pass laws to counter terrorist activity, particularly in the context of globalization and the emergence of new technologies. On the other hand, if we are talking about invading people's privacy, I have some concerns. There is a very fine line between the two. With the advent of new technologies, people's lives are becoming open books.

You pointed out that there was not adequate legislation in place now to assist you there, but what could we do in this area without endangering the right to confidentiality?

[*English*]

Supt. Pilgrim: In relation to the whole issue of creating a balance with respect to developing our capabilities to respond to threats or potential threats so that the government, or the systems or the establishment, is seen to be able to effectively respond, the area to which we turn to determine that that balance exists is usually what we refer to as our "threat assessment." The threat assessments will provide us with a reasonably good assessment as to what are the threats being faced by Canada or Canadians with respect to national security issues. Subsequently, the process, or the procedures or the capabilities, we develop must be balanced out with the threat assessment.

For example, in my previous function in the office of the previous witnesses here, there was always the question of the Americans investing or infusing millions of dollars into terrorism or counterterrorism, and why is Canada not doing that? We must look at it from two different perspectives, one being, as I mentioned earlier, that the U.S. is the number one terrorist target in the world. Subsequently, they need to take measures that we probably would not need to take. In Canada, where the threat is deemed to be much lower — or low, I suppose, from a definitional perspective — it is important that we do not overreact. However, by the same token, we take the necessary steps to ensure that we have a balanced approach to what we see or what is assessed as the actual threat.

Can we do more? I believe there are initiatives in place right now, as was mentioned by Mr. D'Avignon, for government initiatives to develop options or strategy to strengthen Canada's counterterrorism response capabilities. I am hopeful that when that initiative is completed, we will see more of a balance.

Therefore, we will be able to say to the Canadian people — and I believe we can say it now — that there may be some shortfalls but, with the existing threat level and with the methods and the means or the process and the arrangements that are presently in place, we can then say that there is a balance, and we are in a

Le sénateur Pépin: Vous avez mentionné dans votre exposé que, si la confidentialité des dossiers n'était pas respectée, les citoyens avaient moins confiance dans le gouvernement. D'une part, je suis tout à fait d'accord pour que le gouvernement adopte des lois afin de contrer le terrorisme, surtout dans le cadre de la mondialisation et de l'émergence des nouvelles technologies. D'autre part, s'il y a intrusion dans la vie privée des individus, je suis réticente. La marge de manœuvre entre les deux reste très mince. Avec les nouvelles technologies, la vie des gens devient un livre ouvert.

Vous avez souligné le fait qu'il n'y avait pas suffisamment de lois pour vous aider, mais comment pourrions-nous faire cela sans mettre en péril le droit à la confidentialité?

[*Traduction*]

Le surintendant Pilgrim: En ce qui concerne toute la question de la création d'un équilibre dans le développement de nos capacités d'intervenir en cas de menaces ou de menaces potentielles de telle sorte que le gouvernement, ou les systèmes ou les pouvoirs soient perçus comme étant en mesure de réagir de façon effective, nous comptons en règle générale, pour déterminer que cet équilibre existe, sur ce que nous appelons habituellement notre «évaluation de menace». Les évaluations de menace nous donnent une assez bonne idée de la nature des menaces auxquelles sont exposés le Canada ou les Canadiens dans le contexte de la sécurité nationale. En conséquence, les processus, ou les procédures ou les capacités, que nous élaborons, doivent être équilibrés par rapport à l'évaluation de la menace.

Par exemple, dans le cadre de mes fonctions antérieures au bureau du témoin qui m'a précédé ici, il y avait toujours la question des Américains qui investissaient ou engloutissaient des millions de dollars dans le terrorisme ou l'antiterrorisme, et celle de savoir pourquoi le Canada ne faisait pas de même. Il nous faut examiner cela de deux points de vue différents. Premièrement, comme je l'ai déjà mentionné, les États-Unis sont la cible mondiale numéro un des terroristes. Il leur faut en conséquence prendre des mesures que nous n'aurions probablement pas à prendre ici au Canada. Chez nous, où la menace est considérée comme étant bien moins grande — ou faible, je suppose, dans un contexte de définition — il est important que nous ne réagissions pas avec excès. Il nous faut cependant par la même occasion prendre les mesures nécessaires pour veiller à ce qu'il y ait une approche équilibrée dans ce que nous voyons ou dans ce qui est considéré comme étant la véritable menace.

Pouvons-nous faire plus? Je pense qu'il y a en place à l'heure actuelle, comme l'a mentionné M. D'Avignon, un certain nombre d'initiatives: des initiatives gouvernementales en vue de l'élaboration d'options ou de stratégies visant le renforcement des capacités canadiennes de lutte contre le terrorisme. J'espère qu'une fois cette initiative particulière menée à terme nous verrons un meilleur équilibre.

Nous pourrons ainsi dire aux Canadiens — et je pense que nous le pouvons déjà — qu'il y a peut-être certains manquements mais qu'avec le niveau de menace existant et les méthodes et les moyens ou le processus et les arrangements qui sont en place, il y a un équilibre et nous pouvons dire aux gens qu'ils peuvent avoir

position to inform people that they can have confidence in the government, or in their police or in their fire department, or whatever the case may be, to be able to effectively respond to a given situation.

[*Translation*]

Senator Pépin: When you say you have assessed the threat, well, clearly we have no choice but to trust you as far as that information goes. And yet, as parliamentarians, we often have the feeling that we are not being told everything. I understand that you have to protect information and that there are times when you cannot release certain information. However, the answer I got from a previous witness was that he had no information about the question I had asked, when in fact, that information was on the Internet. You can always count on cooperation from parliamentarians. Yet the impression remains that we are not being told everything we should.

As concerns computer networks, we are told that the Senate's computer system could easily be targeted by hackers. Canada is highly dependent on its computer systems. Do we have reason to remain optimistic in the face of threats of cyber-terrorism and are we able to respond effectively to such threats?

[*English*]

Supt. Pilgrim: At the present time I understand OCIPEP are in the process of conducting an assessment. I believe this afternoon that you will probably hear more details of that with respect to the vulnerabilities and the level of preparedness with respect to our information systems. Those witnesses may be in a better position to respond to questions of that nature.

[*Translation*]

Senator Pépin: We have to wonder if making the law more severe will dissuade cyber-terrorists or if they will find another way to proceed.

[*English*]

The Chairman: Superintendent Pilgrim, earlier in the discussion you talked about Canada being less of a target than the United States; is that correct?

Supt. Pilgrim: That is correct.

The Chairman: Therefore, we do not need the same measures that they need, being a major target?

Supt. Pilgrim: That is correct.

The Chairman: The concern that some of the members of the committee are trying to address is that if we do not provide a sufficient level of security at our borders, then the Americans will close the borders to us. That is the conundrum that Senator Atkins was trying to reflect to you that we are hearing from American legislators. They are saying, "Look, we would prefer it if you folks took care of the problem at your borders, but if you are not going to do it, we will do it at our borders." Do you have a comment on that?

confiance dans leur gouvernement, dans leurs services de police, dans leurs services de lutte contre les incendies ou autre, qui sauront intervenir efficacement dans les situations qui se présenteront.

[*Français*]

Le sénateur Pépin: Lorsque vous nous dites que vous avez fait une évaluation de la menace, il est entendu que nous devons vous faire confiance quant à cette information. Pourtant nous, les parlementaires, avons bien souvent l'impression que vous ne nous transmettez pas toute l'information voulue. Je comprends que vous devez protéger vos informations et que parfois vous ne pouvez pas donner certains renseignements. Cependant, le témoin qui vous a précédé m'a répondu ne pas avoir d'information quant à la question que je lui avais posée alors que cette information, en réalité, se retrouvait sur Internet. Vous pouvez toujours compter sur la collaboration des parlementaires. Toutefois, l'impression de ne pas obtenir toute l'information voulue demeure.

En ce qui concerne les systèmes de réseaux informatiques, on nous dit que le réseau informatique du Sénat peut être piraté sans problème. Le Canada est très dépendant de ces systèmes de réseaux informatiques. Pouvons-nous rester optimistes face aux menaces du cyberterrorisme et y réagir efficacement?

[*Traduction*]

Le surintendant Pilgrim: D'après ce que j'ai compris, le BPIEPC est en train de réaliser une évaluation. Je pense que cet après-midi vous entendrez plus de précisions là-dessus, relativement aux sources de vulnérabilité et à l'état de préparation du côté de nos systèmes d'information. Ces témoins seront peut-être mieux en mesure de répondre à ce genre de questions.

[*Français*]

Le sénateur Pépin: Il faut se demander si le fait de rendre la loi encore plus sévère va dissuader les délinquants informatiques ou s'ils vont continuer et trouver une autre façon de procéder.

[*Traduction*]

Le président: Surintendant Pilgrim, plus tôt dans la discussion, vous avez dit que le Canada était moins une cible que les États-Unis, n'est-ce pas?

Le surintendant Pilgrim: C'est exact.

Le président: Une question que se posent certains membres du comité est la suivante: si nous n'assurons pas un niveau de sécurité suffisant à nos frontières, alors les Américains nous fermeront la frontière. C'est là l'énigme que tentait de vous exposer le sénateur Atkins et que nous soumettent les législateurs américains. Ils disent: «Écoutez, nous préférions que vous régliez le problème à vos frontières, mais si vous n'allez pas le faire, nous le ferons à nos frontières.» Auriez-vous quelque chose à dire là-dessus?

Supt. Pilgrim: Except for some of the issues that have been raised publicly concerning the immigration issues and that are being addressed, I believe that Canadians are addressing those issues. We have measures in place through Canada Customs and the enforcement agencies to address the issue of criminal activity across borders.

With that in mind, the arrangements, the partnerships and the joint training we are seeing between agencies on both sides of the border, in my view, will go a long way with respect to developing not only a stronger response capability but also a detection capability. We are seeing a sharing of information and intelligence between agencies, with a cooperative spirit. There is an understanding that the border may very well be vulnerable, on either side of the border. There has always been a high degree of cooperation but there seems to be more of a willingness to develop stronger methods and means of dealing with specific issues. We see that from the cross-border crime forum, in some of the counterterrorism committees or fora that I am personally involved in or have been involved in over the last several years. There is definitely a higher degree of sharing of information and a sense of working closer together to respond or deal with some of those criticisms or issues.

The Chairman: Are there no-go areas for police anywhere along our borders?

Supt. Pilgrim: No, none of which I am aware. I know that was an issue that came up several years ago with a previous committee. The response at that time is that there are no no-go areas. That is still the case.

The Chairman: Let me rephrase the question: Are there places where police officers go less frequently than others?

Supt. Pilgrim: It depends on the arrangements that are in place. Where other police forces have jurisdiction, or there are other policing arrangements, it may well be the case that an RCMP member may not go there as frequently as he would if it were strictly an RCMP jurisdiction. With respect to a no-go area, that is not the case.

The Chairman: Do RCMP officers move freely through Akwesasne?

Supt. Pilgrim: My understanding is that they have a working arrangement in Akwesasne that allows for the RCMP to work within that particular area. I do not have any specific details on the arrangement, but my understanding is that yes, we do work within the Akwesasne area.

The Chairman: In response to Senator Atkins' car problems, you said that you were not sure that any amount of resources would be sufficient to deal with the container problem in ports.

Le surintendant Pilgrim: Exception faite de certaines des questions qui ont été soulevées publiquement relativement à l'immigration, questions dont on s'occupe, je pense que les Canadiens font le nécessaire. Nous avons en place, par le biais de Douanes Canada et des agences d'exécution de la loi, des mesures destinées à résoudre le problème de l'activité criminelle transfrontalière.

Dans ce contexte, les arrangements, les partenariats et la formation conjointe que nous constatons entre agences des deux côtés de la frontière contribueront, je pense, beaucoup à l'établissement non seulement d'une capacité d'intervention plus forte, mais également d'une capacité de détection. Nous constatons entre agences des échanges d'informations et de renseignements, ce dans un esprit de coopération. On comprend de par et d'autre que la frontière pourrait bien être vulnérable dans un pays ou dans l'autre. Il y a toujours eu un degré élevé de collabortion, mais il semble qu'il y ait une plus grande volonté de mettre au point des moyens et des méthodes plus solides de traiter des différents problèmes. Cela ressort clairement dans le cadre du travail du forum sur la criminalité transfrontalière et de certains des comité ou des tribunes sur la lutte contre le terrorisme auxquels je participe personnellement depuis plusieurs années. Il est clair qu'il y a un échange poussé d'informations et une conscience partagée de la nécessité de travailler plus étroitement ensemble afin d'être en mesure de réagir à certaines de ces critiques ou à certains de ces problèmes.

Le président: Existe-t-il n'importe où le long de nos frontières des zones où la police est interdite d'accès?

Le surintendant Pilgrim: Non, pas que je sache. Je sais que c'est une préoccupation qui a été soulevée il y a plusieurs années par un comité antérieur. La réponse donnée à l'époque était qu'il n'y avait pas de zone d'interdiction d'accès, et c'est toujours le cas aujourd'hui.

Le président: Permettez que je reformule la question: y a-t-il des endroits où les agents de police vont moins souvent qu'ailleurs?

Le surintendant Pilgrim: Tout dépend des arrangements en place. Là où d'autres forces de police ont juridiction ou là où existent d'autres arrangements de services de police, il est possible que des membres de la GRC ne s'y rendent pas aussi souvent que s'il s'agissait de zones relevant strictement de la compétence de la GRC. Il n'existe cependant pas de zone de non-accès.

Le président: Les agents de la GRC se déplacent-ils librement dans tout le territoire Akwesasne?

Le surintendant Pilgrim: D'après les renseignements dont je dispose, ils ont en place à Akwesasne un arrangement de travail qui permet aux agents de la GRC d'y mener leurs activités. Je n'ai pas de détails précis quant à l'arrangement en question, mais d'après ce que j'ai compris nous travaillons bel et bien dans la zone Akwesasne.

Le président: En ce qui concerne les problèmes de voiture du sénateur Atkins, vous avez dit douter que les ressources, quelles qu'elles soient, suffisent jamais pour règler le problème des conteneurs dans les ports.

Supt. Pilgrim: The container problem in ports is massive. I go back to my days of working on the East Coast. There are a large number of ships coming in and out of ports on a daily basis. This has always been one of the areas that we have been concerned with, a means to be able to enforce effectively, or at least have a comfortable level of detail to indicate, what is coming in and what is not. I know that Canada Customs has a process in place whereby they look at particular containers. We work hand-in-hand with customs and the police of other jurisdictions in this respect.

To say that no level of resources would resolve the issue might not be correct. However, by the same token, it would be difficult to place a number on it at this point without effectively assessing the entire situation. I am not saying that that assessment is not being done. I know we are looking at all ports on a constant basis to ensure that our approach in dealing with the ports is as effective as it possibly can be.

The Chairman: I appreciate your candour, Supt. Pilgram. However, it sounds as if you are telling this committee that our ports are open to smuggling.

Supt. Pilgrim: To say there is no smuggling would not be correct. To say they are open to smuggling, I cannot give you that assessment. From an enforcement perspective, smuggling, contraband, drugs and human smuggling are areas of concern and priorities for the RCMP, and they are being addressed. To say our ports are open for smuggling, I would not give it that assessment.

Senator Atkins: Having said all that, do you not think that it would be a good idea if there were a federal agency charged with policing the ports throughout this country? That would be a deterrent if people knew they were there. The way it is now, there is a sense that smugglers can get away with something, and they are willing to take their chances. Was it a good idea to eliminate the port police?

Supt. Pilgrim: My understanding is that that was a political decision. It would not be appropriate for me to second-guess it.

Senator Atkins: I do not expect you to do that. It seems to me that we made a big mistake when we got rid of them.

Supt. Pilgrim: I know that the police of jurisdiction at the various ports are doing their best to respond to criminal activity that it is alleged is being committed at the ports. The RCMP and other agencies are working hand-in-hand, trying to respond to that concern. The situation would have to be assessed to determine whether there is a need for another ports police, as would the overall effectiveness of replacing the existing regime with something new.

Senator Atkins: A division of the RCMP?

Supt. Pilgrim: I will let you make that recommendation.

Le surintendant Pilgrim: Le problème des conteneurs dans les ports est gigantesque. Je repense à l'époque où je travaillais le long de la côte Est. Il y a chaque jour un très grand nombre de navires qui arrivent dans les ports et qui en partent. Nous avons toujours été préoccupés par cette question et désireux d'être en mesure d'assurer une surveillance effective ou en tout cas de nous sentir à l'aise avec le niveau de détail des renseignements obtenus sur les navires qui entrent et qui partent. Je sais que Douanes Canada a en place un processus en vertu duquel ils examinent différents conteneurs. Nous travaillons main dans la main avec les gens des Douanes et les autres services de police pour assurer ce contrôle.

Dire qu'aucun niveau de ressources ne suffirait jamais pour régler le problème n'est peut-être pas tout à fait juste. Néanmoins, il serait difficile de citer un chiffre sans faire une évaluation poussée de toute la situation. Je ne dis pas qu'une telle évaluation n'est pas en train d'être effectuée. Je sais que nous examinons constamment tous les ports dans le but de veiller à ce que nos opérations y soient aussi efficaces que possible.

Le président: J'apprécie votre candeur, surintendant Pilgram. J'ai cependant l'impression que vous êtes en train de dire au comité que nos ports sont ouverts à la contrebande.

Le surintendant Pilgrim: Dire qu'il n'y a pas de contrebande ne serait pas exact. Dire que les ports sont ouverts à la contrebande, c'est là autre chose, et je ne peux pas me prononcer là-dessus. Du point de vue exécution de la loi, la contrebande, le trafic de drogues et d'êtres humains sont des sujets de préoccupation prioritaires pour la GRC et nous sommes en train de les examiner. Mais je ne dirais pas que nos ports sont ouverts à la contrebande.

Le sénateur Atkins: Tout cela étant dit, ne pensez-vous pas que ce serait une bonne idée qu'il y ait une agence fédérale chargée de la surveillance des ports partout au pays? La présence d'une telle surveillance dissuaderait les gens s'ils étaient au courant. À l'heure actuelle, l'impression est que les trafiquants pourront s'en tirer et ils sont prêts à prendre des risques. Était-ce une bonne idée d'éliminer la police portuaire?

Le surintendant Pilgrim: D'après ce que j'ai compris, c'était la une décision politique. Il ne serait donc pas approprié que je me prononce là-dessus.

Le sénateur Atkins: Je ne m'y serais pas attendu non plus. Il me semble que nous avons commis une grave erreur lorsque nous les avons supprimés.

Le surintendant Pilgrim: Je sais que la police locale en place à différents ports fait de son mieux pour contrer l'activité criminelle dont on allègue qu'elle y est menée. La GRC et d'autres agences oeuvrent main dans la main dans leurs efforts visant à contenir le problème. Il faudra évaluer la situation pour déterminer s'il y aurait lieu de créer une autre police portuaire et pour déterminer l'efficacité globale du remplacement du régime existant par quelque chose de nouveau.

Le sénateur Atkins: Une division de la GRC?

Le surintendant Pilgrim: Je vous laisserai le soin de faire une telle recommandation.

Senator Forrestall: As an observation, part of this is an economic function. I have been told in the past, and I have no reason to doubt it, that were we to examine every single container coming into the Montreal and Halifax ports, they would grind to a halt. It takes a minimum of 40 minutes to offload, redirect, position, open, have a dog sniff, close, back up and put a container back into the process. With 1,040 containers on big ships, how much time is that? No economic process will allow that, no matter how great the risk. There has to be way, and the best way, which seems to work most of the time, is intelligence and surveillance.

Supt. Pilgrim: We cannot underestimate that.

Senator Forrestall: There seems to be a little confusion on this. We need port police. There is no question about that. This burden has been passed to the local police, who are untrained. They are doing a very good job, but it is a specialized role.

Supt. Pilgrim: We cannot underestimate the value of intelligence, information and the cooperative spirit to ensure that the information is being shared. To echo your comments, there is no question that it is the key element in this entire issue.

Senator Forrestall: It is a difficult problem.

Supt. Pilgrim: Yes, it is.

The Chairman: Thank you, Supt. Pilgrim. We appreciate your testimony today.

The committee adjourned.

OTTAWA, Thursday, July 19, 2001

The Standing Senate Committee on Defence and Security met this day at 2:15 p.m. to conduct an introductory survey of the major security and defence issues facing Canada with a view to preparing a detailed work plan for future comprehensive studies.

Senator Colin Kenny (*Chairman*) in the Chair.

Le sénateur Forrestall: Je dirais, en guise d'observation, qu'un élément de la situation est de nature économique. On m'a déjà dit par le passé, et je n'ai aucune raison d'en douter, que si l'on devait examiner chaque conteneur arrivant dans les ports de Montréal et de Halifax, toute l'activité y serait paralysée. Il faut un minimum de 40 minutes pour décharger, mettre en place, ouvrir, faire inspecter par un chien, fermer, repousser et remettre un conteneur dans la chaîne. Avec de gros navires transportant 1 040 conteneurs, combien de temps cela demanderait-il? Aucun processus économique, quelle que soit la gravité du risque, ne permettrait cela. Il faut qu'il y ait une solution, et la meilleure solution, qui semble fonctionner la plupart du temps, c'est le recours à la surveillance et au renseignement.

Le surintendant Pilgrim: Nous ne pouvons pas sous-estimer cela.

Le sénateur Forrestall: Il semble qu'il y ait un petit peu de confusion entourant cela. Il nous faut une police portuaire, cela est évident. Le fardeau a été transféré à la police locale, qui n'a pas la formation requise. Elle fait un très bon travail, mais l'on parle ici d'un rôle spécialisé.

Le surintendant Pilgrim: Nous ne saurions sous-estimer la valeur des renseignements, de l'information et de l'esprit de collaboration pour veiller à ce que toutes les données soient échangées. Pour reprendre ce que vous avez dit, il n'y a aucun doute que c'est là l'élément clé dans toute cette question.

Le sénateur Forrestall: Il s'agit d'un problème difficile.

Le surintendant Pilgrim: Oui, en effet.

Le président: Merci, surintendant Pilgrim. Nous vous sommes reconnaissants d'être venu témoigner devant nous aujourd'hui.

La séance est levée.

OTTAWA, le jeudi 19 juillet 2001

Le Comité sénatorial permanent de la défense et de la sécurité se réunit aujourd'hui à 14 h 15 pour faire une étude préliminaire des principales questions de défense et de sécurité qui touchent le Canada en vue de la préparation d'un plan de travail détaillé pour des études plus poussées.

Le sénateur Colin Kenny (*président*) occupe le fauteuil.

[*English*]

The Chairman: Good afternoon, ladies and gentlemen. If I may take just a moment on this, I understand that some people who have been watching the broadcast on television or on the Internet have been phoning in with questions for members of the committee. We are not structured to deal with that. It is simply a contact point for further information, and the Web site is a contact point for further meetings of the committee and for information that the committee puts up from time to time, such as a record of the testimony. We would welcome those who are interested in the work of the committee to communicate with us by mail, and we would be happy to get back in touch with you.

If I may, I will turn now to our witnesses today. Our panel includes Mr. James Harlick. Mr. Harlick is Assistant Deputy Minister, Office of Critical Infrastructure Protection and Emergency Preparedness in the Department of National Defence. In this capacity, he provides advice and support to the Associate Deputy Minister on policy and operational matters affecting the government's responsibilities for critical infrastructure protection and emergency management. His recent assignments have included Executive Director, Critical Infrastructure Protection Task Force in the Department of National Defence, and Executive Director, Year 2000, Planning and Coordination Group Activity in the Privy Council Office. Mr. Harlick will speak about the role of the Office of Critical Infrastructure Protection and Emergency Preparedness.

He is accompanied by Mr. Gary O'Bright. Mr. O'Bright joined the Communications Security Establishment in 1975 and has held a wide number of positions at this institution. In 1991 he attended the National Defence College in Kingston. Upon completion of this program he became the Communications Security Establishment Director of Strategic Planning, and in 1995, Director, Corporate Management. In August of 1997, Mr. O'Bright was appointed to the position of Director of the Information Technology Security Strategic Services Group.

In April of 2000, he joined the government's critical infrastructure task force, and in 2001 he assumed his current position as Director, General Operations for the Office of Critical Infrastructure Protection and Emergency Preparedness.

We also have with us Mr. Alan Bartley. Mr. Bartley is the Director General, Policy, Planning and Readiness of the Office of Critical Infrastructure Protection and Emergency Preparedness. He was previously director of security policy with the Solicitor General of Canada. He was a member of the Canadian Security Intelligence Service prior to joining the Department of the Solicitor General. A former journalist, Mr. Bartley has a Ph.D. in political science from McGill University.

Mr. James Harlick, Assistant Deputy Minister, Office of Critical Infrastructure Protection and Emergency

[*Traduction*]

Le président: Mesdames et messieurs, bonjour. Si vous permettez, je crois savoir que certaines personnes qui suivent les délibérations de notre comité à la télévision ou sur Internet ont téléphoné pour adresser des questions à des membres du comité. Nous ne sommes pas organisés pour répondre à ces questions. La télévision est simplement un point de contact pour obtenir un complément d'information et le site Web est aussi un point de contact pour obtenir des renseignements sur d'autres réunions du comité et pour publier occasionnellement des renseignements comme le compte rendu des témoignages. Ceux ou celles qui sont intéressés par les travaux du comité sont invités à communiquer avec nous par la poste et nous nous ferons un plaisir de leur répondre.

Maintenant, je vais céder la parole à nos témoins d'aujourd'hui qui sont M. James Harlick, sous-ministre adjoint, Bureau de la protection des infrastructures essentielles et de la protection civile au ministère de la Défense nationale. À ce titre, M. Harlick conseille et assiste la sous-ministre déléguée sur les questions stratégiques et opérationnelles, sur les responsabilités du gouvernement concernant la gestion des mesures d'urgence et la protection des infrastructures essentielles. M. Harlick a occupé récemment les postes de directeur général, Groupe de travail du ministère de la Défense nationale sur la protection des infrastructures essentielles, ainsi que le poste de directeur général, Groupe de coordination et de planification de l'an 2000 au Bureau du Conseil privé. M. Harlick nous entretiendra du rôle du Bureau de la protection des infrastructures essentielles et de la protection civile.

Il est accompagné de M. Gary O'Bright qui travaille au Centre de la sécurité des télécommunications depuis 1975 où il a occupé plusieurs postes. En 1991, il a suivi des cours au Collège de la Défense nationale à Kingston, après quoi il est devenu directeur de la planification stratégique au Centre et en 1995, directeur de la Gestion ministérielle. En août 1997, M. O'Bright a été nommé directeur du Groupe des services stratégiques et de la sécurité de la technologie de l'information.

En avril 2000, il s'est joint au groupe de travail du gouvernement sur les infrastructures essentielles et en 2001 il a assumé son poste actuel de directeur, Opérations générales, Bureau de la protection des infrastructures essentielles et de la protection civile.

Nous accueillons également M. Alan Bartley, directeur général, Planification des politiques et disponibilité opérationnelle au Bureau de la protection des infrastructures essentielles et de la protection civile. Auparavant, il était directeur de la Politique en matière de sécurité au ministère du Solliciteur général du Canada. Il a également été membre du Service canadien du renseignement de sécurité avant d'entrer au ministère du Solliciteur général. Ancien journaliste, M. Bartley possède un doctorat en science politique de l'Université McGill.

M. James Harlick, sous-ministre adjoint, Bureau de la protection des infrastructures essentielles et de la protection

Preparedness, National Defence Department: Mr. Chairman, I will read my statement to the senators and then take questions.

Mr. Chairman, ladies and gentlemen and members of the committee, I welcome this opportunity to appear before you today. As Senator Kenny, the chairman, has noted, my colleagues Mr. Bartley and Mr. O'Bright accompany me. I thought these individuals could best bring contribution to the hearing today given their respective responsibilities in the office.

I would like to use my opening remarks today to first provide background on the origins of the new office. Second, I would like to talk about the way ahead for Canada on critical infrastructure protection and emergency preparedness. Third, I would like to describe the office's link to the Department of National Defence and to the department and agencies of the portfolio of the Solicitor General. I cite these two departments because you heard yesterday from the Department of National Defence, of which we are a part, and this morning from the portfolio of the Solicitor General.

The new office is a civilian organization located within the Department of National Defence with a mandate to provide national leadership on critical infrastructure protection and effective emergency management. The office reports to the Associate Deputy Minister in the department, Ms Margaret Purdy.

I will address first the origins of the new office and the early work on the critical infrastructure protection. The origins of the government's work can be traced to 1996 when officials in the Canadian security and intelligence community conducted a preliminary review of the implications for Canada of the information technology revolution. This review was prompted by the emergence of serious concerns about the threat of information warfare, or electronic warfare as it was then known.

One of the principle conclusions of that review was that the Government of Canada had to modernize its program of identifying and protecting the most significant facilities in the country; that is, those facility on which the most vital services depended. This review concluded that information technology had transformed the nature and configuration of those facilities, and Canada's protection efforts had not kept pace.

The United States government was reaching similar conclusions at about the same time. A presidential commission on information protection reported in 1997 that urgent action was needed to protect U.S. vital interest from cyber threats and vulnerabilities.

In Canada, we were ready in 1998 to take forward specific proposals on how to approach the challenge. We postponed that work in favour of doing a first-class job on the Y2K computer bug challenge. We could not have pursued both efforts with success

civile, ministère de la Défense nationale: Monsieur le président, je vais vous lire ma déclaration, et je répondrai ensuite aux questions.

Monsieur le président, mesdames et messieurs les membres du comité, je suis heureux de m'adresser à vous aujourd'hui. Comme le président, le sénateur Kenny, l'a signalé, mes collègues MM. Bartley et O'Bright m'accompagnent. Je me suis dit qu'ils pouvaient apporter une contribution remarquable aux délibérations d'aujourd'hui compte tenu des responsabilités que chacun occupe au Bureau.

J'aimerais profiter de l'occasion pour, premièrement, vous relater les origines du Bureau. Deuxièmement, j'aimerais vous parler des perspectives en matière de protection des infrastructures essentielles et de protection civile au Canada. Troisièmement, j'aimerais vous décrire la relation du Bureau avec le ministère de la Défense nationale et le ministère et les organismes du portefeuille du Solliciteur général. Je vous parle de ces deux ministères parce que vous avez entendu hier les témoignages de représentants du ministère de la Défense nationale, dont nous sommes partie, et ce matin, de représentants du portefeuille du Solliciteur général.

Le nouveau Bureau est un organisme civil situé au sein du ministère de la Défense nationale, ayant pour mandat d'assurer le leadership national en matière de gestion de la protection des infrastructures essentielles et de protection civile. Le Bureau relève de la sous-ministre déléguée au ministère de la Défense nationale, Mme Margaret Purdy.

Je vais d'abord vous parler des origines du nouveau Bureau et de ses premières interventions en matière de protection des infrastructures essentielles. Le travail gouvernemental sur la protection des infrastructures essentielles remonte à 1996, lorsque des fonctionnaires de l'appareil canadien de sécurité et de renseignement ont effectué un examen préliminaire des incidences de la révolution informationnelle pour le Canada. Cet examen découlait de l'apparition de graves préoccupations au sujet de la menace d'une guerre de l'information, ou d'une guerre électronique, comme on l'appelait à l'époque.

L'une des principales conclusions de cet examen a été que le gouvernement du Canada devait moderniser son programme d'identification et de protection des installations les plus importantes du pays, c'est-à-dire les installations dont dépendent les services les plus essentiels. L'examen concluait que la technologie de l'information avait transformé la nature et la configuration de ces installations et que les efforts de protection du Canada n'étaient pas demeurés à la hauteur.

Le gouvernement des États-Unis en était arrivé à la même conclusion, à peu près au même moment. La Commission présidentielle sur la protection de l'information essentielle révélait en 1997 qu'il fallait établir des mesures d'urgence pour protéger les intérêts vitaux des États-Unis contre les nouvelles cybermenaces et vulnérabilités.

En 1998, au Canada, nous étions prêts à mettre de l'avant des propositions précises sur la façon d'aborder le défi de la protection des infrastructures essentielles. Toutefois, nous avons reporté ce projet pour faire un excellent travail sur le défi du bogue

given the level of resources both would have required and the involvement of many of the same players.On balance, we believe it was the right decision. The rollover occurred with no significant problems, and we benefited greatly from the sequencing after Y2K.

We now have a clearer picture of the nature of our national critical infrastructure. Y2K showed our dependence on the structure and taught us — that is, private sector, the government, and indeed the public — much about the associated interdependencies and vulnerabilities of our infrastructure.

We also forged groundbreaking relationships with the private sector, particularly the energy, telecommunications, banking and transportation sectors. As well, we formed stronger relationships with the provinces and territories and with our most important foreign partners.

Early in the year 2000, soon after the Y2K file was closed, the government created a one-year task force to prepare detailed proposals on critical infrastructure protection. The work of the task force was to advise ministers on what ongoing role, if any, the Government of Canada should take in terms of protecting the country's critical infrastructure. The task force adopted a broad approach to its work, broader than that taken by the United States, which had focused on the threat of malicious cyber-based attacks.

The tasks force adopted a Y2K-based definition of a critical infrastructure. Critical infrastructure is those systems facilities and networks whose failure or disruption would have a serious impact on the health, safety, security and economic well-being of Canadians and on the effective functioning of government in this country.

Canada's critical infrastructure exists in six highly interdependent sectors. The first is energy and utilities. The second is transportation in all four modes — air, water, rail and land. Communications, which includes telecommunications and the Internet, is the third sector. The fourth sector is safety, including nuclear safety and search and rescue services. The fifth sector is services including financial, food services, and health. The sixth grouping is the government sector in respect of its essential services that all levels of government provide to citizens.

The task force conducted extensive research and consultation in Canada and with international contacts. It concluded that Canada's critical infrastructure, in both its physical and cyber dimensions faced a state of increased risk in the 21st century.

I will now address the threat environment to critical infrastructure. Physical accidents and natural disasters will continue to occur. They will affect our infrastructure with significant consequences for Canadians. Canada has experienced at least 30 major disasters in the past five years. In the years to

informatique de l'an 2000. Nous n'aurions pu nous concentrer simultanément sur ces deux projets avec succès, compte tenu du niveau des ressources qu'ils auraient exigées et de la participation des mêmes intervenants. Tout compte fait, nous croyons avoir pris la bonne décision. Le report s'est effectué sans problème important et nous avons grandement profité du séquencement après l'an 2000.

Nous avons maintenant une vue plus claire de la nature de nos infrastructures nationales essentielles. L'an 2000 a fait ressortir notre dépendance à l'égard de cette infrastructure et nous en a appris beaucoup au sujet des interdépendances et des vulnérabilités connexes.

Nous avons également amorcé des relations avec le secteur privé, en particulier avec les secteurs de l'énergie, des télécommunications, des banques et des transports. En outre, nous avons établi des liens plus solides avec les provinces et les territoires et avec nos plus importants partenaires étrangers.

Au début de l'an 2000, peu après la fermeture du dossier du bogue de l'an 2000, le gouvernement créait un groupe de travail pour une durée d'un an, chargé de préparer des propositions détaillées sur la protection des infrastructures essentielles. Le groupe de travail avait pour mandat de conseiller les ministres sur le rôle permanent que le gouvernement devrait jouer, le cas échéant, pour protéger les infrastructures essentielles du pays. Le groupe de travail a adopté une approche générale, plus générale que celle prise aux États-Unis, qui était centrée sur la menace de cyberattaques malveillantes.

Le groupe de travail a adopté une définition des infrastructures essentielles établie en l'an 2000, à savoir: les systèmes, installations et réseaux dont une panne ou une défectuosité affecterait gravement la santé, la sécurité et le bien-être économique des Canadiens et des Canadiennes, ou qui sont essentiels au fonctionnement efficace des gouvernements dans ce pays.

Les infrastructures essentielles du Canada existent dans six secteurs hautement interdépendants. Le premier est l'énergie et les services publics. Le deuxième, les transports, dans ses quatre modes, soit le transport par air, par eau, par rail et sur terre. Les communications, qui incluent les télécommunications et l'Internet, constituent le troisième secteur. Le quatrième est la sécurité, y compris la sécurité nucléaire, la recherche et le sauvetage. Le cinquième secteur est les services, y compris les services financiers, alimentaires et sanitaires et le sixième groupe est le secteur du gouvernement, c'est-à-dire les services essentiels que tous les paliers de gouvernement offrent aux citoyens et aux citoyennes.

Le groupe de travail a effectué une recherche approfondie et a mené des consultations au Canada et auprès de collègues internationaux. Il a conclu que les infrastructures essentielles du Canada, dans leurs dimensions matérielle et cybernétique, couraient des risques accrus au XXI^{e} siècle.

Je vais maintenant vous parler des menaces aux infrastructures essentielles. Des accidents matériels graves et des catastrophes naturelles continueront de se produire, ce qui aura des répercussions sur nos infrastructures matérielles et entraînera des conséquences importantes pour les Canadiennes et les Canadiens.

come, hazardous spills, fires and other accidents will persist, as will severe weather events.

Between 1996 and 1998, three weather-related events, the Saguenay River flood in Quebec in 1996, the Red River flood in Manitoba in 1997 and the Ontario-Quebec ice storm in 1998, resulted in costs of more than $5 billion for repair and recovery. The Government of Canada alone provided $1.5 billion to provinces in terms of disaster commitments.

At the same time that physical disasters continue to challenge emergency planners in Canada, they have been joined by a new set of threats to our critical infrastructure. These new threats have a cyber dimension in that they exploit or impact information technology and telecommunications and our dependence on them. All of our vital services depend on information technology, which brings brand new vulnerabilities. The Internet is immature, unsecured and unstable. Those who develop commercial, off-the-shelf software are more concerned about getting their product to market than they are with checking the products thoroughly for glitches or faults that might make them vulnerable. Because we tend to migrate towards the same popular software suites, those faults and glitches can spread quickly, and with significant negative consequences.

A range of cyber tools can exploit these vulnerabilities. Viruses, worms and Trojan back doors have become part of our everyday vocabulary. If you use a computer at home or at work, you will recognize the significance of Melissa and the Love Bug as serious cyber attacks that have affected computer users around the world since 1999.

There is little relief in sight. Hacking tools are widely available. They are cheap or, worse, free and easy to use. Their use is becoming increasingly sophisticated.

Old threats are also taking on a new face. Technology is revolutionizing the worlds of crime, espionage and terrorism. Computers, the Internet, data encryption and a full range of communication devices, whether wire line or wireless, are as prevalent in these worlds as in ordinary business. Criminals and terrorists in unfriendly foreign governments can take advantage of these technology-based vulnerabilities and attack tools to defraud individuals, businesses and national economies. They could advance their political, ethnic or religious causes through these tools.

While attackers with clear motives are a clear danger, so too is the so-called recreational hacker. They use their computer skills to attempt to attack, corrupt or manipulate the computers and

Le Canada a connu au moins 30 catastrophes importantes au cours des cinq dernières années. Au cours des années à venir, des déversements dangereux, des incendies et d'autres accidents industriels continueront de se produire, tout comme des événements météorologiques violents.

De 1996 à 1998, trois événements météorologiques, soit l'inondation du Saguenay au Québec en 1996, l'inondation de la rivière Rouge au Manitoba en 1997 et la crise du verglas en Ontario et au Québec en 1998, ont entraîné des coûts de plus de 5 milliards de dollars, pour les travaux de réparation et de récupération. Le gouvernement du Canada à lui seul a fourni 1,5 milliard de dollars aux provinces sous forme d'aide financière en cas de catastrophe.

Pendant que les planificateurs des mesures d'urgence du Canada concentraient leurs efforts sur des désastres matériels et naturels, une nouvelle série de menaces à nos infrastructures essentielles faisait son apparition, des menaces axées sur la cybernétique en ce sens qu'elles exploitent la technologie de l'information et les télécommunications, qu'elles ont une incidence sur cette technologie et ces télécommunications et sur notre dépendance envers ces dernières. Tous nos services essentiels reposent sur la technologie de l'information, qui apporte de toutes nouvelles vulnérabilités. L'Internet manque de maturité, de sécurité et de stabilité. Les personnes qui élaborent des logiciels commerciaux de série se préoccupent souvent davantage d'être des leaders sur le marché plutôt que d'examiner minutieusement leurs produits pour détecter les pannes aléatoires et des défectuosités qui peuvent les rendre vulnérables. Et parce que nous avons tendance à tous opter pour les mêmes séries de logiciels populaires, ces défectuosités et pannes aléatoires peuvent se répandre rapidement et avoir des conséquences négatives importantes.

Une série d'outils cybernétiques peuvent exploiter ces vulnérabilités. Les virus, les vers, les trappes troyennes font déjà partie de notre vocabulaire et de notre vie quotidienne. Si vous utilisez un ordinateur à la maison ou au travail, vous reconnaîtrez l'importance des références à Melissa, au Love Bug, toutes des cyberattaques graves qui ont touché les utilisateurs de l'informatique dans le monde entier depuis 1999.

Il est peu probable que la situation change: les outils du piratage informatique sont facilement disponibles; ils sont peu coûteux ou pire encore, gratuits, et faciles à utiliser — et les criminels les utilisent avec de plus en plus de dextérité.

Les anciennes menaces prennent une nouvelle forme. La technologie révolutionne les milieux du crime, de l'espionnage et du terrorisme. Les ordinateurs, Internet, le cryptage de données et tout l'éventail des outils de communication, que ce soit à l'aide de fil ou sans fil, sont tout aussi répandus dans ces milieux que dans les entreprises ordinaires. Les criminels, les terroristes et les gouvernements étrangers hostiles peuvent tirer profit de ces vulnérabilités et outils de piratage pour escroquer des personnes, des entreprises et des économies nationales, ou pour promouvoir une cause politique, ethnique ou religieuse.

Bien que les agresseurs ayant des motifs précis constituent un danger réel, il en va de même pour les mordus de l'informatique qui utilisent leurs connaissances en informatique pour tenter

networks of others. They often have no motivation beyond seeing how far into a network they can penetrate, and how much damage they can do. Recreational hackers operating alone and not affiliated with any organized group have perpetrated most of the serious cyber attacks in the past three years.

According to CanCERT, which is a private sector-based computer emergency response organization, malicious attacks on computer systems are increasing at an alarming rate. Canadian statistics on scanning and attempted attacks against systems and networks suggest a 430 per cent increase in the level of activity from 1999 to 2000, with a projected level of increase beyond that of an additional 525 per cent in the year 2001.

The threats are real and serious. For example, a hacker in Australia altered the control mechanisms in 100 pumping stations, causing one million litres of raw sewage to overflow. In February 2000, as we will all remember, there was the distributed denial-of-service attacks against eBay, Yahoo, Amazon and several other Internet-based businesses. That attack is estimated to have resulted in lost revenue of up to U.S. $1.2 billion. This attack was the work of a 15-year old Montreal boy who used the cyber name Mafia Boy. Even Microsoft has been victimized. Last October, its high level internal network was hacked for a 7 to 12-day period. Microsoft officials admit that the hacker gained access to the source code of one product in the early stages of development.

In 2001 we have seen the emergence of a new type of cyber event that involves individuals and groups on opposite sides of a political struggle, but not necessarily operating under state control or direction. The first widespread event involved opposite sides in the Israeli-Palestinian conflict. More than 200 cyber attacks were launched, including Web site defacement, denial-of-service attacks and viruses, over a four-month period. The attacks targeted government business and infrastructure, and they spilled over beyond the Middle East.

Another example occurred in December, 1999, when the Electrohippies Collective, a group of five U.K. activists, organized a virtual sit-in of the World Trade Organization's Web site. In a denial-of-service attack, over 450,000 people swamped the site with multiple e-mails, disrupting its online presence. The same group attempted, with lesser effect, to do the same during the recent Summit of the Americas held in Quebec City this spring.

In summary, the threats to our critical physical and cyber infrastructure will put Canadian communities and Canadian businesses at risk in the 21st century. These risks will be magnified by four factors. First, Canada's population infrastructure and wealth are increasingly concentrated in a small number of highly vulnerable areas. Many such communities are at risk from multiple hazards. Second, climate change is expected to increase the frequency and severity of some extreme weather events. Third, Canada's infrastructure is aging, and thus more

d'attaquer, de corrompre ou de manipuler les ordinateurs ou les réseaux des autres. Ils n'ont souvent d'autre motivation que de voir jusqu'où ils peuvent pénétrer dans un réseau et combien de dommages ils peuvent causer. La plupart des cyberattaques les plus graves perpétrées au cours des trois dernières années étaient l'œuvre de pirates informatiques agissant seuls, non affiliés à un groupe organisé.

Selon CanCERT, un organisme privé spécialisé dans la gestion des urgences informatiques, les attaques malveillantes contre les systèmes informatiques s'accroissent à un rythme effarant. Les statistiques canadiennes concernant les balayages et les tentatives d'attaque contre des systèmes et des réseaux révèlent une hausse du niveau d'activité de 430 p. 100, de 1999 à 2000. On prévoit que le niveau d'activité augmentera de 525 p. 100 en 2001.

Les menaces sont réelles et graves. Par exemple, en Australie, un pirate informatique a modifié les mécanismes de contrôle de 100 stations de pompage, causant le débordement d'un million de litres d'eaux d'égout brutes. En février 2000, on s'en souviendra tous, l'attaque contre eBay, Yahoo, Amazon et plusieurs autres entreprises importantes basées sur Internet aurait entraîné une perte de revenus d'environ 1,2 milliard de dollars américains. Cette attaque a été perpétrée par un garçon de Montréal, âgé de 15 ans, qui utilisait le cybernom Mafia Boy. Même la puissante firme Microsoft a écopé. En octobre dernier, son réseau interne de haut niveau a été la cible d'un pirate informatique pour une période de sept à 12 jours. Les représentants de Microsoft ont admis que le pirate avait eu accès au code de source d'un produit aux premiers stades de son développement.

En 2001, nous avons constaté l'apparition d'un nouveau type d'événement cybernétique, mettant en cause des personnes et des groupes s'opposant dans une lutte politique, sans nécessairement agir sous le contrôle ou la direction d'un État. Le premier événement largement diffusé mettait en cause les parties opposées du conflit israélo-palestinien, plus de 200 attaques ont été lancées, y compris la détérioration de sites Web, des attaques de déni de services et des virus, sur une période de quatre mois. Les attaques visaient le gouvernement, les entreprises et les infrastructures et elles se sont répandues au-delà du Moyen-Orient.

Un autre exemple s'est produit en décembre 1999, lorsque le collectif Electrohippies, un groupe de cinq activistes du Royaume-Uni, organisa une «manifestation virtuelle» contre le site Web de l'Organisation mondiale du commerce. Au cours d'une attaque de déni de services, plus de 450 000 personnes inondèrent le site de messages électroniques, interrompant sa présence en ligne. Le même groupe tenta, avec moins de succès, de faire la même chose durant le récent Sommet des Amériques, à Québec le printemps dernier.

En résumé, les menaces à nos infrastructures matérielles et informatiques essentielles mettront en danger les collectivités et les entreprises canadiennes au cours du XXI^{e} siècle. Quatre facteurs amplifieront ces risques. Premièrement, la population, les infrastructures et la richesse du Canada sont de plus en plus concentrées dans un nombre limité de zones très vulnérables et bon nombre de ces collectivités courent des risques liés à des dangers multiples. Deuxièmement, on prévoit que le changement climatique accroîtra la fréquence et la gravité d'événements

susceptible to damage, whether from a tornado or a terrorist bombing. Fourth, communities are increasingly more reliant on advanced technologies that are more vulnerable for the reasons that I noted earlier.

To better equip Canada to respond to these challenges, the Prime Minister created the Office of Critical Infrastructure Protection and Emergency Preparedness on February 5, 2001. In his announcement, he told us why action on critical infrastructure is needed. He stated, "The protection of Canada's critical infrastructure from the risks of failure or disruption is essential to assuring the health, safety, security and economic well-being of Canadians." Mr. Chrétien identified the role of the Government of Canada in this matter. He said, "I am confident that these new measures will enable the Government of Canada to provide national leadership on this important issue and ensure our preparedness to deal with emergencies." Mr. Chrétien further noted that the government cannot accomplish this task alone. He said, "We will also be able to build strong partnerships to ensure the protection of our shared North American infrastructure."

The office is a uniquely Canadian approach — one that several other countries are considering. It embodies a unique "all hazards" approach to protecting both the cyber and physical dimensions of our critical infrastructure, regardless of the source of the vulnerability and threat. Significantly, the office encompasses the mandate and programs of the former agency, Emergency Preparedness Canada.

The work undertaken by the office will directly support three other important national priorities. The first is e-commerce, which depends for its success on public users having sufficient trust in the security and privacy of personal and proprietary information that is provided during commercial transactions. The second is e-government, or government online, as we would term it. E-government is dependent on developing and maintaining client confidence in the security and privacy of its underlying systems and networks. The third is the government commitment to safer communities, which requires the capacity to fight computer crime, maintain essential services and deal effectively with all types of disasters.

The new office has developed a national framework for critical infrastructure protection and effective emergency management that focuses on five elements. I will outline them for you.

The first is to contribute to putting the Government of Canada's own infrastructure house in order. If the government is to provide credible national leadership on critical infrastructure protection and emergency preparedness, it must first ensure an adequate level of protection for its own portion of the national critical infrastructure. This includes physical assets, such as the class 4 Winnipeg laboratory, buildings that house IT systems and networks, bridges and dams; systems and networks such as those that support weather forecasting, search and rescue operations, Employment Insurance and Old Age Security programs.

météorologiques violents. Troisièmement, les infrastructures canadiennes vieillissent et sont par conséquent plus susceptibles d'être endommagées, que ce soit par une tornade ou un attentat à la bombe terroriste. Quatrièmement, les collectivités comptent de plus en plus sur des technologies de pointe qui sont vulnérables pour les raisons déjà mentionnées.

Afin de mieux préparer le Canada à relever ces défis, le premier ministre créait, le 5 février 2001, le Bureau de la protection des infrastructures essentielles et de la protection civile (BPIEPC). Dans son annonce, il a expliqué les raisons pour lesquelles des mesures de protection des infrastructures essentielles sont nécessaires. Il a déclaré ceci: «Il est indispensable de protéger l'infrastructure essentielle du Canada contre les risques de panne ou de dérangement pour assurer la santé, la sécurité et le bien-être économique des Canadiens.» M. Chrétien a souligné le rôle du gouvernement du Canada dans ce domaine: «Je suis persuadé que ces nouvelles mesures permettront au gouvernement du Canada d'assurer un leadership national sur cette importante question et garantiront que nous serons prêts à faire face aux situations d'urgence.» Et il a mentionné que le gouvernement ne pouvait accomplir ce travail seul: «Nous pourrons en outre former des partenariats solides afin d'assurer la protection de l'infrastructure nord-américaine.»

Le Bureau est une approche particulière au Canada, que plusieurs autres pays songent à adopter. Il traduit l'approche «tous risques» spécifique au Canada visant à protéger les dimensions matérielle et cybernétique de nos infrastructures essentielles, peu importe la source de la vulnérabilité et de la menace. De manière significative, le Bureau englobe le mandat et les programmes de l'ancienne Protection civile Canada.

Et le travail entrepris sous la direction du Bureau soutiendra directement trois autres priorités nationales importantes. La première est le commerce électronique dont le succès dépend de la confiance suffisante des utilisateurs publics dans la sécurité et la confidentialité des renseignements personnels et exclusifs fournis lors des transactions commerciales. La seconde est l'administration électronique qui dépend du développement et du maintien de la confiance des clients dans la sécurité et la confidentialité de ses systèmes et de ses réseaux sous-jacents. La troisième est la sécurité des collectivités qui exige une capacité de combattre la criminalité informatique, de maintenir les services essentiels et de réagir efficacement à tous les types de sinistres.

Le nouveau Bureau a élaboré un cadre national pour assurer la protection des infrastructures essentielles et une gestion efficace des catastrophes centrée sur les cinq éléments suivants.

Le premier est de faire en sorte que les infrastructures du gouvernement du Canada prêchent par l'exemple. Si l'on veut que le gouvernement du Canada assure un leadership national crédible, il faut d'abord qu'il protège adéquatement sa propre partie des infrastructures nationales essentielles et de protection civile, notamment les biens matériels comme le laboratoire de Winnipeg de catégorie 4, les immeubles abritant les systèmes et les réseaux de TI, les ponts et les barrages; les systèmes et les réseaux comme ceux qui prennent en charge les prévisions météorologiques, la recherche et le sauvetage, l'Assurance-emploi et la Sécurité de la vieillesse.

The Government of Canada does not have, but will need, a complete "map" of its critical infrastructure, particularly on the cyber side where the most serious knowledge gaps exist. It will need a full understanding of its IT interdependency, vulnerabilities and its overall state of IT security posture. We need to update and expand the excellent work done in this area for the Y2K rollover, so that we are well-positioned to address the possible cascading effects of infrastructure disruptions or failure.

Le gouvernement du Canada ne dispose pas actuellement, mais il en aura besoin, d'une «carte» complète de ses infrastructures essentielles, surtout en ce qui concerne l'aspect cybernétique, où l'on constate un manque de connaissances flagrant. Il aura besoin également d'une compréhension complète de ses interdépendances en matière de TI, de ses vulnérabilités ou de l'ensemble de sa position en matière de sécurité de la TI. Nous devons nous mettre à jour et poursuivre l'excellent travail réalisé dans ce domaine lors de la préparation au passage de l'an 2000, pour être dans une bonne position pour régler les effets graduels des pannes ou des défaillances des infrastructures.

The office is developing a robust, 24-hour-seven-day monitoring and coordinating capability to support the Government of Canada in responding to threats and incidents affecting its own essential systems. Close cooperation with centres in other government departments is essential.

Le Bureau est en train de mettre au point une solide capacité de surveillance et de coordination 24 heures sur 24, sept jours sur sept, pour aider le gouvernement du Canada à réagir aux menaces et aux incidents qui affectent ses propres systèmes essentiels. Il est indispensable d'établir une collaboration étroite avec les centres d'autres ministères.

Examples of the office's operational services and activities will include: information sharing on threats and vulnerabilities, the issuance of timely advisories and alerts, the compilation and dissemination of best IT security practices, the promotion and adoption of common security solutions and the coordination of the response to cyber incidents. These services will be delivered in close collaboration with other key federal security advisory organizations, particularly those in the portfolio of the Solicitor General.

Voici des exemples des services opérationnels et des activités du Bureau: l'échange d'information sur les menaces et les vulnérabilités; la communication d'avis de sécurité et d'alertes au moment opportun; la compilation et la diffusion des pratiques exemplaires en matière de TI; la promotion et l'adoption de solutions communes en matière de sécurité; la coordination de la réaction aux incidents cybernétiques. Ces services seront fournis en collaboration étroite avec d'autres organismes consultatifs de sécurité fédéraux clés, surtout ceux qui appartiennent au portefeuille du Solliciteur général.

We will enhance and build creative and sustainable partnerships. The new office will give high priority to enhancing existing emergency preparedness partnerships and building new critical infrastructure protection partnerships that include: those with federal departments and agencies; provincial, territorial and municipal governments; public and private infrastructure owners and operators in business organizations, for example, the Canadian Chamber of Commerce and the Canadian Bankers' Association; non-governmental organizations such as the Canadian Red Cross; foreign government organizations such as the Federal Emergency Management Agency and the Critical Infrastructure Assurance Office in the United States, and international organizations such as NATO, G8 and OECD.

Nous allons améliorer ou établir des partenariats créateurs et durables. Le nouveau Bureau accordera une priorité élevée à l'amélioration des partenariats existants en matière de protection civile et créera de nouveaux partenariats en matière de protection des infrastructures essentielles, notamment avec tous les ministères et organismes fédéraux; les gouvernements provinciaux et territoriaux, ainsi que toutes les administrations municipales; les propriétaires et exploitants d'infrastructures publiques et privées et les associations d'entreprises comme la Chambre de commerce du Canada et l'Association des banquiers canadiens; des organisations non gouvernementales comme la Société canadienne de la Croix-Rouge; des organisations gouvernementales étrangères comme la Federal Emergency Management Agency, le Critical Infrastructure Assurance Office et les départements responsables des infrastructures aux États-Unis; des organismes internationaux comme l'OTAN, le G8 et l'OCDE.

The new office will build on the solid work and achievements of the former EPC, particularly in the areas of education and awareness, as it develops its programs. It will also enhance research and development work in relation to emergency preparedness and critical infrastructure protection. We will look into the most serious of the cyber security problems and try to improve our protection from these risks.

Le nouveau Bureau misera sur le travail solide et les réalisations de l'ancienne Protection civile Canada, en particulier dans les domaines de l'éducation et de la sensibilisation du public, pour ce qui est de l'élaboration de ses programmes. Il améliorera aussi le travail de recherche et de développement en matière de protection civile et de protection des infrastructures essentielles. Nous examinerons, par exemple, les problèmes les plus graves en matière de sécurité informatique et trouverons les meilleurs moyens de nous protéger contre ces risques.

National operational capabilities will be enhanced. We must strengthen these capabilities to take into account the new risk environment. Through its monitoring and coordination centre, the new office will work with key partners at all levels of

Nous améliorerons les capacités opérationnelles nécessaires. Nous devons renforcer nos capacités opérationnelles nationales d'urgence pour tenir compte du nouvel environnement des risques. Par l'entremise de son centre de surveillance et de

government, the private sector and internationally, to enhance information and intelligence analysis and sharing, incident response, and investigation and prosecution efforts.

We would enhance the existing policy framework for our mandate. The particular challenge in making sound decisions about risk mitigation and adequate levels of response during actual incidents is the timely exchange of threat and vulnerability information. The new office will need to examine whether, in the Canadian context, information sharing arrangements, perhaps modelled on the Information Sharing and Analysis Centre, a concept now under development in the United States, might be a useful way to promote private sector information-sharing.

The office has already had an encouraging dialogue with some key infrastructure sectors on information-sharing. For example, the Canadian banking sector is now considering the creation of such an information-sharing mechanism.

I will discuss now the office's link to the Department of National Defence and the Solicitor General's portfolio. The office fits well in National Defence for several reasons: First, the Canadian Forces, as you know, have a strong and positive reputation for helping Canadians in times of distress as evidenced during the Manitoba flood and the ice storm. The Minister of National Defence is also the lead minister for emergency preparedness and for providing leadership in the areas outlined in the Emergency Preparedness Act. Emergency Preparedness Canada was already well-established in DND at the time of the creation of the office, and both the department and the Canadian Forces put a high priority on cyber-security and contingency planning for emerging threats.

We are working actively to identify and flesh out the possible synergies and partnerships with those in the department and the Canadians Forces who are responsible for a number of the following areas: identifying and understanding vulnerabilities associated with critical physical assets and computer network systems and devices; understanding the threat environment, such as the threats posed by hacking and information warfare to military personnel, operations and facilities; conducting research aimed at dealing more effectively with cyber-security problems; and managing the bilateral military relationship with the United States where homeland defence, critical infrastructure protection and cyber-security are high national priorities.

In a similar fashion, the office will have close cooperative dealings with the Department of the Solicitor General, the Royal Canadian Mounted Police, and the Canadian Security Intelligence Service. These links could encompass the following activity areas where the department and agencies have existing roles and responsibilities, such as: operational response, including threats and incident analysis, vulnerability assessment and threat and

coordination, le nouveau Bureau travaillera avec ses partenaires clés, à tous les paliers de gouvernement dans le secteur privé et à l'échelle internationale, pour améliorer l'analyse et l'échange d'information et de renseignements, la réaction aux incidents et les efforts liés aux enquêtes et aux poursuites judiciaires.

Nous améliorerons le cadre stratégique existant pour notre mandat. Un défi particulier lorsqu'il s'agit de prendre des décisions éclairées concernant l'atténuation des risques et pour assurer des niveaux d'intervention adéquats lors d'incidents est l'échange d'information sur la menace et la vulnérabilité au moment opportun. Le nouveau Bureau devra évaluer si, dans le contexte canadien, les ententes relatives à l'échange d'information, peut-être fondées sur le modèle du concept de l'Information Sharing and Analysis Centre des États-Unis, peuvent être un moyen utile de promouvoir l'échange d'information avec le secteur privé.

Le Bureau a déjà établi un dialogue encourageant avec certains secteurs clés dans le domaine des infrastructures sur l'échange d'information. Par exemple, le secteur bancaire canadien envisage maintenant la possibilité de créer un mécanisme d'échange d'information.

Je vais maintenant vous parler des liens du Bureau avec la Défense nationale et le portefeuille du Solliciteur général. Le Bureau convient bien à la Défense nationale pour diverses raisons: premièrement, les Forces canadiennes, comme vous le savez, ont une réputation solide et positive en ce qui concerne l'aide aux Canadiens et Canadiennes lors de catastrophes, comme l'inondation au Manitoba et la crise du verglas en ont donné la preuve. Le ministre de la Défense nationale est le ministre compétent en matière de protection civile — et pour assurer le leadership dans les secteurs décrits dans la Loi sur la protection civile. Protection civile Canada était déjà bien établie au sein du MDN au moment de la création du Bureau; le ministère et les Forces canadiennes accordent une priorité élevée à la sécurité informatique et à la planification d'urgence en cas de nouvelles menaces.

Nous tentons activement de repérer et de renforcer les synergies et les partenariats possibles avec les personnes du ministère et des Forces canadiennes chargées: d'identifier et de comprendre les vulnérabilités afférentes aux biens matériels essentiels et aux réseaux, systèmes et dispositifs informatiques essentiels; de comprendre l'environnement menaçant comme les menaces que représentent le piratage informatique et la guerre de l'information pour le personnel, les opérations et les installations militaires; d'effectuer des recherches en vue de régler plus efficacement les problèmes de sécurité informatique; de gérer les relations militaires bilatérales avec les États-Unis où la défense du territoire, la protection des infrastructures essentielles et la sécurité informatique constituent des priorités nationales élevées.

De même, le Bureau collaborera étroitement avec le ministère du Solliciteur général, la Gendarmerie royale du Canada et le Service canadien du renseignement de sécurité. Ces relations pourraient couvrir les activités ci-dessous où le ministère et les organismes assument déjà des rôles et des responsabilités: la réaction opérationnelle, y compris l'examen des menaces et incidents, l'évaluation de la vulnérabilité et la réaction aux

incident response, including criminal and security intelligence investigations, which are, of course, conducted by the RCMP and CSIS; awareness and outreach to potential partners in the province and territories and private sector; research on and development of solutions to our technological vulnerabilities and risks; and training and education to teach and equip people and organizations to achieve a higher level of cyber-security awareness.

Canada must respond to the new infrastructure and emergency management challenges I have described today. To do so successfully will require an unprecedented level of cooperation within and outside of government.

Senator Stratton: Mr. Harlick, I had the distinct pleasure earlier last month of meeting with Associate Deputy Minister Margaret Purdy. She was kind enough to come to my office and give me an overview of the new security structure. I applaud the government for establishing such a structure because security is a real and serious problem that we have, and as you have described.

I guess it is tiring to hear me repeat this so often, but I am most concerned about our response to natural disasters, particularly flooding. I live in Manitoba along the Red River where, three times in the last six years, we have seen significant problems with flooding. It seems to be occurring more and more often.

I refer specifically to page 5 of your presentation, where you talk about these disasters. I understand that the Saguenay River flood in 1996 was an avoidable occurrence. Correct me if I am wrong, but I understand that that flood was caused by the operation of the water control structures along the river. The Ontario-Quebec ice storm power failures will be overcome in future by increasing the capability of individual power lines.Are you monitoring those two situations?

I am also concerned that a solution to the Red River problem, despite ongoing studies, is likely to be 12 to 13 years down the road. Are you monitoring that? Can you assure people who live along Manitoba's Red River that they are not likely to re-live another flood like that of 1997? Can you push the province to make up its mind and move on that problem? Please give us an overview on the prevention issues of the Saguenay region, the ice storm, and the Red River flooding. What steps have been taken to prevent recurrence of those events?

Mr. Harlick: I will couch the reply in a fairly broad context. Members of the committee here may well be aware, as is Senator Stratton as an expert in the emergency preparedness world, that unforeseen natural disasters — tornadoes, ice storms, floods — offer some difficult challenges to governments and other response organizations. We need to be prepared to respond when they occur, and to assist in recovery.

menaces et incidents, y compris les enquêtes criminelles et les enquêtes en matière de renseignement et de sécurité qui, bien sûr, sont menées par la GRC et le SCRS; la sensibilisation et l'établissement possible de partenariats avec les provinces et les territoires et le secteur privé; la recherche et le développement en vue de trouver des solutions à nos vulnérabilités et risques technologiques; la formation et l'éducation en vue de mieux renseigner les personnes et les organismes et de les sensibiliser à la sécurité informatique.

Le Canada doit relever les nouveaux défis que j'ai décrits aujourd'hui en matière de gestion des infrastructures et des urgences. Pour y arriver, nous devons atteindre un niveau sans précédent de coopération horizontale au sein du gouvernement et à l'extérieur.

Le sénateur Stratton: Monsieur Harlick, j'ai eu l'insigne honneur au début du mois dernier de rencontrer la sous-ministre déléguée, Mme Margaret Purdy. Elle a eu la gentillesse de venir à mon bureau pour me donner un aperçu de la nouvelle structure en matière de sécurité. Je félicite le gouvernement d'établir une telle structure parce que la sécurité constitue un problème réel et grave auquel nous faisons face, comme vous l'avez mentionné.

Même s'il est pénible de m'entendre répéter la même chose si souvent, je suis très préoccupé par notre façon de réagir aux catastrophes naturelles, plus particulièrement aux inondations. Je vis au Manitoba, près de la rivière Rouge où, à trois reprises au cours des six dernières années, nous avons subi d'importantes inondations. Le phénomène semble se répéter de plus en plus souvent.

Je m'en réfère plus particulièrement à la page 5 de votre exposé où vous évoquez ces catastrophes. Je sais que l'inondation de la rivière Saguenay en 1996 aurait pu être évitée. Corrigez-moi si j'ai tort, mais je crois que cette inondation a été causée par le mauvais fonctionnement des structures de contrôle de l'eau le long de la rivière. Les pannes d'électricité qui se sont produites lors de la crise du verglas au Québec et en Ontario seront évitées à l'avenir en accroissant la capacité des lignes de transmission. Est-ce que vous surveillez actuellement ces deux situations?

Je m'inquiète également à l'idée qu'une solution au problème de la rivière Rouge, malgré les études en cours, ne sera appliquée que dans 12 à 13 ans. Est-ce que vous examinez la situation? Est-ce que vous pouvez assurer les riverains de la rivière Rouge au Manitoba qu'ils ne risquent pas de subir une autre inondation comme celle de 1997? Pouvez-vous forcer la province à réfléchir et à agir? Je vous en prie, donnez-nous un aperçu des questions de prévention touchant la région du Saguenay, le verglas et l'inondation de la rivière Rouge. Quelles mesures ont été prises pour empêcher que ces événements ne se reproduisent?

M. Harlick: Je vais vous répondre de façon assez générale. Les membres du comité aujourd'hui présents savent bien, tout comme le sénateur Stratton, qui est un spécialiste dans les mesures de protection civile, que les catastrophes naturelles imprévues comme les tornades, le verglas, les inondations posent des défis particulièrement difficiles aux gouvernements et aux autres organismes d'intervention. Nous devons être prêts à réagir lorsque ces événements se produisent et à offrir notre aide pour assurer les secours.

The senator referred to the Province of Manitoba. In the emergency preparedness world, provincial and municipal jurisdictions have the primary responsibilities to prepare for and respond to disasters that occur in their jurisdictions. The federal government's role, under the Emergency Preparedness Act, is to ensure that, where we can, we help them to be well prepared for that purpose. We can achieve, through our efforts, a degree of national preparedness for these kinds of disasters.

Let us turn more specifically to this issue: How do we get ahead of the inevitable problems that will occur? Yes, the Red River will flood again. The International Joint Commission report on Red River flooding referred to the fact that the people who live in that area are perpetually at a risk.

One thing that I did not mention in preparedness response and recovery was mitigation. Knowing that the problems will occur, how can we get ahead of them to minimize the inevitable impacts? Senator Stratton did not mention this but he provided the keynote address at the World Disaster Management Conference in Hamilton recently. That was followed a day later by an announcement from Minister of Defence Art Eggleton on a National Disaster Mitigation Strategy. He said he was launching consultations by the federal government with the provinces and territories and non-governmental stakeholders to examine whether a national Canadian disaster-mitigation strategy can be developed to allow us to get ahead of the curve. We want to bring to bear the best practices, some good science and technology and as well, we hope, some resources to minimize the impact of the inevitable.

Mr. Bartley is in fact the official who will be leading those consultations for the National Disaster Mitigation Strategy. With the permission of the chair, I would ask him to supplement my response.

The Chairman: There is a supplementary question from Senator Atkins.

Senator Atkins: Is any consideration being given to developing a disaster relief fund that would be in place and ready for use in equipping the Armed Forces or whatever?

Mr. Harlick: We will look at that in the course of these consultations. People interested in the issue have floated that idea in the recent past. I will ask Mr. Bartley to respond, but this matter will come up in the consultations.

Mr. Alan Bartley, Director General, Policy Planning and Readiness, Office of Critical Infrastructure Protection and Emergency Preparedness: The question of a national disaster mitigation strategy has been around for some time. As some honourable senators may be aware, there were a series of consultations on a regional basis involving the former Emergency Preparedness Canada as well as a number of provinces, territories, non-governmental organizations and stakeholders including the private sector, which started to lay bare some of the issues that needed to be considered in a more detailed way around mitigation.

Le sénateur a mentionné le Manitoba. Dans le contexte de la protection civile, ce sont les provinces et les municipalités qui ont la responsabilité première de se préparer et de réagir aux catastrophes qui se produisent sur leur territoire. Le rôle du gouvernement fédéral, en vertu de la Loi sur la protection civile, est de veiller, là où nous le pouvons, à les aider à bien se préparer à réagir. Nos efforts nous permettent d'atteindre un niveau de préparation nationale pour faire face à ce genre de catastrophes.

Permettez-moi d'aborder plus spécifiquement cette question: quelle prévention faisons-nous pour enrayer les inévitables problèmes qui se produiront? Oui, la rivière Rouge va encore déborder. Selon le rapport de la Commission mixte internationale sur l'inondation de la rivière Rouge, les gens qui vivent dans cette région sont constamment en danger.

L'une des choses que j'ai omis de souligner en relation avec la protection civile et les secours, c'est l'atténuation des risques. Si on sait qu'il y aura des problèmes, quel genre de prévention pouvons-nous faire pour réduire au minimum les impacts inévitables? Le sénateur Stratton n'en a pas fait mention, mais il a prononcé le discours-programme lors de la Conférence mondiale sur la gestion des catastrophes qui s'est tenue à Hamilton dernièrement. Le lendemain, le ministre de la Défense, Art Eggleton, a annoncé la création d'une Stratégie nationale d'atténuation des catastrophes. M. Eggleton a indiqué que le gouvernement fédéral entreprendrait des consultations avec les provinces, les territoires et les intervenants non gouvernementaux pour envisager la possibilité d'élaborer une stratégie canadienne d'atténuation des catastrophes qui nous permettrait de prévoir les événements. Nous voulons faire ressortir les pratiques exemplaires, les éléments scientifiques et technologiques et de même, nous espérons, obtenir certaines ressources pour réduire au minimum l'impact de l'inévitable.

M. Bartley dirigera ces consultations sur la Stratégie nationale d'atténuation des catastrophes. Avec votre permission, monsieur le président, je vais lui demander de compléter ma réponse.

Le président: Le sénateur Atkins aimerait poser une question supplémentaire.

Le sénateur Atkins: Est-ce que vous songez à créer un fonds de secours aux victimes de catastrophes qui servirait à équiper les forces armées ou un autre groupe?

M. Harlick: Nous allons examiner cette question dans le cadre des consultations. Les gens intéressés par la question ont lancé cette idée récemment. Je vais demander à M. Bartley de répondre, mais cette question sera abordée lors des consultations.

M. Alan Bartley, directeur général, Planification des politiques et disponibilité opérationnelles, Bureau de la protection des infrastructures essentielles et de la protection civile: Le sujet d'une stratégie nationale d'atténuation des catastrophes a été maintes fois soulevé. Comme le savent peut-être les honorables sénateurs, il y a eu une série de consultations régionales impliquant l'ancienne Protection civile Canada, plusieurs provinces et territoires, des organisations non gouvernementales et d'autres intervenants du secteur privé. Ils ont entrepris d'examiner les questions d'atténuation des risques qui

Flood plain mapping, water management issues and flood control matters were areas that were floated during those discussions. This is an area that has been under some discussion for some time.

The experiences of the floods of 1996-97 and some smaller incidents since those times and the issue of compensation for disaster recovery have brought home to us how much mitigation is a factor in helping us to avoid some recovery expenses which are borne by citizens, provinces, territories and the Government of Canada generally in the recovery effort.

This is a broad-ranging area that has real economic consequences. In the discussions that occurred in 1998 — and we anticipate that they will come up again during the current consultation exercise — there has been some suggestion of a disaster fund. We are looking at that as part of the overall review.

We are conscious of the impact that recovery costs have on the public treasury and the existing mechanisms under the disaster financial assistance arrangements for assisting the provinces and territories to help their citizens get back on their feet. There may be other, better ways of dealing with these issues, and that is something that we would want to look at in that context.

More generally, with respect to flooding issues, that is again something that is under consideration in the consultation. We anticipate hearing from the Province of Manitoba, specifically, on some of the concerns that they have in this area. At the end of the consultation exercise, I hope we will be able to provide you and others with more specific comments on the way forward with respect to mitigation issues.

Senator Stratton: It is the gentle persuasion part of it that I would appreciate from your side, to keep the pressure on the provinces, to ensure that action is taken as quickly as possible.

After the Red River flood of 1950, it took 18 years before the floodway was in operation, from the study, the debates and then the final construction of the system. My worry is that we are already into completing the fourth year after the 1997 flood. If we must spin it out another 14 years, that is a worrisome issue. When you look at the flood of 1997, it has a recurrence factor of about once every 100 years. They are now talking about trying to protect against one flood every 500 years, minimum, or one flood every 1,000 years. It is a real concern because it just does not seem to be getting better. The situation is dramatically worsening to the degree that when you talk about flooding once every three out of the last six years, that is significant flooding. It is not just flooding to the level where we can implement protections, but the worrisome part is that we will be hit with a 250-year flood or a 500-year flood within the next 14 years.

If you go back to the 19th century, there were three floods in a period of 35 years that were equal to or greater than the flood of 1997; there were two floods within nine years that were equal to

doivent être étudiées plus à fond. Par exemple, au cours de ces discussions, on a proposé d'établir une carte des inondations, on a mentionné la gestion de l'eau et le contrôle des inondations. Oui, on en discute depuis un certain temps.

Les expériences des inondations de 1996 et de 1997, certains incidents ultérieurs de moindre envergure et le projet d'indemnisation pour les plans de secours nous ont fait voir à quel point une stratégie d'atténuation des catastrophes pourrait nous aider à éviter que les citoyens, les provinces, les territoires et le gouvernement fédéral en général aient à assumer certaines dépenses de secours.

C'est une question très vaste qui a des répercussions sur le plan économique. Dans les discussions qui ont eu lieu en 1998 — et nous prévoyons que les questions vont être soulevées à nouveau lors de l'exercice de consultation — certains ont proposé la création d'un fonds de secours. Nous examinons cette question dans le cadre de notre étude globale.

Nous sommes conscients de l'impact que les coûts des plans de secours exercent sur le Trésor public et sur les mécanismes existants en vertu des ententes d'aide financière en cas de catastrophe pour que les provinces et les territoires aident leurs citoyens à se remettre sur pied. Il y a peut-être d'autres façons plus adéquates de régler ces problèmes, et c'est ce que nous aimerions examiner dans ce contexte.

De façon plus générale, l'atténuation des risques d'inondations sera à l'ordre du jour des consultations. Nous entendrons les représentants du Manitoba, plus spécifiquement, sur certaines de leurs préoccupations à cet égard. À la fin de l'exercice de consultation, j'espère être en mesure de vous donner, ainsi qu'à d'autres, des commentaires plus spécifiques sur la façon dont nous prévoyons aborder les enjeux touchant l'atténuation des risques.

Le sénateur Stratton: J'aimerais que vous fassiez preuve de gentillesse et de persuasion à cet égard, que vous exerciez une pression sur les provinces pour qu'elles prennent des mesures le plus rapidement possible.

Après l'inondation de la rivière Rouge en 1950, il a fallu attendre 18 ans à partir de l'étude, des débats et enfin de la construction du système avant que le canal de dérivation ne fonctionne. Ce qui m'inquiète, c'est que quatre ans sont passés depuis l'inondation de 1997. Si nous devons étirer les choses encore 14 ans, cela m'inquiète. Une inondation comme celle de 1997 a un facteur de récurrence d'environ une fois tous les 100 ans. On pense maintenant à protéger les populations contre une inondation tous les 500 ans, au minimum, ou une inondation tous les 1 000 ans. C'est vraiment inquiétant parce que la situation ne semble tout simplement pas s'améliorer. La situation est dramatiquement inquiétante parce que lorsqu'on parle d'inondation une fois tous les deux ans, c'est important. Il ne s'agit pas ici que d'inondations qui peuvent être contrôlées par des mesures de protection, mais ce qui est grave, c'est que nous allons être frappés par une inondation de 250 ou 500 ans au cours des 14 prochaines années.

Au XIX^{e} siècle, il y avait des inondations tous les 35 ans, des inondations semblables ou supérieures à celle de 1997; il y a eu deux inondations en neuf ans, semblables ou supérieures à celle de

or greater than the flood of 1997. As you know, and you are experts in this field, as well, floods can come in clumps. My worry is that we are in that situation and we will need to move as quickly as possible. Your support in that area, and in pushing for a rapid conclusion for what we are trying to do in Manitoba, would be appreciated.

Senator Banks: Mr. Bartley, am I correct in understanding that you have taken over from Emergency Preparedness Canada?

Mr. Harlick: The Office of Critical Infrastructure Protection and Emergency Preparedness is composed of three organizations, the largest of which was Emergency Preparedness Canada. The second element that was rolled in was the Critical Infrastructure Protection Task Force that I referred to in my remarks.The third small entity was called the Government Information Protection Coordination Centre that was located at the RCMP headquarters in the east end of Ottawa. That body provided threat and incident analysis and coordination with the federal government with respect to computer problems or attacks. Those three elements were rolled together to form this office.

Senator Banks: In Alberta we have a public radio network called the CKUA ratio network that is comprised of 17 radio stations throughout the province. CKUA has been in engaged by the Province of Alberta and the Government of Canada as the means by which the warning of an impending crisis, natural disasters or otherwise, will be made known to Albertans, and at the flip of a switch will take over all the radio stations in Alberta. That plan is largely in place. I assume that comes under the aegis of the new agency, or the federal contribution to it does. We are very happy about that in Alberta, because almost all Albertans can be reached almost instantly in that way, in the event, for example, of a tornado.

Is there a plan in place to make that kind of early warning system, if I can call it that, available to other provinces?

Mr. Bartley: The Alberta system is unique to the Province of Alberta. The jurisdictional responsibility for those kinds of services resides with the provinces. We support all forms of public warning for emergency situations in principle. We think the Alberta system is a good one. There was an announcement earlier this week that will see that system expanded to cover the entire area of Alberta. That is, from our perspective, a good thing.

Given that this is a provincial jurisdiction, at our level we have no plans to support or encourage other provinces to do similarly. I understand that other provinces have been given access to the technology and the principle of how this particular system operates. However, it is their decision as to whether they wish to go forward with it.

Senator Banks: I certainly hope they will.

At present, the Energy Committee of the Senate is conducting a study into the subject of nuclear safety. As with many areas of concern, there are many different views about what is right and what is not right.

1997. Comme vous le savez, et vous êtes des spécialistes dans le domaine, les inondations peuvent se produire en masses. Ce qui m'inquiète, c'est que nous vivons actuellement cette situation et que nous devrons agir le plus rapidement possible. Votre aide à cet égard, et les pressions que vous exercerez pour que l'on en vienne rapidement à une conclusion sur ce que l'on essaie de faire au Manitoba, seraient appréciées.

Le sénateur Banks: Monsieur Bartley, ai-je raison de dire que vous avez englobé Protection civile Canada?

M. Harlick: Le Bureau de la protection des infrastructures essentielles et de la protection civile est constitué de trois organismes, dont le plus important était Protection civile Canada. Le deuxième élément qui a été intégré est le Groupe de travail sur la protection des infrastructures essentielles dont j'ai parlé dans mon exposé. Le troisième organisme, plus modeste, était le Centre de coordination de la protection de l'information du gouvernement, logé à l'Administration centrale de la GRC dans l'est d'Ottawa. Cet organisme offrait des services de coordination et d'analyse des menaces et des incidents au gouvernement fédéral pour lutter contre les problèmes ou les attaques informatiques. Ces trois éléments ont été intégrés pour former le Bureau.

Le sénateur Banks: En Alberta, nous avons un réseau radiophonique public, CKUA, formé de 17 stations de radio réparties dans toute la province. Le réseau CKUA a été retenu par la province de l'Alberta et le gouvernement du Canada pour prévenir les Albertains d'une crise imminente, d'une catastrophe naturelle ou autre et, le temps de le dire, il prendra le contrôle de toutes les stations de radio en Alberta. Une bonne partie de ce plan est en place. Je suppose que ce réseau est confié au nouvel organisme ou dépend d'une contribution fédérale. Nous en sommes très heureux en Alberta parce que de cette façon, on peut joindre presque tous les Albertains en cas, par exemple, de tornade.

Est-ce qu'il est prévu d'offrir ce genre de système d'alerte préalable, si je peux dire, à d'autres provinces?

M. Bartley: Le système de l'Alberta est particulier à cette province. La responsabilité de ce genre de services est de compétence provinciale. Nous appuyons normalement toutes les formes d'avertissement public en cas de situations d'urgence. Le système de l'Alberta est un bon système. On a annoncé au début de la semaine qu'il s'étendra à toute la province. Nous croyons que c'est une bonne chose.

Compte tenu du fait qu'il s'agit d'une compétence provinciale, à notre niveau, nous ne prévoyons pas appuyer ou encourager d'autres provinces à faire de même. D'autres provinces ont accès à la technologie et au principe de fonctionnement de ce système en particulier, mais c'est à elles de décider si elles veulent le mettre en pratique.

Le sénateur Banks: J'espère sincèrement qu'elles le feront.

Actuellement, le Comité sénatorial de l'énergie mène une étude sur la sécurité nucléaire. Comme pour bien des problèmes, les opinions diffèrent sur ce qui est bon et sur ce qui ne l'est pas.

How much attention have you had a chance to pay to the question of nuclear safety in a couple of areas? You may want to answer these questions later by contacting the clerk. First, the reopening of the nuclear plant in Ontario that is in process, against which there are some arguments, as there always are with things like that. Subsequent to the building of the plant now operated by OPG, which I believe is the Bruce plant, there have been fault lines discovered in the lake very close to that plant. I wonder if that has been made known to you?

The second is a larger question. We heard a disquieting piece of evidence with respect to nuclear safety and radiation in general. There is radiation all over the place and we are getting it all the time. There are people who determine the acceptable level of radiation by which everyone in the world measures themselves, and according to which nuclear regulatory agencies in Canada and other countries are able to say that they are way below the accepted level of radiation. It turns out that an international commission, all members of which are appointed by the nuclear industry, determines the acceptable level of radiation. As far as we can determine, there are no medical doctors on the commission, although we will investigate that further. We have been told that that has been the case since the late 1940s or early 1950s.

Are you paying attention to the refiring up of the OPG nuclear plant? Are you comfortable with it and in favour of it? I am sure that you are or you would have let us know by now.

Second, have you any concern about what is the "acceptable level of radiation," which is arrived at on the basis of a cost-benefit analysis? An acceptable number of deaths per 100,000 is acceptable because of the benefits derived therefrom. That is the basis of the standard by which the world governs itself.

I am not saying that the sky is falling, but in your concerns about nuclear safety, have you considered either of those things?

Mr. Harlick: I am afraid that I cannot respond directly to those two very pertinent questions because we are not in the nuclear safety business. When I referred to nuclear in my opening remarks, I spoke of critical infrastructure protection and critical infrastructures, one of which might be the nuclear sector. We are certainly interested in how well the nuclear sector manages its risk because if the risks are not managed well, the impact on the populace could be significant. We come at it from a slightly different perspective than a regulatory one.

Senator Banks: I am not talking about regulatory. Examination of the lakebed underneath the Bruce plant has found fault lines the existence of which were not known of when the plant was built. Some trenching has been done by which geologists are able to determine how old and how serious the fault lines are. We are in the process of determining whether that study has been completed and what the results are. If we have them, I do not know about it. I am talking precisely about what could be a catastrophic event. I cannot imagine anything more catastrophic. Again, I am not raising an alarm because I have no doubt that the chances of such

Avez-vous eu l'occasion de vous pencher sur la question de la sécurité nucléaire dans quelques secteurs? Peut-être voudrez-vous répondre à ces questions plus tard en communiquant avec la greffière. Premièrement, les démarches pour réactiver l'usine nucléaire en Ontario suscitent des protestations, ce qui est normal dans ce genre de projets. Après la construction de l'usine, qui est maintenant exploitée par le gouvernement de l'Ontario, l'usine de Bruce, je crois, on a découvert des failles dans le lac à proximité de cette usine. Je me demande si vous en avez été informé.

Ma deuxième question est plus vaste. Nous avons entendu un témoignage troublant en ce qui concerne la sécurité nucléaire et la radiation en général. Il y a de la radiation partout, tout le temps. Il y a des gens qui déterminent le niveau acceptable de radiation qui sert de barème à tous les pays du monde, et selon lequel les organismes de réglementation nucléaire au Canada et dans d'autres pays peuvent vérifier qu'ils sont bien en deçà du niveau accepté de radiation. Or, il s'avère que c'est une commission internationale, dont tous les membres sont nommés par l'industrie nucléaire, qui détermine le niveau acceptable de radiation. Pour autant que nous sachions, il n'y a pas de médecins qui siègent à la commission, mais nous allons pousser notre recherche. On nous a dit que c'est le cas depuis la fin des années 40 ou le début des années 50.

Est-ce que vous vous intéressez à la remise en état de l'usine nucléaire de l'Ontario? Êtes-vous satisfaits des mesures de réactivation? Êtes-vous d'accord? Je suis sûr que vous l'êtes sinon vous nous l'auriez dit.

Deuxièmement, est-ce que le «niveau acceptable de radiation» que l'on établit en se fondant sur une analyse coûts-avantages vous inquiète? Un nombre de morts par 100 000 personnes est acceptable à cause des avantages que l'on tire du système. C'est la norme de conduite qu'utilise le monde.

Je ne dis pas que le ciel est en train de nous tomber sur la tête, mais est-ce que vos analyses de la sécurité nucléaire englobent l'un ou l'autre de ces faits?

M. Harlick: Je crains de ne pouvoir répondre directement à ces deux questions très judicieuses parce que nous ne nous occupons pas de sécurité nucléaire. Quand j'ai mentionné le nucléaire dans mes remarques préliminaires, je parlais des infrastructures essentielles et de leur protection. Une structure essentielle pourrait être le secteur nucléaire. Nous sommes certainement désireux de voir comment le secteur nucléaire gère ses risques parce que si les risques sont mal gérés, l'impact sur la population pourrait être alarmant. Nous abordons la question d'un point de vue légèrement différent de celui des organismes de réglementation.

Le sénateur Banks: Je ne parle pas ici de réglementation. L'examen du lit du lac qui se trouve sous l'usine de Bruce a permis de déceler des failles qui étaient inconnues lorsque l'usine a été construite. On a creusé des tranchées qui ont permis aux géologues de déterminer l'âge et l'importance de ces failles. Nous nous demandons si cette étude a été terminée et quels en sont les résultats. S'ils sont connus, je n'en sais rien. Je parle précisément de ce qui pourrait être une catastrophe. Je ne peux imaginer rien de plus catastrophique. Là encore, je ne veux pas être alarmiste parce que je suis convaincu que les possibilités d'un tel accident

an event are one in a million, or perhaps a billion. However, a question about a large earth movement beneath a nuclear plant is not a regulatory one; it concerns an event that could have catastrophic effects, and that is the context of the question.

Mr. Harlick: I certainly appreciate your level of concern. From the point of view of nuclear safety, our responsibility would be to handle the consequences of a nuclear radiological accident or deliberate event. There is a federal nuclear emergency plan under the leadership of Health Canada for responding to that. We would work very closely with them on that issue in preparing for and responding to a nuclear radiological event that posed a threat to the population. It is from that point of view that we would be responding, as opposed to an oversight of the nuclear industry's standards of safety and that kind of thing.

Senator Banks: I am asking about the reaction: into whose bailiwick would it fall? In the last two days, we have asked a lot of people a lot of questions about a lot of situations that overlap a great deal. I am beginning to be concerned about who is in charge. When this happens, who will run it? Who calls the shots? Who gives the orders? Is it you?

Mr. Harlick: No, it is not. Obviously the provincial government is very strongly involved in nuclear —

Senator Banks: Not in nuclear regulation.

Mr. Harlick: In terms of Ontario Hydro, it is. There are also the federal nuclear arrangements, the National Energy Board and that kind of thing.

Senator Banks: Nuclear generation is not regulated by any province. It is the only kind of energy generation that is not. It is regulated by a federal agency only.

Mr. Harlick: Yes, by the Atomic Energy Commission and that kind of thing. It belongs to the Natural Resources Canada portfolio of agencies and departments here under that minister.

Senator Banks: In the event of a nuclear accident, there or elsewhere, is your agency in charge?

Mr. Harlick: No, it is not. As I mentioned, the lead agency for the federal nuclear emergency plan is Health Canada. We do liaise with them very closely as part of our coordination and support role. Given the uniqueness of that particular instance, it has been decided in government that they have the lead. We would generally have the lead in other, non-nuclear accidents.

Senator Wiebe: I certainly applaud the government on this initiative. I must say, however, that you gentlemen have a tremendous job on your hands. I understand that the purpose of this office will be, in large part, to set up preparedness for an event similar to Y2K, if such a disaster again threatened this country.

sont de une sur un million, ou peut-être un milliard. Cependant, l'éventualité d'un tremblement de terre sous une usine nucléaire n'est pas une question de réglementation. C'est un risque qui pourrait avoir des conséquences catastrophiques et c'est le sens de la question.

M. Harlick: Je comprends très bien votre inquiétude. Du point de vue de la sécurité nucléaire, notre responsabilité consisterait à gérer les conséquences d'un accident ou d'une agression nucléaire radiologique. Il existe un plan d'urgence en matière de sécurité nucléaire au gouvernement fédéral qui a été confié à Santé Canada. Nous travaillerions en étroite collaboration avec ce ministère pour nous préparer à faire face à un événement radiologique nucléaire qui menacerait la population. Tel serait notre mandat, qui n'est pas de surveiller les normes de sécurité de l'industrie nucléaire, ni d'assumer d'autres fonctions de ce genre.

Le sénateur Banks: Ma question concerne la réaction: qui serait responsable? Au cours des deux derniers jours, nous avons posé beaucoup de questions à beaucoup de gens sur un grand nombre de conjonctures qui toutes se chevauchent. Je commence à m'inquiéter et à me demander qui est responsable. Si un accident se produit, qui prendra les commandes? Qui prendra les décisions? Qui donnera les ordres? Est-ce votre Bureau?

M. Harlick: Non. De toute évidence, le gouvernement provincial est très impliqué dans le nucléaire...

Le sénateur Banks: Mais pas dans la réglementation du nucléaire.

M. Harlick: En ce qui concerne Hydro Ontario, oui. Il y a aussi des ententes fédérales sur le nucléaire, l'Office national de l'énergie, ce genre d'organisme.

Le sénateur Banks: Aucune province ne réglemente la production d'énergie nucléaire. C'est le seul type de production d'énergie qui n'est pas de compétence provinciale. Cela est réglementé uniquement par un organisme fédéral.

M. Harlick: Oui, par la Commission de l'énergie atomique, ce genre d'organismes ou de commissions affiliés à Ressources naturelles Canada et qui relèvent du ministre.

Le sénateur Banks: En cas d'accident nucléaire, là ou ailleurs, est-ce que c'est votre organisme qui est en charge?

M. Harlick: Non. Comme je l'ai dit, c'est Santé Canada qui est l'organisme fédéral responsable du plan d'urgence en matière d'énergie nucléaire. Oui, nous avons des liens très étroits avec le ministère, liens que nous assumons dans le cadre de notre rôle de soutien et de coordination. Compte tenu du caractère particulier de ce cas précis, le gouvernement a décidé d'en confier la responsabilité à Santé Canada. Normalement, nous sommes les responsables dans le cas d'autres accidents non nucléaires.

Le sénateur Wiebe: Je félicite le gouvernement d'avoir pris cette initiative. Cependant, je dois dire que vous, messieurs, avez d'énormes responsabilités. Je comprends que l'objectif du Bureau sera, en grande partie, d'établir les mesures d'urgence pour un événement comme le passage à l'an 2000, si une telle catastrophe menaçait à nouveau notre pays.

How long do you anticipate that the program will be in place such that you will be able to tell Canadians to rest assured in the event of a disaster? Second, we do not know whether what we did with regard to Y2K was successful. Either we did too good a job of ensuring that it did not happen, or it was never going to happen in the first place. We had up to 10 years to prepare for that. The next disaster could happen 10 minutes from now, or it could be a year from now. We will not have the time frame to prepare that we did in the Y2K situation. That is why I am asking about the time frame in which you believe that this office will be operating.

Mr. Harlick: As I noted in my opening remarks, the Y2K event was a pretty seminal event in the field of critical infrastructure protection. We learned a lot about the criticality and interdependency of infrastructures. Y2K was driven by a unique kind of failure — the failure of code, that is, inability to read the date correctly at a very particular point in time. The world of critical infrastructure protection and cyberfailure attack is much more diverse than that. In fact, it has been with us for some time and will continue with us until an unforeseeable time in the future. There is no beginning or end. It is a constant situation of managing risk. In that sense, we do not want to tie ourselves unduly to the Y2K example.

The second part is that it is a very diverse problem. Although the federal government put a lot of effort into Y2K, so did every other governmental jurisdiction, as well as companies and associations themselves. No one person or entity or level of government could fix the problem. That is quite similar to critical infrastructure protection.

The Americans say that 90 per cent of their nation's critical infrastructure — and I would imagine it would be the same for us — is not owned or controlled by the U.S. federal government, and thus neither is it owned by the Canadian federal government in our case. It is out there, owned, controlled and operated by the provinces, and particularly by the private sector. As one knows, there is the principle of accountability. They are accountable and responsible for making sure that it works. It is all part of the business, whether we refer to electricity production, banking or telecommunications.

The need is, in fact, very difficult. What is the problem? It could be any number of things, not just the failure of one kind of code at one point in time, never to be repeated for several hundreds of years. It is a very diverse, distributive problem.

What the government has decided to do, and as the Prime Minister has articulated in his press release, is to try to create this office of CIP and Emergency Preparedness in order to provide a locus for national leadership on this issue. However, it is not a "silver bullet" fix; it is a focal point for the federal government to get its act together vis-à-vis its own systems security, and to dialogue with other levels of government and the private sector and to engage in a cooperative venture to help them protect

Dans combien de temps prévoyez-vous que le programme vous permettra de convaincre les Canadiens de ne pas s'inquiéter en cas de catastrophe? Deuxièmement, nous ne savons pas si les mesures que nous avons prises en ce qui concerne le passage à l'an 2000 ont été un succès. Ou le travail a été si formidable que rien ne s'est produit, ou rien ne devait arriver de toute façon. Nous avons eu dix ans pour nous y préparer. La prochaine catastrophe pourrait survenir dans dix minutes, ou dans un an. Nous n'aurons pas le même délai pour nous y préparer que pour assumer le passage à l'an 2000. C'est la raison pour laquelle je vous demande dans combien de temps, à votre avis, votre Bureau sera opérationnel.

M. Harlick: Comme je l'ai précisé dans ma déclaration préliminaire, le passage à l'an 2000 a été très fructueux pour nous renseigner sur la protection des infrastructures essentielles. Nous en avons appris beaucoup sur le caractère essentiel et l'interdépendance des infrastructures. Le bogue de l'an 2000 était axé sur un type unique de panne — la panne du code, c'est-à-dire l'incapacité de lire la date correctement à un moment précis. Le monde de la protection des infrastructures essentielles et des attaques contre les cyberéchecs est beaucoup plus complexe que cela. En réalité, nous faisons face à ce problème depuis un certain temps et il continuera de nous menacer jusqu'à un avenir indéterminé. Il n'y a ni début ni fin. C'est un état permanent de gestion de risques. En ce sens, nous ne voulons pas nous lier indûment à l'exemple du bogue de l'an 2000.

Deuxièmement, il s'agit d'un problème très complexe. Bien que le gouvernement fédéral ait déployé beaucoup d'efforts pour assurer le passage en douceur à l'an 2000, tous les autres paliers de gouvernement ainsi que les entreprises et les associations ont fait de même. Aucun particulier, aucune entité ou aucun palier de gouvernement ne pourrait régler le problème. C'est assez semblable à la protection des infrastructures essentielles.

Les Américains disent que 90 p. 100 de leurs infrastructures essentielles — et j'imagine que ce serait la même chose pour nous — n'appartiennent pas au gouvernement fédéral des États-Unis, ni n'en relèvent. En ce qui nous concerne, le gouvernement fédéral est dans la même situation. Ce sont les provinces, et surtout le secteur privé, qui sont les propriétaires de ces infrastructures qui les contrôlent et les exploitent. Comme on le sait, il y a le principe de la responsabilisation. Les provinces et le secteur privé sont responsables de veiller à ce que ça fonctionne. Ça fait partie du métier, que l'on pense à la production d'électricité, au système bancaire ou aux télécommunications.

C'est très difficile de répondre aux besoins. Quel est le problème? Ça pourrait être n'importe quoi, pas seulement une panne de code à un moment précis, qui ne se répéterait pas pendant plusieurs centaines d'années. Le problème est très diversifié et très étendu.

Ce que le gouvernement a décidé de faire, comme l'a précisé le premier ministre dans son communiqué de presse, c'est de créer un Bureau de la protection des infrastructures essentielles et de la protection civile qui soit un noyau pour assurer le leadership national sur cette question. Cependant, ce n'est pas une solution «à toute épreuve». C'est un point de mire où le gouvernement fédéral peut rassembler toutes ses forces pour gérer nos propres systèmes de sécurité, pour dialoguer avec d'autres paliers

themselves through the sharing of knowledge and information, through the coordinated analysis of threats, to a coordinated response to problems when they occur.

Now that this office has been created, we are actively putting in place our capability, starting first with getting the government's own house in order, and at the same time dialoguing with key critical infrastructure sectors in Canada, to partner with them on very substantive, concrete, analytical and response functions.

Senator Wiebe: You are telling me, then, that this is really, in effect, not a program or an agency that will protect Canadians from a national disaster? Provincial governments will get involved if it is a regional disaster, with some cooperation from the national agency. If it is large disaster, such as an ice storm or flood, we may try to bring in some reservists or army people to help. Basically, we will not be coordinating the effort or have a plan or program in place?

Mr. Harlick: I may have misled you. National leadership coordination is the whole purpose. That is what the office's role is. However, there is no magic wand for the office to go out and say, "fixed, fixed, fixed." We must coordinate our efforts, as we did with the telecommunications sector with Y2K, so that they are apprised of problems and are coordinating with us to fix them. They must fix their systems. We want to work with them to ensure that that is done, and to contribute what we know about threats and vulnerabilities to assist them to do it.

Senator Wiebe: You are unable to give me a time frame as to when you feel this will be up and running?

Mr. Harlick: No, I can do that. Is the office up and running today? Yes, it is. Does it have a program for dealing with the banking sector? Yes, it does. Does it have a program for dealing with the electrical sector? Yes, it does. Will there ever be a solution to the problem? Will the problem go away? No. That is the nature of this particular problem of cyber-defence.

Senator Wiebe: That is not very comforting.

Senator Forrestall: That is scary.

Mr. Harlick: It is not comforting, but it does recognize what the problem is.

Senator Wiebe: Recognizing the problem and doing something about it, and giving assurances to the general public that we are doing something about it, is very key. I can recognize the problem until I am 400 years old, but I must do something within that 400 years to demonstrate that we are cognizant of the problem and indicate that this is how we will address it.

de gouvernement et le secteur privé, pour faire preuve de collaboration afin d'aider tout le monde à se protéger et ce, en transmettant des connaissances et de l'information, en effectuant une analyse coordonnée des menaces et en assurant une réaction coordonnée aux problèmes lorsqu'ils se posent.

Maintenant que le Bureau a été créé, nous sommes en voie de consolider notre capacité, en commençant par mettre de l'ordre dans les affaires du gouvernement, tout en communiquant avec les secteurs clés en matière de protection d'infrastructures essentielles au Canada pour établir avec eux des partenariats sur des fonctions d'analyse et de réaction très substantielles et concrètes.

Le sénateur Wiebe: Vous êtes en train de me dire qu'en réalité, le Bureau n'est pas un programme ou un organisme qui va protéger les Canadiens contre une catastrophe naturelle? Les gouvernements provinciaux devront se débrouiller s'il s'agit d'une catastrophe régionale, et pourront compter sur une certaine collaboration de l'organisme national. S'il s'agit d'une catastrophe majeure, comme une tempête de verglas ou une inondation, on pourra peut-être demander l'aide de quelques réservistes ou des gens de l'armée. Essentiellement, nous ne coordonnerons pas les efforts ou nous n'aurons pas de plan ou de programme en place?

M. Harlick: Je vous ai peut-être induit en erreur. La coordination des efforts à l'échelle nationale est l'objectif premier. C'est le rôle du Bureau. Cependant, le Bureau n'a pas de baguette magique lui permettant de tout régler. Nous devons coordonner nos efforts, comme nous l'avons fait dans le secteur des télécommunications avec le bogue de l'an 2000, afin que les provinces soient informées des problèmes et qu'elles coordonnent leurs efforts avec nous pour les régler. Elles doivent régler leurs systèmes. Nous voulons travailler avec elles pour nous assurer que c'est fait et pour leur transmettre ce que nous savons au sujet des menaces et des vulnérabilités afin de les aider à y faire face.

Le sénateur Wiebe: Vous êtes incapable de me donner une date à laquelle, vous pensez, le système sera opérationnel?

M. Harlick: Oui, je le peux. Est-ce que le Bureau est opérationnel aujourd'hui? Oui, il l'est. Dispose-t-il d'un programme pour faire face à une éventualité dans le cadre des services bancaires? Oui. A-t-il un programme pour le secteur électrique? Oui. Y aura-t-il une solution au problème? Le problème disparaîtra-t-il? Non. C'est là la nature de ce problème particulier en matière de cyberdéfense.

Le sénateur Wiebe: Ce n'est pas très rassurant.

Le sénateur Forrestall: Ça fait peur.

M. Harlick: Ce n'est pas rassurant, mais on connaît la nature du problème.

Le sénateur Wiebe: Connaître le problème, prendre des mesures pour le régler, donner des assurances au public que nous faisons quelque chose, cela est essentiel. Je peux reconnaître qu'il y a un problème jusqu'à ce que j'aie 400 ans, mais je dois faire quelque chose pendant ce temps pour montrer que nous sommes conscients du problème et déterminer comment nous allons l'aborder.

Mr. Harlick: That is right. I have laid out for you the fivefold national framework that shows the components of how this office, partnering with other government departments and other levels of government, and particularly the private sector, will bring national leadership to that issue to tackle the problem and to try to get results.

Senator Stratton: I have a very quick supplemental in defence of these folks. I believe this new office will do a remarkable job. If you look at the past, Emergency Preparedness Canada has done a remarkable job with respect to floods in Manitoba, as have the Armed Forces. I have great confidence in what they are setting out to do and I feel they will do a good job if past history speaks, and I think it does.

Senator Wiebe: Past history is such that we can be very proud of what our reservists and our regular army people have done in the past. However, what frightens me, from a westerner's point of view, is that National Defence is starting to centralize a tremendous amount of its command positions. The west now has one command position, which is in Edmonton. That is where the men and the equipment are.

Will we thin ourselves out more and more? We have two Hercules aircraft to fly men and equipment into an area, providing there is not a snowstorm. This causes me great concern, especially when I see that the key player in all of this will be the office of the Department of National Defence. Our reservists and our regular army people did a tremendous job in all three, particularly our reservists. I see us spreading ourselves too thin, and that is where my concern comes in.

Senator Atkins: With global warming and weather patterns these days, there is one area we have not talked about that is a potential flooding area almost every year. That is the Lower Saint John River Valley. Since 1973 it has not happened, but I point that out because every spring we are concerned about whether we will have serious floods. The 1973 flood was a disaster.

In dealing with the provinces, I assume each province has an emergency preparedness organization or set-up. Does it come under the Solicitor General or does it come under some minister designated by the premier in each individual province? Do you work with them? Do you feel comfortable with that relationship?

Mr. Harlick: Just on your first note about the Saint John River, I will say that, in the past, our office has been proud to be able to organize the financial contribution of the federal government to the Province of New Brunswick to compensate it for some of its expenditures to return to the status quo in the Saint John River flooding area.

With respect to the provinces, each province and territory does have its own emergency measures or preparedness organization. They report to a variety of ministers. It is at the choice of the province. In Ontario, for example, it is the Solicitor General. It could be the Minister of Housing or Community Affairs.

M. Harlick: C'est exact. Je vous ai fait état du cadre national à cinq composantes qui indique la façon dont le Bureau, en partenariat avec d'autres ministères et d'autres paliers de gouvernement, et plus particulièrement avec le secteur privé, assumera le leadership national à cet égard pour régler le problème et obtenir des résultats.

Le sénateur Stratton: Je voudrais faire un bref commentaire additionnel à la défense de ces messieurs. Je crois que ce nouveau Bureau fera un travail remarquable. Si on regarde ce qui s'est fait dans le passé, Protection civile Canada a accompli un travail remarquable pour combattre les inondations au Manitoba, tout comme les Forces armées. J'ai bonne confiance dans le projet en cours et j'estime qu'ils feront un bon travail si on se fie à l'histoire, et je pense qu'on doit le faire.

Le sénateur Wiebe: L'histoire nous enseigne que nous pouvons être très fiers de ce que nos réservistes et les soldats réguliers ont réalisé dans le passé. Cependant, ce qui m'inquiète, à titre d'habitant de l'Ouest, c'est que la Défense nationale est en voie de centraliser énormément les postes de commande. L'Ouest possède maintenant un poste de commande à Edmonton où sont logés les hommes et l'équipement.

Est-ce que nous allons nous dépouiller de plus en plus? Nous avons deux appareils Hercules qui peuvent amener les hommes et l'équipement dans une région, à la condition qu'il n'y ait pas de tempête de neige. Cela m'inquiète beaucoup, surtout quand je vois que l'intervenant clé dans tout ça sera le Bureau du ministère de la Défense nationale. Nos réservistes et nos soldats réguliers ont fait un travail remarquable, lors des trois inondations, surtout les réservistes. Moi je pense que l'on dilue trop nos forces, et c'est ce qui me préoccupe.

Le sénateur Atkins: Avec le réchauffement de la planète et les modèles météorologiques actuels, il y a une région dont nous n'avons pas parlé, c'est cette région où l'on risque d'avoir des inondations tous les ans, c'est-à-dire la vallée de la rivière Saint-Jean. Depuis 1973, rien ne s'est produit, mais je le fais remarquer parce que tous les printemps, nous nous demandons si nous allons avoir de graves inondations. Celle de 1973 a été une catastrophe.

En ce qui concerne les provinces, je suppose que chacune d'elles a un organisme de protection civile. Est-ce que cet organisme relève du solliciteur général ou d'un ministre désigné par le premier ministre de chaque province? Est-ce que vous travaillez avec ces organismes? Les relations vous satisfont-elles?

M. Harlick: Pour revenir à votre premier commentaire au sujet de la rivière Saint-Jean, je vous dirai que dans le passé, notre Bureau a été fier de pouvoir organiser la contribution financière du gouvernement fédéral à la province du Nouveau-Brunswick pour l'indemniser d'une partie des dépenses qu'elle a engagées pour ramener la région de la rivière Saint-Jean à son état d'origine.

Quant aux provinces, chacune ou chaque territoire a sa propre organisation de mesures d'urgence ou de protection civile. Chaque organisme est comptable à divers ministres, selon la province. En Ontario, c'est le solliciteur général. Ce pourrait être le ministre du Logement ou des Affaires communautaires. Peu importe le

Regardless of where they report to, our office, through our regional directors in our regional offices, deals closely with the provinces and their emergency management organizations. We have an office in each province and territory, and they are in daily contact with each other. It is our regional offices, through the regional director, that are the principal point of contact with the federal level from the provincial level in terms of both preparedness and the handling of an actual incident. It has been very tight historically and there has been very good cooperation. Senator Stratton's earlier point reflected that very good cooperation at the local level.

Senator Atkins: Senator Banks made a point: I assume that if there were a nuclear problem in Ontario, the Ontario government would be called to move in as quickly as you would.

Mr. Harlick: The liaison would be between the Ontario Emergency Management Organization, via our regional office in Toronto, directly to us in fast time.

[*Translation*]

Senator Pépin: My question deals with information technology services, as well as hacking tools that are currently available. This morning, I put a question to a representative of the RCMP, who told me you could probably give me a better answer.

Like other industrialized countries, our country is increasingly dependent on computer systems. Having heard your presentation, should we be more concerned about these viruses that are circulating and the kinds of cyber-attacks that can occur? Without going into detail, can you tell us whether Canadians should feel reassured given what is currently in place? Have you already taken concrete action to counter such attacks? Also, if we passed tougher laws and increased the penalties, do you believe that would deter young computer hacks from attacking Internet sites?

Mr. Harlick: I believe Canadians have every reason to feel reassured given the efforts currently being made by the federal government. We are in the process of implementing a plan of action. In terms of protection of our own computer systems, even our personal computers, we all have to take our responsibilities in this regard. I am sure you remember the Love Bug virus that affected users around the world. As soon as a user opened up the message attachment, his or her computer became infected. And yet in the months that followed, other viruses did not have the same impact, because we learned how to deal with the problem. We learned that you should never open up e-mail attachments if you are unsure of their origin. We are now learning how to deal with this type of problem and how to protect ourselves better.

Senator Pépin: It is a learning/training process for everyone.

Mr. Harlick: Yes, exactly. People have to be aware of the problem and know how to respond. Within the federal government, we are currently helping departments and agencies resolve issues associated with their computer network. Mr. O'Bright, the Director General of Operations, and his

ministère responsable, nos directeurs régionaux entretiennent d'étroites relations avec les provinces et les organisations de gestion des mesures d'urgence. Nous avons un bureau dans chaque province et territoire, et tous ces bureaux sont en contact quotidien l'un avec l'autre. Et nos bureaux régionaux, par l'entremise du directeur régional, sont le principal point de contact entre le fédéral et la province en ce qui a trait à la protection civile et à la façon de traiter un incident. Les liens ont toujours été très étroits et la collaboration extrêmement bonne. Le point qu'a soulevé le sénateur Stratton tout à l'heure reflétait cette très bonne collaboration au niveau local.

Le sénateur Atkins: Le sénateur Banks a soulevé une question intéressante: je suppose que s'il devait y avoir un problème nucléaire en Ontario, le gouvernement de l'Ontario serait appelé à intervenir aussi rapidement que vous.

M. Harlick: La liaison se ferait directement et rapidement entre la Protection civile de l'Ontario et notre Bureau central, via notre bureau régional à Toronto.

[*Français*]

Le sénateur Pépin: Ma question porte sur les services de la technologie de l'information ainsi que des outils de piratage disponibles. Ce matin, j'ai posé une question au représentant de la GRC qui m'a dit que vous alliez probablement me fournir une meilleure réponse.

Notre pays, à l'instar des autres pays industrialisés, est de plus en plus dépendant du système informatique. Après votre présentation, devrions-nous être plus inquiets avec tous ces virus électroniques qui circulent et ces attaques cybernétiques qui peuvent se produire? Pouvez-vous nous dire si, sans entrer dans les détails, les Canadiens et les Canadiennes peuvent être rassurés avec les moyens mis en place actuellement? Avez-vous déjà fait quelque chose de concret contre ces attaques? Si jamais on rendait la loi plus sévère et qu'on augmentait les peines, croyez-vous que cela dissuaderait les jeunes délinquants informatiques à attaquer les sites Internet?

M. Harlick: Je pense que les Canadiens et les Canadiennes peuvent être rassurés par les efforts du gouvernement fédéral. Nous sommes en train d'implanter un plan d'action. Quant à la protection de nos ordinateurs, même personnels, chacun doit prendre ses responsabilités. Vous vous souviendrez du virus «Love Bug» qui a fait le tour du monde. Dès que l'utilisateur ouvrait l'annexe de ce message, son ordinateur était infecté. Cependant, dans les mois suivants, les autres virus n'ont pas eu le même impact parce que nous avons appris comment gérer le problème. Il ne fallait donc plus ouvrir les annexes des courriels dont on ne connaissait pas l'origine. Nous sommes en train d'apprendre comment faire face à ce genre de problèmes et comment nous pouvons mieux nous protéger.

Le sénateur Pépin: Il y a un processus d'éducation et d'entraînement pour tout le monde.

M. Harlick: Exactement. Il faut que les gens prennent conscience du problème et qu'ils prennent connaissance des solutions. Au sein du gouvernement fédéral, nous sommes en train d'aider les ministères et les agences à résoudre les problèmes qui se trouvent dans leur réseau cybernétique. M. O'Bright, le

colleagues respond on a daily basis to questions and requests for assistance and support from other federal organizations with respect to threats to, or attacks on, their systems.

Also, with a view to protecting our critical national infrastructure outside of the federal government, we are currently in discussions with critical areas to determine what we can do together to protect their systems. We had one meeting with the electricity sector a week ago to exchange information and advice with a view to gaining a better understanding of the problem. We will also be addressing questions that have to do with the kind of training that is needed, so that we can better protect ourselves against such attacks and find appropriate technological solutions.

You also asked a question about criminal legislation here in Canada. According to my colleagues from the Department of Justice, the current provisions of the Criminal Code dealing with this sort of activity are relatively adequate for the time being. Parliament passed amendments to the Criminal Code four or five years ago. As you know, we can institute criminal proceedings against "Mafia Boy" here in Canada, whereas authorities in the Philippines were unable to proceed with charges against the person behind "Love Bug" virus. However, officials with the Justice Department are also aware that it is important to closely follow developments in computer technology, to ensure that our employees are able to deal with problems effectively. We can provide them with information based on our experiences.

[*English*]

Senator Forrestall: Could we deal with your structure, size, cost and the fact that you operate outside legislation as a line item of your own? Nevertheless, we want to know who you are and what you are doing. We must go to DND to search around for information. How big is your budget for critical infrastructure?

Mr. Harlick: The budget for the office has not yet been fixed; it is in the process of being considered at senior levels of government. As I mentioned before, we were initially Emergency Preparedness Canada, and now, in two small entities, we are operating off the A base of Emergency Preparedness Canada and supplemented by resources provided to us on an interim basis by the Department of National Defence, pending a final decision on our A base. That final number will be available when the department approaches Parliament for the Supplementary Estimates.

Senator Forrestall: Will we not see the numbers before then? You are as secretive as the rest of the bunch.

Mr. Harlick: I cannot predict what the figures will be.

Senator Forrestall: How many people do you envision for your staff when you are fully up and running one year from now? How large do you expect the organization to be?

Mr. Harlick: Again, that is a function of the amount of money we will receive. I would envisage that we will be in the range of 180 to 200 persons, maybe a bit higher.

directeur général des opérations, et ses collègues sont chaque jour occupés à répondre aux questions et aux demandes d'aide de soutien de la part des organisations fédérales quant à des menaces et des attaques dans leur système.

Également, pour protéger les infrastructures essentielles nationales, c'est-à-dire en dehors du gouvernement fédéral, nous sommes en discussion avec les secteurs essentiels pour déterminer ce que nous pouvons faire ensemble pour protéger leur système. Nous avons eu une réunion avec le secteur de l'électricité il y a une semaine pour échanger de l'information et des conseils dans le but d'avoir une meilleure connaissance du problème. Nous allons aussi aborder des questions qui traitent de l'entraînement nécessaire pour mieux nous protéger contre les attaques et pour trouver des solutions technologiques.

Vous avez également posé une question au sujet de la législation criminelle du Canada. Selon mes collègues du ministère de la Justice, les dispositions actuelles dans le Code criminel qui touchent ce genre de phénomène sont plus ou moins adéquates pour le moment. Le Parlement a adopté des amendements au Code criminel il y a quatre ou cinq ans. Comme vous savez, nous pouvons intenter des poursuites contre «Mafia Boy» ici au Canada alors que les autorités des Philippines ne pouvaient pas le faire contre la personne qui a créé le virus «Love Bug». Cependant, les gens du ministère de la Justice sont aussi conscients qu'il faut suivre de près l'évolution de la technologie s'assurer que nos employés sont en mesure de faire face aux problèmes. Nous pouvons leur donner de l'information basée sur nos expériences.

[*Traduction*]

Le sénateur Forrestall: Est-ce que nous pourrions parler de votre structure, de la taille de votre Bureau, des coûts et du fait que vous n'êtes assujetti à aucune loi? Quoi qu'il en soit, nous voulons savoir qui vous êtes et ce que vous faites. Il nous faut nous adresser au MDN pour obtenir l'information. De quel budget disposez-vous pour les infrastructures essentielles?

M. Harlick: Le budget du Bureau n'a pas encore été établi; il est à l'étude dans les hautes sphères du gouvernement. Comme je l'ai dit tout à l'heure, nous étions au départ Protection civile Canada, et maintenant, en deux petites entités, nous travaillons à partir du budget de services votés de Protection civile Canada et les ressources nous sont fournies de façon intérimaire par le ministère de la Défense nationale, en attendant une décision finale au sujet de notre budget. Le budget définitif sera disponible lorsque le ministère en fera la demande au Parlement au moment du vote sur les crédits supplémentaires.

Le sénateur Forrestall: Nous ne verrons donc pas les chiffres avant? Vous êtes aussi secret que tous les autres.

M. Harlick: Je ne peux prédire quels seront les chiffres.

Le sénateur Forrestall: Combien de personnes prévoyez-vous engager lorsque le Bureau sera pleinement opérationnel d'ici un an? Quelle sera la taille de votre organisation?

M. Harlick: Là encore, cela dépend des crédits que nous recevrons. Je dirais que nous serons entre 180 et 200 personnes, peut-être un peu plus.

Senator Forrestall: Do you anticipate being governed by legislation that supports the office? Or do you envision that you will remain under the legislation that generally supports the National Defence Act?

Mr. Harlick: We will want to look at that question. In our current legislative base, we look to the Emergency Preparedness Act which sets out responsibilities of the minister responsible for emergency preparedness, which, for the last number of years, has been the Minister of National Defence. The former EPC, as a branch of the Department of National Defence, derived its authorities and power and mandate from that source.

With the addition of critical infrastructure protection to the mandate of the government in this office, we will want to look at whether or not a legislative base would be desired or appropriate or necessary for the office. With the office being a part of DND and not a stand-alone agency, as I understand it, the usual practice in government may not be for it to require legislation, because it is part of another organization as opposed to a separate entity. We would want to look at that in the medium term. Now we are concentrating our efforts on getting staffed up to meet the challenges that we have today.

Senator Forrestall: How many do you have now?

Mr. Harlick: At the moment we would have about 110, 120. We are growing every day.

Senator Forrestall: Do you have a competent, professional cyber staff?

Mr. Harlick: We do, in fact. If the committee is interested, I can ask Mr. O'Bright to lay out the general components of his directorate, because that is where the threat analysis and incident response capability are located.

Senator Forrestall: I would like to hear that but, first, I have a question. A critical event in the Port of Halifax would not be disruption of the rail line because that can be fixed in 72 hours. Rather, if someone were to confuse the bills of lading for 8,000 or 10,000 containers, to the point where none of the contents or destinations are identified, that would be mischief of a major proportion. It would disrupt banking and irritate the directors and chief executives of many companies across the country. It would not endanger anyone, but it demonstrates how simple it would be to turn away critical business from the Port of Halifax.

Mr. Gary O'Bright, Director General, Operations, Office of Critical Infrastructure and Emergency Preparedness, Department of National Defence: The operations component of the new office will have five major parts. We are hoping that they will all work synergistically together.One part will deal with threat and incident analysis. We will not be front-line collectors of intelligence, for example, but we will hope to have close working relationships with the security service and others to receive their information. We will look at that information particularly in light of the impact on a particular sector, for example, the rail sector.

Le sénateur Forrestall: Prévoyez-vous être assujetti à une loi habilitante? Ou croyez-vous demeurer assujetti à la Loi sur la défense nationale?

M. Harlick: Nous allons examiner la question. Notre fondement législatif actuel relève de la Loi sur la protection civile qui détermine les responsabilités du ministre responsable de la protection civile. Ces dernières années, c'était le ministre de la Défense nationale. L'ancienne Protection civile Canada, en tant que direction du ministère de la Défense nationale, tirait ses pouvoirs et son mandat de cette source.

Avec l'ajout de la protection des infrastructures essentielles au mandat du gouvernement confié à notre Bureau, nous verrons s'il est souhaitable, approprié ou nécessaire que le Bureau soit assujetti à une loi habilitante. Si le Bureau est intégré au MDN et n'a pas le statut d'organisme autonome, d'après ce que je comprends, la pratique au gouvernement pourrait s'appliquer et nous ne serions pas dotés d'une loi parce que nous ferions partie d'une autre organisation et nous ne serions pas une entité distincte. Nous allons examiner la question à moyen terme. Pour l'instant, nous concentrons nos efforts sur l'embauche de personnel pour relever les défis que nous avons aujourd'hui.

Le sénateur Forrestall: Combien de personnes avez-vous maintenant?

M. Harlick: Pour l'instant, nous en avons environ 110 à 120. Le nombre augmente chaque jour.

Le sénateur Forrestall: Est-ce que vous avez un personnel professionnel et compétent en matière d'informatique?

M. Harlick: Effectivement. Si vous le voulez, je peux demander à M. O'Bright de décrire les composantes générales de sa direction parce qu'elle est responsable de l'analyse des menaces et de la réaction aux incidents.

Le sénateur Forrestall: J'aimerais bien entendre ce qu'il a à dire, mais d'abord j'aimerais poser une question. Un événement critique qui se produirait dans le port de Halifax ne perturberait pas le transport ferroviaire parce que le problème peut être réglé en 72 heures. Mais si quelqu'un brouillait les connaissements de 8 000 ou 10 000 conteneurs, au point où le contenu et la destination de ces conteneurs ne puissent plus être identifiés, nous aurions un problème majeur. Cela viendrait perturber les services bancaires, irriter les directeurs et les présidents-directeurs généraux de nombreuses entreprises de tout le pays. Cela ne mettrait pas la vie de personne en danger, mais montrerait qu'il serait facile de priver le port de Halifax d'une importante activité.

M. Gary O'Bright, directeur général, Opérations, Bureau de la protection des infrastructures essentielles et de la protection civile, ministère de la Défense nationale: La composante Opérations du nouveau Bureau comportera cinq éléments majeurs. Nous espérons que la synergie fonctionnera entre tous ces éléments. Un élément portera sur l'analyse des menaces et des incidents. Nous ne serons pas les premiers à recueillir les renseignements, par exemple, mais nous espérons entretenir d'étroites relations de travail avec le service de sécurité et d'autres services pour recevoir l'information. Nous allons

What is the threat? Where does it come from and what is its potential impact on that particular sector?

The second division within operations will deal with something we call the "mapping" of the national critical infrastructure. Mapping may be a slightly incorrect term but it is the best we could think of at the moment to imply that we will try to depict the infrastructures. What do they look like? In a physical world, a dam or a bridge does not usually move, so that is not so bad. As you move into the world of cyber, it is a significant challenge to map out infrastructure because networks are changed and reconstituted regularly by the owners or operators.

The third division of operations directorate will deal with vulnerabilities and dependencies. In this particular area, we will look at how the infrastructures interact with each other. The ice storm was an interesting example. The hydro was taken out but there were many other ripple effects across a variety of infrastructures. We are looking at how the infrastructures are connected and where they are at risk. That will all be in close cooperation, we expect, with the people who own and operate these systems.

The fourth division is essentially a planning division. We did some early work in the lead-up to the Summit of the Americas in April. A group of individuals, some from our organization and under the leadership of the RCMP, went to Quebec City to assess the information technology systems to be used by the participants. We were able to offer advice in terms of safeguarding those systems.

The final division within operations is the organization to which Mr. Harlick referred — a 24-hour, 7-days-a-week, 365-days-a-year coordination centre that will monitor events as they occur, be they physical or cyber. It will handle any issue that requires Canadians to be alerted to potential problems, issue advisories on evolving issues, and then coordinate federal responses to those particular problems as they occur, particularly the serious ones.

Senator Forrestall: Where are you physically located?

Mr. Harlick: At the present time, we are at Bank and Slater Streets in the Jackson building. That is where Emergency Preparedness Canada was located.

Senator Forrestall: If you had your 'druthers,' would you prefer the route you are taking now or to have your own legislation?

Mr. Harlick: At present, the implicit authorities and powers that we have as a part of DND are quite adequate. As I mentioned, we will review whether it is desirable or prudent, for a variety of reasons, to incorporate this responsibility and any of its associated requirements into a piece of legislation, a self-standing National

examiner cette information plus particulièrement à la lumière de l'impact qu'elle peut avoir sur un secteur en particulier, comme le secteur ferroviaire. Quelle est la menace? D'où vient-elle et quel est son impact potentiel sur ce secteur précis?

La deuxième division au sein des Opérations s'occupera de ce que l'on appelle la «cartographie» des infrastructures essentielles à l'échelle nationale. Le terme est peut-être légèrement inexact, mais c'est le meilleur auquel on peut penser pour l'instant pour indiquer que nous allons essayer de décrire les infrastructures. À quoi ressemblent-elles? Dans le monde réel, un barrage ou un pont ne déménage pas habituellement, donc c'est facile. Si on entre dans le cybermonde, ça devient plus compliqué de cartographier les infrastructures parce que les propriétaires ou les opérateurs changent et reconstituent régulièrement les réseaux.

La troisième division de la Direction des opérations s'occupera des vulnérabilités et des dépendances. À cet égard, nous chercherons à comprendre les interactions réciproques des infrastructures. La crise du verglas est un exemple intéressant. L'électricité était coupée, mais il y avait beaucoup d'autres effets multiplicateurs qui se sont fait sentir dans diverses infrastructures. Nous cherchons à voir comment les infrastructures sont reliées et où elles sont en danger. Tout le monde travaillera en étroite collaboration, nous l'espérons, avec les personnes qui possèdent et exploitent ces systèmes.

La quatrième division est essentiellement une division de planification. Nous avons fait certains travaux préalables avant le Sommet des Amériques en avril. Un groupe de personnes, quelques-unes provenant de notre organisation et sous la direction de la GRC, se sont rendues à Québec pour évaluer les systèmes informatiques à la disposition des participants. Nous avons pu donner des conseils relativement à la protection de ces systèmes.

La dernière division est celle dont a parlé M. Harlick — c'est-à-dire un Centre de coordination 24 heures sur 24, sept jours sur sept, 365 jours sur 365 qui surveillera les événements au fur et à mesure qu'ils se déroulent, qu'ils soient matériels ou virtuels. Le Centre s'occupera de toute question qui exige de prévenir les Canadiens contre les problèmes susceptibles de les menacer, d'émettre des avis sur l'évolution des dangers et de coordonner ensuite les réactions du gouvernement fédéral face aux problèmes particuliers au fur et à mesure qu'ils se produisent, surtout les problèmes graves.

Le sénateur Forrestall: Où sont vos locaux?

M. Harlick: Actuellement, nous sommes à l'angle de Bank et Slater, dans l'édifice Jackson. C'est là qu'étaient les locaux de Protection civile Canada.

Le sénateur Forrestall: Si vous aviez votre mot à dire, préféreriez-vous la voie que vous empruntez maintenant ou avoir votre propre loi?

M. Harlick: Actuellement, les pouvoirs implicites que nous avons en tant qu'élément du MDN sont adéquats. Comme je l'ai dit, nous allons examiner s'il est souhaitable et prudent, pour diverses raisons, d'incorporer cette responsabilité et toutes les exigences connexes en une mesure législative, une loi autonome

Defence Act or whatever. For the moment we see no problems in doing what we must do within the current legislative context.

Senator Forrestall: If you can do something about cyber problems, I frankly do not care what it costs — just do it. Good luck.

Mr. Harlick: Your example about bills of lading in Halifax is a very good one. Many people in the surface transport world or even in air transport think of it as nothing more than an information transportation world. The actual, physical goods themselves are so often tracked by networks and systems that the information system is, in fact, a very significant area of vulnerability, as would be supervisory control and acquisition systems for pipelines. What makes a pipeline run but the electricity and the telecommunications riding on it? People in that industry are well aware of that, too. The question was examined in Y2K and we will be looking at it further in our examination of the transportation sector in Canada.

The Chairman: Mr. Harlick, could you tell the committee what the payment formula arrangement is with the provinces in the event of a natural disaster?

Mr. Harlick: I may turn to Mr. Bartley for the fine details but the government has put into place disaster financial assistance arrangements which are federal government arrangements to compensate provinces and municipalities for expenditures they make to restore property, businesses, homes, to the condition they were in previous to a disaster like a flood, an ice storm or a tornado.There is a formula in the DFAA, or Disaster Financial Assistance Arrangements, to get at that. The formula starts by saying that it is the responsibility of a province to pick up the tab up to a cost of $1 per capita of the population of the given province. If the province is 4 million strong, then it picks up the first $4 million. There is a scale on which the feds pick up an increasing proportion of the cost. In the large disasters, the figure is 90 cents of every dollar of eligible expenditures. There is a 90/10 split at that point.

The Chairman: Following on Senator Wiebe's comments, when people first hear the name of your organization, do they think of you as being in charge of any emergency; would that be fair to say?

Mr. Harlick: No, it would not. However, the office could well be in charge of handling a national emergency on behalf of the federal government.

The Chairman: Are you able to give us an example of what you would be in charge of?

Mr. Harlick: This derives from ministerial accountability and responsibility. If the Minister of National Defence were responsible for leading the federal government's response to a given emergency, then he would be able to rely on the office as well as on the rest of DND and the Canadian Forces to do so.

sur la Défense nationale ou quelque chose du genre. Pour l'instant, nous ne voyons aucun problème à faire ce que nous devons faire en vertu de la loi actuelle.

Le sénateur Forrestall: Si vous pouvez faire quelque chose au sujet des cyberproblèmes, franchement, les coûts m'importent peu, allez-y tout simplement. Bonne chance.

M. Harlick: Votre exemple au sujet des connaissements à Halifax est bien choisi. Beaucoup de gens dans le monde des transports de surface ou même du transport aérien voient ce monde comme rien d'autre qu'un mode de transport de l'information. Les biens matériels comme tels sont si souvent repérés par les réseaux et les systèmes que le système d'information est, en fait, très vulnérable, tout comme le seraient le contrôle de la surveillance et les systèmes d'acquisition pour les pipelines. Qu'est-ce qui fait qu'un pipeline est exploité si ce n'est de l'électricité et des télécommunications? Les gens de l'industrie en sont très conscients aussi. La question a été examinée lors du bogue de l'an 2000 et nous allons pousser la recherche dans notre examen du secteur du transport au Canada.

Le président: Monsieur Harlick, pouvez-vous dire au comité quelle formule de paiement vous avez conclue avec les provinces en cas de catastrophe naturelle?

M. Harlick: Je vais peut-être demander à M. Bartley de vous donner les détails, mais le gouvernement a mis en place des ententes d'aide financière en cas de catastrophe. Il s'agit d'ententes fédérales en vue de compenser les provinces et les municipalités pour les dépenses qu'elles engagent afin de restaurer des biens, des entreprises, des maisons, dans leur état originel précédant une catastrophe comme une inondation, une crise du verglas ou une tornade. Les Accords d'aide financière en cas de catastrophe prévoient une formule à ce sujet. Elle prévoit que la province a la responsabilité de payer les coûts jusqu'à concurrence de 1 dollar par tête d'habitant de la province. Si la province compte 4 millions d'habitants, elle assume alors les 4 premiers millions de dollars de dépenses. Ensuite, il y a une échelle selon laquelle le gouvernement fédéral assume une proportion plus grande des coûts. Dans les grandes catastrophes naturelles, c'est 90 cents au dollar de dépenses admissibles. Il y a à ce moment-là proportion de 90/10.

Le président: Pour faire suite aux commentaires du sénateur Wiebe, lorsque les gens entendent le nom de votre organisation pour la première fois, n'est-il pas juste de dire qu'ils ont l'impression que vous êtes responsables des urgences?

M. Harlick: Non, quoique le Bureau pourrait très bien être chargé de s'occuper d'une urgence nationale au nom du gouvernement fédéral.

Le président: Pouvez-vous nous donner un exemple?

M. Harlick: Cela découle de la responsabilité ministérielle. Si on confiait au ministre de la Défense nationale la responsabilité de diriger la réaction du gouvernement fédéral à une urgence donnée, à ce moment-là il pourrait s'en remettre à notre Bureau et aux autres éléments du MDN et des Forces canadiennes pour faire le travail.

For example, during an ice storm or a flood, the office would be looking at trying to coordinate the provision of federal assistance to the impacted province.

The Chairman: Coordinate, not direct; is that correct?

Mr. Harlick: That is correct. Especially in the emergency preparedness world, the jurisdiction primarily responsible for responding to public emergencies is the province. When their capacity is overloaded, or they need specialized assistance which the federal government can give, that request for assistance and flow comes from them through the regional offices to this office, which coordinates measures and assures delivery, to the extent that the federal government has that capability of assistance, to the region.

The Chairman: As I understand your role, it is an important one. To a large extent your role is one of discussion, consultation, persuasion and planning. That sort of effort is very useful. There is a tendency for one to say, "Here are the folks in charge and they will make everything happen." However, that is not really how you see your role, is it?

Mr. Harlick: I do not exclude that, sir. The office has the ability to act. For example, with respect to a cyber problem. In the last couple of weeks, we have been giving very good, direct advice to departments who have had a cyber attack on their systems: do this, fix that, see this as a source of information. That is not just saying, "Oh, we will hold your hand."

The Chairman: I get terrific advice from my office, but I am the one who decides. Are you saying that you decide what the department should do?

Mr. Harlick: No. That is important for purposes of accountability. To echo Senator Wiebe's earlier concern, it is impossible, either in the emergency preparedness world or the critical infrastructure world, for an office like ours to ride to the rescue on every issue at every time.

Particularly in the cyber world, the people who know their systems and what the problems are and have the responsibility to fix them are those who own them and are responsible for them. The challenge is when they do not know what to do; otherwise they would not phone us, they would fix the problem if they could, or call their supplier. When they come to us, they are getting close to the end of their tether; it is spilling over, it is causing problems for them. They want advice beyond the box. That is what we are organized to do. We can pull on and from within the Canadian government, as well as within the private sector, expert advice to deal with this new variant of worm or virus in respect to this kind of system and give them advice on how they might fix it.

The Chairman: You are advice providers, then?

Mr. Harlick: Pretty much.

The Chairman: Do you plan to do an evaluation of the top 100 events that might happen to critical infrastructure and the impacts that could flow from those events?

Par exemple, lors d'un verglas ou d'une inondation, le Bureau pourrait coordonner la prestation de l'aide fédérale à la province touchée.

Le président: Coordonner, non pas diriger, est-ce exact?

M. Harlick: C'est exact. Surtout dans le domaine de la protection civile, c'est la province qui est la première responsable de réagir à une urgence publique. Lorsqu'elle n'y arrive plus, ou qu'elle a besoin d'aide spécialisée que le gouvernement fédéral peut fournir, la province fait alors parvenir sa demande à l'administration régionale de notre Bureau, et c'est ce dernier qui coordonne les interventions et assure la prestation d'aide à la région, dans la mesure où le gouvernement fédéral a la capacité nécessaire d'intervenir.

Le président: D'après ce que je comprends, vous jouez un rôle important. Dans un sens large, votre rôle est un rôle de discussion, de consultation, de persuasion et de planification. Ce travail est très utile. Les gens ont tendance à dire: «Voici les personnes qui sont responsables et qui vont s'occuper de tout.» Mais ce n'est pas vraiment votre perception de votre rôle, n'est-ce pas?

M. Harlick: Je n'exclus pas cela non plus, monsieur. Le Bureau a la capacité d'agir. Prenons le cas d'un cyberproblème. Au cours des dernières semaines, nous avons donné des conseils judicieux et directs aux ministères qui ont subi une cyberattaque: faites ceci, réparez cela, consultez telle ou telle source d'information. On n'a pas juste servi de canne blanche.

Le président: Je reçois d'excellents conseils de mon bureau, mais c'est moi qui décide. Êtes-vous en train de me dire que vous décidez de ce que le ministère devrait faire?

M. Harlick: Non. C'est important pour des fins de responsabilité. Pour faire écho à la préoccupation du sénateur Wiebe, il est impossible, soit dans le monde de la protection civile ou des infrastructures essentielles, qu'un bureau comme le nôtre se porte au secours de tout le monde chaque fois.

Plus particulièrement, dans le monde cybernétique, les gens qui connaissent leurs systèmes et les problèmes et qui ont la responsabilité de les réparer sont ceux qui en sont les propriétaires et qui en ont la responsabilité. Le problème, c'est lorsqu'ils ne savent pas quoi faire. S'ils le savaient, ils ne nous appelleraient pas, ils régleraient le problème s'ils le pouvaient, ou ils consulteraient leurs fournisseurs. Lorsqu'ils s'adressent à nous, c'est qu'ils sont pratiquement au bout de leur rouleau, ça déborde, les problèmes se multiplient. Ils cherchent de l'aide ailleurs. C'est notre champ d'intervention. Nous pouvons obtenir, du gouvernement canadien tout autant que du secteur privé, les conseils d'experts pour exterminer cette nouvelle variante de ver ou de virus qui attaque ce genre de système et donner des conseils pour le restaurer.

Le président: Vous donnez donc des conseils?

M. Harlick: C'est exact.

Le président: Prévoyez-vous faire une évaluation des 100 principaux dangers qui pourraient perturber les infrastructures essentielles, et des répercussions de ces dangers?

Mr. Harlick: We have no explicit plan to do that, as of today, but it is quite likely we will do something like that. That was what was done in a very crude way during Y2K. A number of experts under the auspices of a national contingency planning group sat down and developed a matrix on what are the critical infrastructures, what is the criticality of each of those, and what is their degree of interdependency with each other. In other words, if something happened here, what would be the impact over there?

That is what Mr. O'Bright was talking about when he spoke about vulnerability and dependency analysis. When you put that in the context of a geographic area of the country, or a system or network, that is what you map. Where is that infrastructure, what is its criticality and interdependency? If you have good hardware and software, you can game out what might happen if there is a failure here, what would be the consequences on a region, a people, a sector or an industry. That is important to do. We will do that and, in a way, we will end up doing 30 or 50 scenarios about what would happen. That informs the infrastructure owners and us as to what could happen. They then apply a risk analysis to that based on what might be happening in their area. That engages them in putting up appropriate protective measures. We will be working in that area. You are bang on there.

The Chairman: Mr. Harlick, I would like to thank you and your colleagues for an interesting presentation today. It gave the committee a good insight into the work that you are doing.

This portion of the meeting is now adjourned and the committee will now move to an *in camera* session.

The committee continued *in camera*.

M. Harlick: Nous n'avons pas de plan précis à cet égard, au moment où on se parle, mais c'est fort possible que nous nous engagions dans cette direction. C'est ce qui a été fait de façon rudimentaire pour le bogue de l'an 2000. Un certain nombre de spécialistes, sous les auspices d'un groupe de planification d'urgence à l'échelle nationale, se sont rencontrés et ont conçu une matrice sur la nature des infrastructures essentielles, le caractère de chacune, et leur degré d'interdépendance réciproque. Autrement dit, si quelque chose frappe une infrastructure, quel en est l'impact sur les autres?

C'est ce à quoi faisait allusion M. O'Bright lorsqu'il a parlé d'analyse des vulnérabilités et des dépendances. Quand on considère le contexte d'une aire géographique du pays, ou un système ou un réseau, on cartographie les infrastructures. Quelle est cette infrastructure, quels sont son caractère essentiel et son interdépendance? Si vous avez du bon matériel et de bons logiciels, vous pouvez deviner ce qui pourrait se produire en cas de panne à cet endroit, quelles seraient les conséquences pour la région, les gens, tel secteur ou telle industrie. C'est important de le faire. Nous le ferons et nous allons finalement nous retrouver à élaborer 30 ou 50 scénarios d'éventualités. Ces scénarios informeront les propriétaires des structures et le Bureau sur les conséquences possibles. Les propriétaires effectueront alors une analyse de risques en se fondant sur ce qui pourrait se produire dans leur région. Ils adopteront les mesures de protection appropriées. Nous allons travailler dans ce domaine. Vous avez tout à fait raison.

Le président: Monsieur Harlick, je tiens à vous remercier ainsi que vos collègues de cette intéressante présentation. Vous avez donné au comité un bon aperçu de ce que vous êtes en train de faire.

Cette partie de la réunion est terminée et le comité siégera maintenant à huis clos.

La séance se poursuit à huis clos.

WITNESSES—TÉMOINS

Thursday, July 19, 2001 (morning session)

From the Department of the Solicitor General:

Mr. Michel D'Avignon, Director General, National Security, Policing and Security Branch;

Ms Annie Leblanc, Acting Director, Technology and Lawful Access Division;

Mr. Mike Theilmann, Acting Director, Counter-Terrorism Division.

From the Royal Canadian Mounted Police:

Superintendent J. Wayne Pilgrim, Officer in Charge, National Security Investigations Branch, Criminal Intelligence Directorate.

Thursday, July 19, 2001 (afternoon session)

From the Department of National Defence:

Mr. James Harlick, Assistant Deputy Minister, Office of Critical Infrastructure Protection and Emergency Preparedness;

Mr. Gary O'Bright, Director General, Operations, Office of Critical Infrastructure Protection and Emergency Preparedness;

Mr. Alan Bartley, Director General, Policy Planning and Readiness, Office of Critical Infrastructure Protection and Emergency Preparedness.

Le jeudi 19 juillet 2001 (séance de l'avant-midi)

Du ministère du Solliciteur général:

M. Michel D'Avignon, directeur général, Sécurité nationale, Secteur de la police et de la sécurité;

Mme Annie Leblanc, directrice intérimaire, Division de la technologie et de l'accès légal;

M. Mike Theilmann, directeur intérimaire, Division de la lutte contre le terrorisme.

De la Gendarmerie royale du Canada:

Le surintendant J. Wayne Pilgrim, officier responsable de la Sous-direction des enquêtes relatives à la sécurité nationale, Direction des renseignements criminels.

Le jeudi 19 juillet 2001 (séance de l'après-midi)

Du ministère de la Défense nationale:

M. James Harlick, sous-ministre adjoint, Bureau de la protection des infrastructures essentielles et de la protection civile;

M. Gary O'Bright, directeur général, Opérations, Bureau de la protection des infrastructures essentielles et de la protection civile;

M. Alan Bartley, directeur général, Planification des politiques et disponibilité opérationnelle, Bureau de la protection des infrastructures essentielles et de la protection civile.

Available from:
Public Works and Government Services Canada — Publishing
Ottawa, Ontario K1A 0S9

En vente:
Travaux publics et Services gouvernementaux Canada — Édition
Ottawa, Canada K1A 0S9