SENATE SÉNAT

CANADA

First Session
Forty-first Parliament, 2011-12

Première session de la
quarante et unième législature, 2011-2012

Proceedings of the Standing Senate Committee on

NATIONAL SECURITY AND DEFENCE

Chair:
The Honourable PAMELA WALLIN

Monday, November 5, 2012
Monday, November 19, 2012

Issue No. 10

Fifteenth and sixteenth meetings on:

Canada's national security and defence policies, practices, circumstances and capabilities

WITNESSES:
(*See back cover*)

Délibérations du Comité sénatorial permanent de la

SÉCURITÉ NATIONALE ET DE LA DÉFENSE

Présidente :
L'honorable PAMELA WALLIN

Le lundi 5 novembre 2012
Le lundi 19 novembre 2012

Fascicule n^{o} 10

Quinzième et seizième réunions concernant :

Les politiques, les pratiques, les circonstances et les capacités du Canada en matière de sécurité nationale et de défense

TÉMOINS :
(*Voir à l'endos*)

49784-49814

STANDING SENATE COMMITTEE
ON NATIONAL SECURITY AND DEFENCE

The Honourable Pamela Wallin, *Chair*

The Honourable Roméo Antonius Dallaire, *Deputy Chair*

and

The Honourable Senators:

* Cowan (or Tardif)	Manning
Dawson	Mitchell
Day	Nolin
Lang	Plett
* LeBreton, P.C. (or Carignan)	

* Ex officio members

(Quorum 4)

Changes in membership of the committee:

Pursuant to rule 12-5, membership of the committee was amended as follows:

The Honourable Senator Plett replaced the Honourable Senator Johnson (*November 7, 2012*).

The Honourable Senator Johnson replaced the Honourable Senator Plett (*November 5, 2012*).

The Honourable Senator Nolin replaced the Honourable Senator Boisvenu (*October 30, 2012*).

COMITÉ SÉNATORIAL PERMANENT
DE LA SÉCURITÉ NATIONALE ET DE LA DÉFENSE

Présidente : L'honorable Pamela Wallin

Vice-président : L'honorable Roméo Antonius Dallaire

et

Les honorables sénateurs :

* Cowan (ou Tardif)	Manning
Dawson	Mitchell
Day	Nolin
Lang	Plett
* LeBreton, C.P. (ou Carignan)	

* Membres d'office

(Quorum 4)

Modifications de la composition du comité :

Conformément à l'article 12-5 du Règlement, la liste des membres du comité est modifiée, ainsi qu'il suit :

L'honorable sénateur Plett a remplacé l'honorable sénateur Johnson (*le 7 novembre 2012*).

L'honorable sénateur Johnson a remplacé l'honorable sénateur Plett (*le 5 novembre 2012*).

L'honorable sénateur Nolin a remplacé l'honorable sénateur Boisvenu (*le 30 octobre 2012*).

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

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

MINUTES OF PROCEEDINGS

OTTAWA, Monday, November 5, 2012
(20)

[*English*]

The Standing Senate Committee on National Security and Defence met this day at 4 p.m., in room 2, Victoria Building, the chair, the Honourable Pamela Wallin, presiding.

Members of the committee present: The Honourable Senators Dallaire, Dawson, Day, Johnson, Lang, Manning, Mitchell, Nolin, and Wallin (9).

In attendance: Holly Porteous, Analyst, Parliamentary Information and Research Service, Library of Parliament.

Also present: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Wednesday, June 22, 2011, the committee continued its study of Canada's national security and defence policies, practices, circumstances and capabilities. (*For complete text of the order of reference, see proceedings of the committee, Issue No. 1.*)

WITNESSES:

National Defence:

Brigadier-General Greg Loos, Director General Cyber, Chief of Force Development;

Brigadier-General Roberto Mazzolin, Director General, Information Management Operations.

Communications Security Establishment Canada:

John Forster, Chief;

Toni Moffa, Deputy Chief, IT Security.

Brigadier-General Loos made a statement and, together with Brigadier-General Mazzolin, the witnesses answered questions.

At 5:04 p.m., the committee suspended.

At 5:06 p.m., the committee resumed.

Mr. Forster made a statement and, together with Ms. Moffa, the witnesses answered questions.

At 6:02 p.m., the committee adjourned to the call of the chair.

ATTEST:

PROCÈS-VERBAUX

OTTAWA, le lundi 5 novembre 2012
(20)

[*Traduction*]

Le Comité sénatorial permanent de la sécurité nationale et de la défense se réunit aujourd'hui, à 16 heures, dans la pièce 2 de l'édifice Victoria, sous la présidence de l'honorable Pamela Wallin, (*présidente*).

Membres du comité présents : Les honorables sénateurs Dallaire, Dawson, Day, Johnson, Lang, Manning, Mitchell, Nolin et Wallin (9).

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

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mercredi 22 juin 2011, le comité poursuit son étude des politiques, des pratiques, des circonstances et des capacités du Canada en matière de sécurité nationale et de défense. (*Le texte intégral de l'ordre de renvoi figure fascicule nº 1 des délibérations du comité.*)

TÉMOINS :

Défense nationale :

Brigadier-général Greg Loos, directeur général Cybersécurité, chef, Développement des forces;

Brigadier-général Roberto Mazzolin, directeur général, Opérations de la gestion de l'information.

Centre de la sécurité des télécommunications Canada :

John Forster, chef;

Toni Moffa, chef adjointe, Sécurité des TI.

Le brigadier-général Loos fait une déclaration et, avec le brigadier-général Mazzolin, répond aux questions.

À 17 h 4, la séance est suspendue.

À 17 h 6, la séance reprend.

M. Forster fait une déclaration et, avec Mme Moffa, répond aux questions.

À 18 h 2, le comité s'ajourne jusqu'à nouvelle convocation par la présidence.

ATTESTÉ :

OTTAWA, Monday, November 19, 2012
(21)

[*English*]

The Standing Senate Committee on National Security and Defence met this day at 4:02 p.m., in room 2, Victoria Building, the chair, the Honourable Pamela Wallin, presiding.

Members of the committee present: The Honourable Senators Dallaire, Dawson, Day, Lang, Manning, Mitchell, Nolin, Plett and Wallin (9).

In attendance: Holly Porteous, Analyst, Parliamentary Information and Research Service, Library of Parliament.

Also present: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Wednesday, June 22, 2011, the committee continued its study of Canada's national security and defence policies, practices, circumstances and capabilities. (*For complete text of the order of reference, see proceedings of the committee, Issue No. 1.*)

WITNESSES:

National Defence:

Brigadier-General Rick Pitre, Director General Space;

Colonel André Dupuis, Director of Space Requirements.

As an individual:

James A. Boutilier, Professor, Centre for Asia-Pacific Initiatives, University of Victoria, Special Advisor (Policy) at the Maritime Forces Pacific.

The chair made a statement.

Brigadier-General Pitre made a statement and, together with Colonel Dupuis, the witnesses answered questions.

At 5:06 p.m., the committee suspended.

At 5:12 p.m., the committee resumed.

Mr. Boutilier made a statement and answered questions.

At 6:04 p.m., the committee adjourned to the call of the chair.

ATTEST:

OTTAWA, le lundi 19 novembre 2012
(21)

[*Traduction*]

Le Comité sénatorial permanent de la sécurité nationale et de la défense se réunit aujourd'hui, à 16 h 2, dans la pièce 2 de l'édifice Victoria, sous la présidence de l'honorable Pamela Wallin, (*présidente*).

Membres du comité présents : Les honorables sénateurs Dallaire, Dawson, Day, Lang, Manning, Mitchell, Nolin, Plett et Wallin (9).

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

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mercredi 22 juin 2011, le Comité poursuit son étude des politiques, des pratiques, des circonstances et des capacités du Canada en matière de sécurité nationale et de défense. (*Le texte intégral de l'ordre de renvoi figure au fFascicule nº 1 des délibérations du comité.*)

TÉMOINS :

Défense nationale :

Brigadier-général Rick Pitre, directeur général Espace;

Colonel André Dupuis, directeur du développement de l'espace.

À titre personnel :

James A. Boutilier, professeur, Centre for Asia-Pacific Initiatives, Université de Victoria, conseiller spécial (politiques) auprès des Forces maritimes du Pacifique.

La présidente fait une déclaration.

Le brigadier-général Pitre fait une déclaration et, avec le colonel Dupuis, répond aux questions.

À 17 h 6, la séance est suspendue.

À 17 h 12, la séance reprend.

M. Boutilier fait une déclaration et répond aux questions.

À 18 h 4, le comité s'ajourne jusqu'à nouvelle convocation par la présidence.

ATTESTÉ :

La greffière du comité,

Josée Thérien

Clerk of the Committee

EVIDENCE

OTTAWA, Monday, November 5, 2012

The Standing Senate Committee on National Security and Defence met this day at 4 p.m. to examine and report on Canada's national security and defence policies, practices, circumstances and capabilities.

Senator Pamela Wallin (*Chair*) in the chair.

[*English*]

The Chair: Ladies and gentlemen, welcome to the meeting of the Standing Senate Committee on National Security and Defence.

We will continue our look at the issue of cyber security as we did last week at the committee. A little later on we will hear from the chief of the Communications Security Establishment Canada, but we begin today by looking at the cyber safety and security issue inside the Department of National Defence. Public Safety, as we are trying to explain, is Canada's lead department for cyber security, and officials told us last week that about $155 million in new cyber spending has now been agreed to. Their role is also to coordinate cyber security within the government and with the private sector.

However, National Defence also plays a cyber role, and last spring a new cyber directorate was set up in that department. So far our main ally, the United States, has taken a slightly different approach. In the military, they have declared cyberspace to be a new military domain — along with land, sea, aerospace — with its own cyber command. We will look at different approaches to this today.

From the Department of National Defence, I would like to welcome Brigadier-General Greg Loos, Director General Cyber, Chief of Force Development; and Brigadier-General Roberto Mazzolin, Director General, Information Management Operations.

Welcome, gentlemen. We are glad to have you here at committee. I understand Brigadier-General Loos has an opening statement.

[*Translation*]

Brigadier-General Greg Loos, Director General Cyber, Chief of Force Development, National Defence: Thank you, Madam Chair. Hello, I am the Director General Cyberspace responsible for the force development of the Canadian Forces cyber capabilities. I

TÉMOIGNAGES

OTTAWA, le lundi 5 novembre 2012

Le Comité sénatorial permanent de la sécurité nationale et de la défense se réunit aujourd'hui, à 16 heures, pour examiner, en vue d'en faire rapport, les politiques, pratiques, circonstances et capacités du Canada en matière de sécurité nationale et de défense.

Le sénateur Pamela Wallin (*présidente*) occupe le fauteuil.

[*Traduction*]

La présidente : Mesdames et messieurs, je vous souhaite la bienvenue au Comité sénatorial permanent de la sécurité nationale et de la défense.

Nous reprenons notre examen de la cybersécurité, que nous avons amorcé à la réunion de la semaine dernière. Un peu plus tard, nous entendrons le chef du Centre de la sécurité des télécommunications du Canada, mais nous commençons aujourd'hui par examiner les questions de la cybersécurité et de la sécurité à l'intérieur du ministère de la Défense nationale. Comme nous tentons de l'expliquer, c'est le ministère de la Sécurité publique qui est le principal responsable de la cybersécurité au Canada. Ses fonctionnaires nous ont dit la semaine dernière qu'une somme d'environ 155 millions de dollars, en argent frais, avait été approuvée à ce chapitre. Leur rôle consiste aussi à coordonner la cybersécurité au sein du gouvernement et avec le secteur privé.

Toutefois, le ministère de la Défense nationale joue également un rôle à cet égard. Au printemps dernier, une nouvelle Direction de la cybersécurité a été mise sur pied au sein du ministère. Jusqu'à maintenant, notre principal allié, les États-Unis, a adopté une approche légèrement différente. Au sein des forces, les États-Unis ont établi le cyberespace comme étant un nouveau domaine militaire — au même titre que les éléments terre, mer et aérospatiale — doté de son propre cybercommandement. Nous examinerons aujourd'hui différentes approches possibles à cet égard.

Je souhaite la bienvenue au brigadier-général Greg Loos, directeur général de la Cybersécurité et chef du Développement de la force, et au brigadier-général Roberto Mazzolin, directeur général des Opérations de la gestion de l'information, tous deux du ministère de la Défense nationale.

Bienvenue, messieurs. Nous sommes heureux de vous accueillir à notre comité. Je crois comprendre que le brigadier-général Loos désire faire une déclaration préliminaire.

[*Français*]

Brigadier-général Greg Loos, directeur général Cybersécurité, chef, Développement des forces, Défense nationale : Merci, madame la présidente. Bonjour, je suis le directeur général cyberespace responsable du développement de la force affectée

am pleased to be given the opportunity to provide this committee with an overview of my organization, including its establishment, role and future plans.

[*English*]

Joining me at the table is Brigadier-General Roberto Mazzolin, who is responsible for most of our current cyber capabilities, our network operators and defenders, strategic military signals intelligence and the CF electronic warfare support unit.

[*Translation*]

I would like to begin by situating our efforts within the context of the whole-of-government approach to cyber security.

As you will be aware, Public Safety Canada is the Government of Canada lead on cyber security. Public Safety Canada developed and leads the implementation of Canada's first national Cyber Security Strategy, issued about two years ago.

The three pillars of the Strategy are: securing government systems, partnering to secure vital systems outside government, and helping Canadians to be safe online.

[*English*]

The strategy calls on the Department of National Defence and Canadian Forces to strengthen our capacity to defend our own networks, work with other government departments to identify threats and possible responses, and work with allies to exchange best practices and develop policy and frameworks for the military aspects of cyber security. Maintaining and strengthening the defence of DND/CF networks is a top priority for my organization in collaboration with the Communications Security Establishment Canada and Shared Services Canada. However, it is also my responsibility to develop the capability for the CF to operate more effectively in the cyber environment writ large. The *Canada First* Defence Strategy stipulated in June 2008 that the Canadian Forces requires core capabilities and flexibility to successfully address both conventional and asymmetric threats, including cyber attacks. As I will explain in a moment, the Canadian Forces must be able to operate as effectively in the cyber environment as it does on land, on and under the water, and in air and space.

[*Translation*]

Before describing what I mean by this, allow me take a step back and explain the origins and specific mandate of my organization.

aux capacités cybernétiques des Forces armées canadiennes. Je suis ravi qu'on me donne la possibilité de donner aux membres de ce comité un aperçu de mon organisation, y compris son effectif, son rôle et ses plans d'avenir.

[*Traduction*]

Je suis accompagné par le brigadier-général Roberto Mazzolin, qui est responsable de la plupart de nos capacités cybernétiques actuelles : les opérateurs et défenseurs de nos réseaux, le renseignement stratégique militaire d'origine électromagnétique ainsi que l'unité de soutien en matière de guerre électronique des Forces canadiennes.

[*Français*]

J'aimerais, en premier lieu, situer nos efforts dans le contexte de l'approche pangouvernemental de la sécurité cybernétique.

Comme vous le savez, Sécurité publique Canada est le chef de file du gouvernement du Canada en matière de cybersécurité. Sécurité publique Canada a élaboré et dirige la mise en œuvre de la première stratégie nationale du Canada en matière de sécurité cybernétique en vigueur depuis environ deux ans.

Les trois piliers de la stratégie sont les suivants : protéger les systèmes gouvernementaux, établir des partenariats pour assurer la sécurité des systèmes vitaux à l'extérieur du gouvernement et aider les Canadiens à naviguer en ligne en toute sécurité.

[*Traduction*]

La stratégie fait appel au ministère de la Défense nationale et aux Forces canadiennes pour renforcer notre capacité de défendre nos propres réseaux, collaborer avec d'autres ministères pour déceler les menaces cybernétiques et les réactions possibles, et travailler avec nos alliés pour échanger des pratiques exemplaires et élaborer des politiques et des cadres juridiques liés aux aspects militaires de la sécurité cybernétique. Le maintien et le renforcement de la défense des réseaux du MDN et des FC sont des activités hautement prioritaires de mon organisation, en collaboration avec le Centre de la sécurité des télécommunications du Canada et Services partagés Canada. Mais je suis aussi responsable d'accroître la capacité des Forces canadiennes d'opérer plus efficacement dans l'environnement cybernétique au sens large. La Stratégie de défense *Le Canada d'abord* affirmait, en juin 2008, que les Forces canadiennes ont besoin des capacités fondamentales et de la souplesse requises pour contrer les menaces conventionnelles et asymétriques, notamment les cyberattaques. Comme je l'expliquerai dans un moment, les Forces canadiennes doivent être en mesure d'opérer aussi efficacement dans l'environnement cybernétique qu'elles le font sur terre, sur et dans la mer, et dans l'espace aérien.

[*Français*]

Avant de décrire ce que j'entends par là, permettez-moi de revenir en arrière et d'expliquer les origines et les mandats précis de mon organisation.

In September 2010, the Canadian Forces established an ad hoc Cyber Task Force to determine the military's cyber requirements. Its mandate was to optimize current cyber-related capabilities while setting the conditions for the force development, force generation and force employment of future cyber capabilities, with capabilities being defined as people, processes and equipment or tools.

One of its first tasks was to develop a coherent definition of the cyber environment and to conceptualize what it means for the military to operate within that environment.

[*English*]

In April 2011, the Chief of the Defence Staff established a permanent DG cyberspace organization belonging to the Vice Chief of the Defence Staff and reporting directly to the Chief of Force Development, Rear-Admiral Lloyd, who spoke here last month. As that DG, I am responsible for the Director Cyber Force Development. This directorate is tasked primarily with identifying and developing future cyber capabilities, including continuing critical conceptual work and designing and building cyber capabilities. It incorporates the Canadian Forces Cyber Task Force with ongoing support from Level 1 organizations across DND/CF. These organizations are branches headed by assistant deputy ministers or their military equivalents.

Let me skip to my organization's work plan. It is organized along four lines of effort. First is a policy line. Along with our ADM(Pol) team, we provide input to Public Safety Canada on the implementation of the Canada's Cyber Security Strategy as well as informing policy development regarding the role of the military in the cyber environment. Second is command and control, including designing an authority, responsibility and accountability regime for cyber capabilities to be led by operational commanders. Much like the national Cyber Security Strategy, our approach is to avoid treating anything cyber as fundamentally new and instead seek to integrate our cyber activities into existing planning and operational frameworks as fully as possible.

The third line is capability building, including ensuring that resources are appropriately focused on core functions and helping to synchronize the force's various cyber-related programs. A top priority for strengthening our cyber capability within the Canadian Forces is to provide commanders with a common operating picture and improved situational awareness of their cyber environment to enable more timely and informed decision making. Finally and most importantly is human resources and training through the definition of training requirements,

En septembre 2010, les forces canadiennes ont créé un groupe de travail spécial sur la cybernétique pour établir les besoins militaires dans ce domaine. Son mandat consistait à optimiser les capacités actuelles en matière de cybernétique tout en mettant en place les conditions nécessaires au développement, à la mise sur pied et à l'utilisation des forces en ce qui a trait aux capacités futures en matière de cybernétique. Les capacités étant définies comme les gens, les processus et l'équipement ou outils.

L'une de ses premières tâches a consisté à élaborer une définition cohérente de l'environnement cybernétique et à conceptualiser l'intervention des forces armées dans cet environnement.

[*Traduction*]

En avril 2011, le chef d'état-major de la Défense a créé au sein du groupe du vice-chef d'état-major une organisation permanente, la Direction générale du cyberespace, qui relève directement du chef du Développement de la force, le contre-amiral Lloyd, qui s'est adressé à vous le mois dernier. En tant que directeur général, je suis le supérieur du directeur du Développement de la force cybernétique. Cette direction a pour principale tâche de cerner et de développer les futures capacités cybernétiques. Cela comprend un travail conceptuel critique, ainsi que la conception et l'établissement de capacités cybernétiques. Elle englobe le groupe de travail sur la cybernétique des Forces canadiennes, et bénéficie du soutien permanent de ce que nous appelons les organisations de « niveau 1 » dans l'ensemble du MDN et des FC. Ces organisations de niveau 1 sont dirigées par des sous-ministres adjoints ou leurs homologues militaires.

Je passe maintenant au plan de travail de mon organisation. Il est divisé en quatre volets. Le premier a trait aux politiques. Tout comme notre équipe du sous-ministre adjoint aux politiques, nous faisons des suggestions à Sécurité publique Canada sur la mise en œuvre de la Stratégie du Canada en matière de sécurité cybernétique, et nous participons à l'élaboration de politiques concernant le rôle des forces armées dans l'environnement cybernétique. Le deuxième porte sur le commandement et le contrôle, et comprend la conception d'un régime d'autorité, de responsabilité et de reddition de comptes pour les capacités cybernétiques qui relèvent des commandants opérationnels. Comme pour la Stratégie nationale en matière de sécurité cybernétique, notre approche consiste à éviter de traiter tout ce qui concerne la « cybernétique » comme fondamentalement nouveau, et à tenter plutôt d'intégrer, dans la mesure du possible, nos activités cybernétiques dans les cadres de planification et d'opération existants.

Le troisième volet est le renforcement des capacités. Il consiste notamment à assurer que les ressources sont adéquatement axées sur les fonctions fondamentales, et à contribuer à la synchronisation des divers programmes des forces liés à la cybernétique. L'une des grandes priorités, pour renforcer notre capacité cybernétique dans les Forces canadiennes, est de fournir aux commandants une image commune de la situation opérationnelle et de leur permettre de mieux comprendre leur environnement cybernétique, favorisant ainsi une prise de

development of a program for building the specialized competencies required to operate effectively in the cyber environment, and putting in place measures to sustain the competencies by avoiding skill fade and ensuring appropriate retention levels.

[*Translation*]

As I noted earlier, the top priority of DND and the CF is to defend its own systems. Our needs are quite different from those of most other government departments, particularly in that commanders must remain accountable for command and control and sensor systems upon which our military operations entirely rely.

We work closely with Shared Services Canada and CSEC to help secure and defend some of our networks, but we must also maintain a capability of our own. Current DND/CF cyber capabilities related to computer network operations are focused primarily on defensive cyber operations and information technology security measures. The core defensive capabilities reside within the Canadian Forces Information Operations Group, housed in the Canadian Forces Network Operations Centre.

The mission of the unit is to conduct cyber defence operations and to conduct network operations.

[*English*]

A common thread through all of our work is the need to continue the shift from treating cyber as a series of discreet, and often technical, management activities towards a more coherent operational command-driven approach. This will require new processes and procedures, new training at all levels and a different way of thinking. I would be happy to elaborate, but we will leave it at that for now.

Recognizing that operating effectively in the cyber environment requires close coordination and cooperation with other government departments and with our closest allies, building and strengthening partnerships is another ongoing priority. In particular, DND and CF have enjoyed a long partnership with CSEC that will only become more important in the years to come.

We of course also place great value on our partnerships with the U.S, the U.K., Australia and New Zealand. The trust amongst this group is a great strength as we each grapple with similar challenges. NATO will be another key forum for cooperation.

décisions plus éclairée en temps opportun. Finalement viennent les ressources humaines et la formation. On définit les besoins en matière de formation, on élabore un programme permettant de rassembler les compétences spécialisées requises pour opérer de façon efficace dans l'environnement cybernétique et on met en œuvre des mesures pour conserver ces compétences, éviter l'érosion des compétences et assurer un niveau de rétention du savoir approprié.

[*Français*]

Comme je l'ai mentionné précédemment, la principale priorité du MDN et des forces canadiennes consiste à défendre ses propres systèmes. Nos besoins diffèrent passablement de ceux des autres ministères, surtout en raison du fait que nos commandants doivent assurer la responsabilité du commandement et du contrôle, ainsi que des systèmes capteurs dont dépendent entièrement nos opérations militaires.

Nous collaborons étroitement avec Services partagés Canada et le CSTC pour aider à sécuriser et à défendre certains de nos réseaux, mais nous devons également maintenir notre propre capacité. Les capacités cybernétiques actuelles du MDN et des forces canadiennes liées aux opérations des réseaux informatiques sont axées principalement sur les opérations cybernétiques défensives et les mesures de sécurité en matière de technologie de l'information. Les capacités défensives fondamentales relèvent du groupe des opérations d'information des forces canadiennes qui réside au sein du centre d'opération des réseaux des forces canadiennes.

Cette unité a pour mission de mener des opérations de défense cybernétique et de diriger l'exploitation des réseaux.

[*Traduction*]

Un thème commun dans l'ensemble de notre travail est la nécessité d'abandonner graduellement l'idée que la cybernétique est une série d'activités de gestion distinctes et souvent techniques afin d'adopter une approche opérationnelle axée sur le commandement plus cohérente. Pour y arriver, de nouveaux processus et procédures, une nouvelle formation à tous les niveaux et une manière de penser différente sont nécessaires. J'aimerais vous en dire plus, mais je m'arrête ici pour le moment.

Compte tenu du fait que l'efficacité opérationnelle dans l'environnement cybernétique exige une coordination et une collaboration étroites avec d'autres ministères ainsi qu'avec nos plus proches alliés, la création et le renforcement de partenariats sont d'autres activités permanentes hautement prioritaires. En particulier, le MDN et les FC ont bénéficié d'un long partenariat avec le Centre de la sécurité des télécommunications qui ne peut que prendre de l'importance dans les années à venir.

Bien sûr, nous apprécions grandement aussi nos partenariats avec les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande. La confiance réciproque des membres de ce groupe nous rend plus forts, étant donné que nous devons tous relever des défis semblables. L'OTAN sera également un forum important en matière de coopération.

[*Translation*]

In summary, DND/CF is taking the cyber threat seriously. It is real and present, so we have to be vigilant and effective in combating threats and reducing vulnerabilities in the cyber environment. More broadly, a modem military must be able to understand and operate effectively in the cyber environment. My organization is still in its early stages, but we have begun to make a difference and are actively working with key interdepartmental partners in the context of Government of Canada policy direction to deliver credible and comprehensive options for further development.

[*English*]

That concludes my overview of the CF cyber force development efforts and my organization's responsibilities. Brigadier-General Mazzolin and I would be happy to respond to your questions.

The Chair: As we begin, let us see how you frame it. In our discussions last week we talked about a recent speech from Leon Panetta, Secretary of Defense, talking about the responsibility of a cyber Pearl Harbour. He talks about cyberwarriors; the U.S. military is looking at new rules of engagement. Are you using the military terminology as you discuss this and look at it from your vantage point?

Brig.-Gen. Loos: We are trying to look at it through a normal military operational lens. We do look at it as another environment that has been institutionalized and normalized. We will have to undertake operations in the cyber environment. We look at it as a domain and it is something that we have to understand from an enabling perspective of providing capabilities to enable command and control, to enable operations in other domains but as well emerging as its own domain where you can undertake operations or others can undertake operations against us, to take away from our ability to command and control or connect up our sensors to decision makers, to military units that will have to deliver effects.

The Chair: Thank you very much. That is helpful.

[*Translation*]

Senator Dallaire: I want to be sure I understand correctly. We operate on land, sea and in the air. We have ventured into space a bit. Cyber space, by nature, makes us perceive this environment as new, somewhat as a fourth dimension of possibilities for conflict. Is that the basis of your analysis?

Brig.-Gen. Loos: That is exactly what we believe.

Senator Dallaire: The magnitude of this is significant, which leads me to the following point.

[*Français*]

En résumé, le plus MDN et les Forces canadiennes prennent au sérieux la menace cybernétique. Elle est réelle et présente. Nous devons donc être vigilants et efficaces pour contrer les menaces et réduire les vulnérabilités dans l'environnement cybernétique. Au sens plus large, des forces armées modernes doivent être en mesure de comprendre l'environnement cybernétique et opérer efficacement dans ce contexte. Mon organisation en est à ses débuts, mais nous avons commencé à faire une différence et travaillons activement avec des partenaires interministériels importants dans le cadre de la directive d'orientation du gouvernement du Canada visant à offrir des solutions crédibles et complètes pour poursuivre le développement.

[*Traduction*]

Ainsi s'achève le survol des efforts de développement de la force cybernétique des Forces canadiennes et des responsabilités de mon organisation. Le brigadier-général Mazzolin et moi-même serons heureux de répondre à vos questions.

La présidente : Pour commencer, voyons dans quelle perspective vous concevez les choses. La semaine dernière, nous avons discuté d'un discours récent de Leon Panetta, secrétaire à la Défense, dans lequel il parlait de la possibilité d'un Pearl Harbour cybernétique. Il a parlé de cyberguerriers. Ainsi, les forces militaires américaines envisagent de nouvelles règles d'engagement. En discutant de cette éventualité, utilisez-vous la terminologie militaire? L'étudiez-vous du point de vue des forces armées?

Bgén Loos : Nous essayons d'étudier la question d'un point de vue opérationnel normal dans les forces. Nous considérons ce domaine comme un nouvel environnement institutionnalisé et normalisé. Nous devrons mener des opérations dans un cyberenvironnement. Nous considérons cette question comme un domaine en soi, et c'est quelque chose que nous devons concevoir d'une perspective habilitante de manière à assurer le commandement et le contrôle, afin que des opérations puissent être menées dans d'autres domaines en même temps que dans celui-ci. Nous devons pouvoir mener des opérations dans ce domaine, ou d'autres pourraient en mener contre nous afin de supprimer notre capacité de commandement et de contrôle ou de nous empêcher de connecter nos capteurs avec les décideurs et les unités militaires qui devront passer à l'action.

La présidente : Merci beaucoup. Ça nous éclaire.

[*Français*]

Le sénateur Dallaire : J'aimerais être sûr de bien comprendre. Nous opérons sur terre, en mer et dans les airs. On s'est lancé un peu dans l'espace. La nature de l'espace cybernétique fait en sorte que l'on perçoit cet environnement comme nouveau, en quelque sorte une quatrième dimension de possibilités de conflits. Est-ce la nature de votre analyse?

Bgén Loos : C'est exactement ce que nous croyons.

Le sénateur Dallaire : L'ampleur est significative. Ce qui m'amène au point suivant.

[*English*]

Your shop, working for the vice, versus let us say General Beare's outfit, means you are working at the strategic level for establishing the doctrines that will be required, the structures that will be needed, the rules of engagement, as the chair has mentioned, beyond our borders, because there are no more borders with your environment. Your offensive operations and active defence, all that stuff, are you saying nothing has been put together yet in sort of an environmental construct like we see within the army with its doctrine and training and so on, that you are actually trying to create that from scratch with this new directorate?

Brig.-Gen. Loos: That is a very interesting question, and I will try to step through it and answer it in a way that is helpful.

From first principles, we already have a structure in place that allows us to carry out a number of the functions that we are talking about. Some of what we are doing is a little bit of old wine into new bottles. The cyber environment has been around for a long time. We have had to defend our networks for a long time. What we are looking at now is a first principles analysis of what we have and what we need, and then we will let form follow function to decide what we need to do to build beyond that.

I work for the vice, but I work for the Chief of Force Development, who is responsible for all joint capabilities. This is, if anything, a joint capability that will touch all the other environments. It is explicitly a process of going from conceive and design to then build, but we will build on what we already have. In relative and comparative terms, we have a strong starting point in terms of what we have on the shelf today, what we have in terms of capabilities. What is emerging is how that environment is being leveraged by our allies and adversaries. We have to look at it first conceptually to see what is in the range of possibility, what will be confronting us, and then look at the capabilities we need to deal with that, to make sure we can operate, to make sure we can defend and protect, to make sure we have freedom of manoeuvre, but ultimately, depending on what that analysis yields, it may speak to new structures.

One of the areas we are working on in my force development organization is command and control: How does that have to be shaped? We are already building on the structures we have. We are putting pieces in place at the start to inform our effort. We have folks working inside the new joint operational command to make sure we can synchronize what we are trying to do in the cyber environment and make it just another range of capabilities that has to be organized, planned, synchronized and laid out for joint commanders.

Senator Dallaire: You are scaling significantly, and we are talking a new environment, and we are not talking about ADMIM, making sure we have firewalls and tempest rooms

[*Traduction*]

Comme votre bureau travaille pour le vice-chef, plutôt que, disons, pour le général Beare, cela signifie que vous travaillez sur le plan stratégique pour l'établissement des doctrines, des structures et des règles d'engagement, comme l'a dit le président, qui seront nécessaires au-delà de nos frontières, parce qu'il n'y a plus de frontières dans cet environnement. Pour vos opérations offensives, la défense active, tout cela, êtes-vous en train de nous dire qu'aucun cadre n'a été établi, comme on en voit normalement dans une armée, qui a sa doctrine, son instruction, ainsi de suite? Êtes-vous en fait en train de créer tout cela à partir de rien au sein de cette nouvelle direction?

Bgén Loos : C'est une question très intéressante. J'essaierai d'y répondre de façon utile.

Comme principes de base, nous avons déjà une structure en place qui nous permet de réaliser certaines des fonctions dont nous parlons maintenant. Pour certaines choses, nous appliquons de vieux principes dans un nouveau cadre. Le cyberenvironnement existe depuis longtemps. Nous devons défendre nos réseaux depuis longtemps. Nous avons maintenant besoin d'une première analyse de ce que nous avons et de ce dont nous avons besoin. Ensuite, nous déciderons ce que nous voulons faire une fois que les fonctions voulues auront été établies.

Je travaille pour le vice-chef, mais aussi pour le chef du Développement de la force, qui est responsable de l'ensemble des capacités interarmées. Or, c'est bien là un motif de capacité interarmées qui touchera tous les autres environnements. Il s'agit d'un processus où l'on doit explicitement concevoir d'abord, puis mettre au point et bâtir, mais nous allons bâtir à partir de ce que nous avons déjà. Relativement et comparativement, nous avons une bonne base de départ, si l'on pense à ce que nous avons déjà sur le plan des capacités. Ce qui est nouveau, c'est ce que font nos alliés et nos adversaires pour augmenter leurs capacités. Nous devons d'abord faire des études conceptuelles pour voir quelles sont les possibilités, à quoi nous devrons faire face, puis nous demander de quelles capacités nous aurons besoin pour être sûrs d'être opérationnels, capables de nous défendre et de nous protéger — pour être sûrs que nous avons toute liberté d'agir. Au bout du compte, selon ce qui ressortira de cette analyse, nous pourrions avoir besoin de nouvelles structures.

Au sein de mon organisme de développement de la force, nous travaillons notamment sur le commandement et le contrôle. Quelle structure faut-il adopter à ces fins? Nous développons les structures que nous avons déjà. Nous rassemblons des pièces pour commencer, et nous apprenons au fur et à mesure. Il y a des gens au sein du nouveau commandement opérationnel interarmées qui sont chargés de s'assurer que nous pouvons synchroniser ce que nous essayons de faire dans le cyberenvironnement et de traiter cela comme tout autre éventail de capacités devant être organisé, planifié, synchronisé et présenté aux commandants interarmées.

Le sénateur Dallaire : Vous entreprenez quelque chose de grand, et nous parlons d'un nouvel environnement. Il ne s'agit pas de gestion de l'information, par exemple de s'assurer que nous

and that kind of stuff. We are not just talking garrison here; we are talking garrison but also in the field, and both of them are continuously interwoven because they are linked in. Does ADMIM become a three-star position and we take a different perspective to cyber versus what has often dominated, which is the environments do the operational stuff and you do most of the garrison stuff?

Brig.-Gen. Loos: At this point, it is too early to come up with final. You have touched on one of the key issues. When we get to the end of analysis and look at what we have versus what we think we need, there is a question about presenting that operational value case to the senior leadership in a department and beyond. We can afford something but we cannot afford everything in terms of what we can build. We will be on a different scope and scale than some of our allies — that much is clear at the outset — but we do have a view to significantly enhancing our capability to operate.

There are a number of options for how that structure will pan out. Regardless of what the structure is, we have it clearly in our sights to ensure that the command and control relationships will allow commanders and staffs to properly integrate this into their set of tools as necessary to make sure they have a proper appreciation for what is going on in the cyber environment because it will affect all of their operational environments, but as well, to make sure we have the right governance and oversight.

We intend to treat this like other operations — rules of engagement, strategic targeting oversight when and where appropriate to make it normalized and institutionalized in a way that makes it not something new and different but just part of the mix.

The Chair: Thank you. That was a very good answer.

Senator Johnson: You state in your opening remarks that Public Safety is the lead department under which cyber security falls. You have also said there is a role for National Defence in protecting Canadians against cyber attacks. Can you expand on and explain what role National Defence and the Canadian Forces play currently and what role they will play in the future as the cyber threat develops further?

Brig.-Gen. Loos: The Cyber Security Strategy is fairly clear about DND's role. We have a responsibility to protect our own information and networks; that is clearly within our remit. We have a role to contribute to the whole-of-government effort in characterizing the threat and sharing information on what is going on in the cyber environment. Beyond that, it is the normal

avons les pare-feu et les installations TEMPEST nécessaires ou ce genre de choses. Nous ne parlons pas seulement de garnison. Il s'agit bien de garnison, mais aussi de travail en campagne, et les deux sont toujours interreliés. Le sous-ministre adjoint responsable de la gestion de l'information acquiert-il l'équivalent d'un poste trois étoiles — ce qui permet d'envisager la cybernétique d'un point de vue différent par rapport à ce qui a souvent été la norme, soit que les différents environnements s'occupent des questions opérationnelles et vous vous occupez de la majorité des questions de garnison?

Bgén Loos : Il est encore trop tôt pour arriver à des décisions finales. Vous avez abordé l'un des principaux enjeux. Quand nous aurons terminé l'analyse, nous pourrons comparer ce que nous avons actuellement à ce qui nous semble nécessaire. Dans ce genre de cas, il faut présenter une justification de la valeur opérationnelle aux cadres supérieurs d'un ministère et à d'autres intervenants. Nous aurons les moyens de bâtir certaines choses, mais nos moyens ne sont pas illimités. Nos activités n'auront pas la même ampleur ni la même portée que celles de certains de nos alliés — nous le savons dès le départ — mais nous avons l'intention d'améliorer considérablement notre capacité opérationnelle.

La structure pourrait prendre diverses formes. Quelle que soit l'option choisie, nous sommes déjà résolus à faire en sorte que les relations de commandement et de contrôle permettent aux commandants et aux membres du personnel d'intégrer adéquatement cet élément à leurs outils selon les besoins. Nous voulons nous assurer qu'ils comprennent bien ce qui se passe dans l'environnement cybernétique, puisqu'il a des répercussions sur tous leurs environnements opérationnels. Nous devons aussi nous assurer d'avoir la gouvernance et la surveillance appropriées.

Nous avons l'intention de traiter cette question de la même manière que les autres opérations, ce qui suppose des règles d'engagement et une surveillance des cibles stratégiques, au moment et à l'endroit appropriés. Nous voulons normaliser et institutionnaliser cet élément afin qu'il soit considéré non plus comme une exigence nouvelle et différente, mais simplement comme un élément de l'ensemble.

La présidente : Merci pour cette excellente réponse.

Le sénateur Johnson : Vous avez mentionné, au début de votre intervention, que Sécurité publique est le chef de file du gouvernement du Canada en matière de cybersécurité. Vous avez aussi dit que la Défense nationale avait un rôle à jouer quand il s'agit de protéger les Canadiens contre les cyberattaques. Pourriez-vous nous en dire davantage sur le rôle que la Défense nationale et les Forces canadiennes jouent actuellement à cet égard et sur le rôle qu'elles joueront à l'avenir, alors que les cybermenaces iront en s'amplifiant?

Bgén Loos : La Stratégie de cybersécurité décrit assez clairement le rôle du MDN. Nous avons la responsabilité de protéger les renseignements et les réseaux qui nous appartiennent; cela fait clairement partie de notre mandat. Nous devons aussi contribuer aux efforts pangouvernementaux qui visent à définir les menaces et à partager des renseignements sur ce qui se produit

extension of the department's remit to provide assistance to other government departments when the security situation reaches a point where the scope, scale and consequences take it from being an isolated incident to something of greater importance, or it becomes a security event at a national level.

That is pretty much the current limitation on how we are directing our efforts. I think there is more to be looked at as we go forward. We will not lead in that space; that is not our role. However, I do believe we will have a seat at the whole-of-government table. When the threats are coming in, we see events at network speed, and it is necessarily difficult in the early stages to figure out what is going on. If that is the case, then we have to be at the whole-of-government table early to be informed and to have visibility to what is going on.

Normally, events affecting the Government of Canada will be handled by Public Safety and the Communications Security Establishment Canada, CSEC, but when it trips beyond an isolated event and looks like it is something that is either state-sponsored or something with wider repercussions, then clearly National Defence would be brought in if not to assist then at least to be at the table to provide advice to government.

Senator Johnson: This is such a new area for most Canadians. I am a replacement on this committee and this is my third week here, unlike some of my colleagues. I am asking from the ordinary-Canadian point of view of public safety.

You mentioned a bit about NATO. What about our allies and working with CF to combat this growing threat? Do you think NATO will play a more prominent role in cyber security?

Brig.-Gen. Loos: NATO has much on the go in terms of their conceptual and policy work and in terms of smart defence. They will be part of our way ahead.

The problem space, in my estimation, is much larger than any one nation or any one government department. Therefore, we look at it as a team sport in that the only way to get a leg up on those who would cause us harm or take malicious actions is to share information in every venue and every forum we can. When we do that, we will be better off. NATO and our key allies in the Fives Eyes offer us those opportunities. We attempt to move at the speed of trust. The more we can share and safeguard the information we share the better off we will be.

The Chair: I guess one of the distinctions we are trying to get at here is that you are a department unlike others in some respects. A breach or a hack at DND has larger implications than at some other departments, so you have to focus on that primarily; is that fair to say?

dans l'environnement cybernétique. Notre ministère a déjà la responsabilité d'aider les autres ministères quand l'ampleur, la portée ou les conséquences d'un problème de sécurité sont telles qu'il s'agit non plus d'un incident isolé, mais d'un problème plus important ou qui touche la sécurité à l'échelle nationale.

Ces diverses balises guident nos efforts actuels. Je crois que nous examinerons d'autres éléments à mesure que nous progresserons. Nous ne serons pas les chefs de file dans ce dossier, car ce n'est pas notre rôle. Je crois toutefois que nous aurons une place à la table pangouvernementale. Quand les menaces se concrétisent, la situation évolue à la vitesse des réseaux et, au début, il est toujours difficile de comprendre ce qui est en train de se produire. Dans des situations comme celle-là, nous devons participer à la table pangouvernementale dès le début pour être bien informés et savoir ce qui se passe.

En temps normal, les événements qui touchent le gouvernement du Canada seront traités par la Sécurité publique et par le Centre de la sécurité des télécommunications Canada, le CSTC. Mais s'il ne s'agit plus d'un incident isolé et qu'on semble avoir affaire à une attaque qui est parrainée par un État ou qui aura de vastes répercussions, la Défense nationale sera évidemment appelée à participer. Si elle ne participe pas à la résolution du problème, elle sera à tout le moins à la table de discussion pour pouvoir conseiller le gouvernement.

Le sénateur Johnson : Ce domaine est tout à fait nouveau pour la plupart des Canadiens. Je fais office de remplaçant à ce comité, contrairement à certains de mes collègues, et c'est ma troisième semaine. J'ai donc le point de vue d'un Canadien ordinaire en ce qui concerne la sécurité publique.

Vous avez mentionné brièvement l'OTAN. Nos alliés collaboreront-ils avec les Forces canadiennes pour combattre cette menace grandissante? Croyez-vous que l'OTAN jouera un rôle plus important en matière de cybersécurité?

Bgén Loos : L'OTAN a déjà entrepris des travaux importants sur les concepts, les politiques et la défense intelligente. Cet organisme jouera un rôle dans nos travaux.

À mon avis, ce problème dépasse largement les frontières d'un pays ou d'un ministère. Nous devons traiter cette question comme un sport d'équipe. Autrement dit, la seule façon de contrecarrer ceux qui voudraient nous nuire ou poser des gestes malveillants, c'est de partager des renseignements de toutes les manières et dans tous les forums possibles. C'est la stratégie la plus productive, et nous pouvons l'utiliser parce que nous avons accès à l'OTAN et à nos alliés des « Five Eyes ». Nous tentons d'avancer aussi vite que la confiance nous le permet. Plus nous pourrons partager de renseignements et protéger ce que nous partageons, meilleure sera notre situation.

La présidente : Je crois que l'une des distinctions que nous tentons d'établir aujourd'hui, c'est que votre ministère est, à certains égards, différent de tous les autres. Des failles ou des accès non autorisés aux systèmes du MDN auraient des conséquences plus graves que dans d'autres ministères. Vous devez donc vous concentrer d'abord sur cet aspect. C'est bien exact?

Brig.-Gen. Loos: That is absolutely so. In fact, Brigadier-General Mazzolin has most of our current forces under his control today. His folks are waging the daily battle.

The Chair: Will you speak to that for a moment Brigadier-General Mazzolin?

Brigadier-General Roberto Mazzolin, Director General, Information Management Operations, National Defence: Fundamentally, it becomes an issue. This is what we consider cyber or the network environment — the Internet as most Canadians would recognize it. The technology embeds itself into the very fabric of everything that Canadians do. By extension, that applies to militaries.

The challenge that we face is one we share with our partners in defence around the world. The doctrine, tactics, techniques and procedures that normally apply to any global commons such as the air, land and maritime environments have been established for millennia and the organizational constructs and the doctrine for that period is long-standing. Air power has been in place for 100 years. Cyber is intrinsically new from that perspective.

Conceptually framing this is the challenge that many militaries are dealing with. When we look at the role of defence in this context as the means of asserting national will or national political intent as part of a broader strategic security construct, the challenge is how we fit into this environment. Cyber permeates every facet of everything we do. Where do we fit into these broader areas? These are some of the challenges we seek to embrace.

Senator Lang: I just want to go back and refer to Secretary of Defense Panetta's statement two months ago on September 11. As you well know, he had a significant statement to make on cyber security. I want to quote this, because I want to follow on to what Senator Johnson said in terms of most Canadians not being aware of how serious the situation we face is. I want to ask you to elaborate further on the significance of Mr. Panetta's statement and what we actually do face and the reason why we are doing what we have to do.

For the record, in talking about breach of cyber security, he said:

> The collective result of these kinds of attacks could be a cyber Pearl Harbor, an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability.

Statements like this made by the Secretary of Defense for the United States have to be taken seriously. Can you comment on that? I think it is important that Canadians understand the significance of what this is.

Bgén Loos : Oui, c'est absolument vrai. En fait, le brigadier-général Mazzolin contrôle la plupart de nos forces actuelles. Ce sont ses employés qui livrent ce combat quotidien.

La présidente : Brigadier-général Mazzolin, pourriez-vous nous en parler un peu?

Brigadier-général Roberto Mazzolin, directeur général, Opérations de gestion de l'information, Défense nationale : Cela devient un enjeu, fondamentalement. C'est ce que nous appelons l'environnement cybernétique ou l'environnement réseau, et que la plupart des Canadiens appellent Internet. Cette technologie fait partie intégrante de tout ce que font les Canadiens. Cela s'applique donc aussi aux organisations militaires, par le fait même.

Nous sommes aux prises avec le même défi que nos partenaires de la défense du monde entier. La doctrine, les tactiques, les techniques et les procédures qui s'appliquent normalement aux patrimoines communs —notamment les environnements aérien, terrestre et maritime — se sont formées au fil des millénaires. Les construits organisationnels et la doctrine sont établis depuis longtemps. La puissance aérienne est en place depuis 100 ans. En comparaison, l'univers cybernétique est encore nouveau.

Le défi de nombreuses forces militaires consiste à définir le cadre conceptuel. Si on considère que, dans ce contexte, la défense a pour rôle de faire respecter la volonté nationale ou les intentions politiques de la nation dans le cadre d'un objectif de sécurité stratégique plus vaste, le défi consiste à définir notre place dans cet environnement. L'informatique est omniprésente dans toutes les facettes de tout ce que les gens font. Quelle est notre place dans ces domaines très vastes? Voilà certains des défis sur lesquels nous devons nous pencher.

Le sénateur Lang : J'aimerais revenir sur ce qu'a déclaré le secrétaire américain à la Défense Panetta il y a deux mois, le 11 septembre. Comme vous le savez, il a fait une déclaration importante sur la cybersécurité. J'aimerais en citer un extrait, pour faire suite à l'observation du sénateur Johnson, qui a souligné que la plupart des Canadiens ne sont pas conscients de la gravité de la situation. J'aimerais que vous nous parliez davantage de l'importance de la déclaration de M. Panetta, des menaces auxquelles nous sommes confrontés et des raisons qui nous amènent à poser les gestes que nous devons poser.

À titre d'information, voici ce qu'il a dit au sujet des atteintes à la cybersécurité :

> Le résultat collectif des attaques de ce genre pourrait se comparer à un Pearl Harbor informatique, donc à une attaque qui causerait des pertes matérielles et des décès. En fait, une attaque comme celle-là paralyserait la nation, causerait un choc et créerait un profond sentiment de vulnérabilité.

Quand le secrétaire à la Défense des États-Unis fait de telles déclarations, il faut les prendre au sérieux. Pourriez-vous nous dire ce que vous en pensez? Il m'apparaît important que les Canadiens comprennent l'ampleur du problème.

Brig.-Gen. Loos: Absolutely. I will share the mic with Brig.-Gen. Mazzolin on this one. I do not think I am in a position to either affirm or discount Secretary Panetta. I think there are many commentators out there who will offer up what are technically valid representations of what is possible. I am not in a position to comment on what is probable.

There is a bit more of a calculus that goes into determining those actors, and there is a range of threat actors out there from hacktivists, to criminal organizations, through to terrorist organizations that are perhaps enabled down to state-sponsored, where we see the most sophisticated capabilities. However, when you get to the most sophisticated capabilities, there is a cognizance that, if it is state-sponsored, there are other factors that go into the determination of whether they will use those capabilities in some of the ways described there.

I do not necessarily have an opinion. I think there are some possibilities there. I certainly would be loath to predict whether we see that rising up to us tomorrow.

However, back to the question, the point was about that scenario, this department and the Canadian Forces. Clearly, when it becomes a broader security issue, then we will be involved. We have to be aware of it, if only from the simple perspective that we have to assure the military mission. If the power is out, telecommunications are down or transportation is affected, that affects the military's ability to carry out its mission. To go back to my earlier point, that is why we have to be at the whole-of-government table and be aware of what is going on at the same time as other partners in government are carrying out their functions and roles.

I would suggest that if the repercussions of the event have either online or off-line implications, then we would be part of dealing with that. However, in terms of tying that back to my effort to build what is right for the Canadian Forces today, it is not a big driver. I do not think the apocalyptic predictions are what will fundamentally bound and describe what we will build, certainly within DND and the CF.

I do not know if Brigadier-General Mazzolin wanted to speak to the threat.

Brig.-Gen. Mazzolin: Thank you. Again, it is very difficult to predict the likelihood of any scenario in terms of characterizing the threat. There is a tendency to focus on foreign state actors and the high end of the threat continuum. That is represented and understood by many in the intelligence community, and it would be inappropriate to speak to that specifically here.

A significant effort is devoted to protecting our own defence infrastructure, command and control networks to allow us to operate.

Bgén Loos : Tout à fait. Je demanderai aussi au brigadier-général Mazzolin de répondre à cette question. Pour ma part, je ne pense pas être en mesure de confirmer ou d'infirmer ce qu'a dit le secrétaire Panetta. Je crois que de nombreux commentateurs proposeront différents scénarios techniquement valides et possibles. Je ne peux pas me prononcer sur les probabilités.

Il faut faire de savants calculs pour déterminer qui sont les auteurs de ces menaces. Il en existe une grande variété, qui vont des hacktivistes aux organisations criminelles, en passant par les organisations terroristes parfois soutenues ou parrainées par un État, qui ont les moyens les plus sophistiqués. Toutefois, quand un groupe parrainé par un État a des moyens très sophistiqués, il faut tenir compte d'autres facteurs pour déterminer s'il passera effectivement à l'action et posera des gestes comme ceux dont nous parlons aujourd'hui.

Je n'ai pas vraiment d'opinion à ce sujet. Je crois qu'il existe plusieurs possibilités. Je ne voudrais vraiment pas tenter de prédire si cette menace se dressera devant nous demain.

Pour revenir à la question, les éléments essentiels sont le scénario, le ministère et les Forces canadiennes. De toute évidence, si un incident devient un problème de sécurité plus vaste, nous aurons un rôle à jouer. Nous devrons en être informés, ne serait-ce que pour pouvoir assurer la poursuite de notre mission militaire. En effet, s'il y a une panne d'électricité ou une interruption des télécommunications ou des transports, cela peut avoir des répercussions sur notre capacité de nous acquitter de notre mission. Pour revenir à ce que je disais plus tôt, c'est pourquoi nous devons participer à la table pangouvernementale et être informés des événements au même moment que les autres partenaires du gouvernement, qui s'acquittent de leurs propres tâches et jouent leur rôle.

Je crois que si l'incident a des répercussions sur Internet ou dans le monde physique, nous participerons à la résolution. Toutefois, en ce qui concerne les efforts que j'ai entrepris en vue de bâtir les Forces canadiennes comme elles doivent être bâties, ce dossier n'est pas un moteur important. Je ne crois pas que nous nous appuyions sur des prédictions apocalyptiques pour définir ce que nous allons bâtir, du moins pas au MDN ni dans les Forces canadiennes.

Le brigadier-général Mazzolin aimerait peut-être ajouter quelque chose à propos de cette menace.

Bgén Mazzolin : Merci. Encore une fois, il est très difficile de prédire la probabilité d'un scénario ou d'un autre et de définir la menace. La tendance générale veut qu'on se concentre sur les acteurs des États étrangers, qui se classent au niveau le plus élevé sur l'échelle des menaces. C'est un fait bien connu parmi les intervenants du monde du renseignement, et il serait inapproprié de donner plus de détails ici.

Nous déployons des efforts considérables afin de protéger les réseaux qui servent à notre infrastructure, au commandement et au contrôle, afin d'assurer le maintien de nos activités.

Perhaps the more challenging question is that of the asymmetric threats we end up having to face. That is of particular interest to the Canadian Forces, where we are a general-purpose military. We have a long tradition of responding to a wide range of operational exigencies, from disaster relief, humanitarian operations, to high-intensity conflict. Part of that responsibility includes supporting our federal first responders and security agencies when called upon to do so.

The challenge with an asymmetric threat is that the threat has very little investment: The initiative is always with the attacker, and this requires a nation or military to devote significant effort to defending against a threat that can be initiated with nominal resources.

To that end, the big challenge for us is how we embrace cyber in the context of facilitating operations.

Senator Lang: To follow that through, the reason I raise this is that the way I see, in part, your responsibility is to do whatever we can to prevent that particular event taking place.

General Loos, in your statement you said this will require new processes, procedures, new training at all levels and a different way of thinking, not unlike the body of the statement made by the Secretary of Defense for the United States two months ago.

What time frame are we looking at here? We are changing the way we look at cyberspace threat. Some resources have been made available. What time frame are you looking at from the point of view of bringing in these new procedures, new training, different way of thinking and the question of whether you have the trained personnel to do that, which again was referred to in Secretary of Defense Panetta's public statement?

Brig.-Gen. Loos: In terms of time frame, you are absolutely right that time is pressing on us. I would characterize it as a ramped-up effort to move up on those lines of operations I mentioned, looking at capabilities, looking at command and control, looking at the policy and governance issues that need to be normalized so we can carry on and look at the HR.

Realistically, the HR piece of it is likely to be the most challenging. How do we, in the short term, use our existing system of trades and classifications in our HR system to deliver some of the right answers in the short term while we go through a very methodical force development process to analyze what we need and then put in place the program and the pieces that we need to get there? This will likely involve structural change, some new approaches to HR and doctrinal changes in how we bring this in, not just for a specialist cadre but across the rank and file of everyone in the Canadian Forces.

Le plus grand défi qui se pose est peut-être celui des menaces asymétriques auxquelles nous sommes confrontés. C'est particulièrement important pour les Forces canadiennes, puisque nous sommes une force militaire généraliste. Comme le veut notre longue tradition, nous intervenons dans une grande variété de contextes opérationnels, qu'il s'agisse de secours en cas de catastrophe, d'opérations humanitaires ou de guerres intensives. Nous avons aussi pour responsabilité de soutenir les premiers intervenants fédéraux et les organismes de sécurité quand on nous le demande.

Les menaces asymétriques comportent un investissement minime, c'est d'ailleurs ce qui pose problème. Comme l'attaquant prend toujours l'initiative, le pays ou les forces armées en cause doivent déployer des efforts considérables pour se défendre contre une menace qui, quant à elle, nécessite très peu de ressources.

Notre principal défi à cet égard consiste donc à déterminer comment intégrer la cybernétique dans un contexte où nous voulons faciliter les opérations.

Le sénateur Lang : Si je soulève la question, c'est qu'il vous incombe, du moins en partie selon moi, de faire le nécessaire pour prévenir ce genre de choses.

Général Loos, vous avez dit dans votre discours qu'il faudra de nouveaux processus et de nouvelles procédures, une nouvelle formation à l'intention de tous les niveaux et une manière de penser différente, ce qui n'est pas sans rappeler la déclaration prononcée il y a deux mois par le secrétaire américain à la Défense.

À quoi ressemble au juste votre échéancier? Nous changeons la façon dont nous percevons les menaces cybernétiques. Des ressources ont été débloquées. Quel est votre échéancier pour mettre en œuvre ces nouvelles procédures, offrir la nouvelle formation et changer la façon de penser? Avez-vous le personnel qualifié nécessaire? Il s'agit là aussi d'un point soulevé par M. Panetta, le secrétaire à la Défense, dans sa déclaration publique.

Bgén Loos : Vous avez raison pour ce qui est de l'échéancier, nous sommes pressés par le temps. J'ai parlé des différents volets dans mon organisation et je dirais qu'il faut d'abord se pencher sur les capacités, sur le commandement et le contrôle, ainsi que sur les politiques et les questions de gouvernance qui doivent être normalisées, avant de pouvoir s'attaquer aux ressources humaines.

Le volet ressources humaines sera fort probablement le plus exigeant. Comment utiliserons-nous notre système de classification des métiers pour trouver, à court terme, les solutions nécessaires? Nous traversons, je le rappelle, un processus très méthodique de développement de la force dans le but d'analyser nos besoins et, par la suite, de mettre en place un programme et des éléments pour y répondre. Il y aura sans aucun doute des changements structurels, de nouvelles approches en matière de ressources humaines et des changements de doctrine pour appliquer les nouvelles mesures. Tant les spécialistes que les membres ordinaires des Forces canadiennes sont concernés.

Everyone who sits at a keyboard is part of that environment and represents both an actor for good but also vulnerability when we do not attend to information assurance and protection of information.

As for realistic time frames, we are looking at a number of years, initially, to better organize and apply the resources that we have and introduce some of the initial cadres for some new capabilities. We are looking at a number of years beyond that before the full program will start to deliver.

A bit further down the road is an architectural piece as well. We have what we have today in terms of our network space and infrastructure, but it is not necessarily completely designed and architected with network protection and defence in mind. In some cases, that gets added on as we go along. In an enabling vein, trying to make our operations better and more swept up, we get involved with connecting things up to help commanders and staff understand their environment and prosecute operations.

Knowing what we know now and designing for our infrastructure of the future, we will make it stronger at the outset in our design, but also instrument it so we can make it more defendable in the future in terms of specific capabilities for the defence.

There is a lot that goes into the program. You are entirely right that there are a number of challenging areas that we have to move out on.

Senator Day: There are many things spinning around in my head here in terms of the discussion we have had. Thank you for being here to help us gather a little bit of understanding. In my reading, I am looking at the various relationships that exist.

First, can you clarify for me, are Shared Services Canada in DND, or are all the people in information technology in DND separate from Shared Services Canada?

Brig.-Gen. Loos: I will share the microphone with General Mazzolin on this, because he is in the organization that has Shared Services Canada as part of its integrated approach.

Part of the statement that I did not go into detail on is that we do not look at the cyber environment as just our network space from a military perspective. It necessarily involves, beyond network space, anything that goes over radio frequency, anything that connects up between our sensors and sensor systems, back to decision makers and then out to units or platforms that have to take action. All of that we consider to be part of our cyber domain or cyber environment. That is definitely beyond the remit of Shared Services Canada.

Tous ceux qui se trouvent devant un écran d'ordinateur font partie de cet environnement. Ils peuvent prendre les mesures qui s'imposent, mais ils peuvent aussi être vulnérables si nous ne nous occupons pas de l'assurance de l'information et de la protection des renseignements.

De façon réaliste, il nous faudra, dans un premier temps, quelques années pour mieux organiser et utiliser les ressources dont nous disposons et mettre en place les premiers cadres qui régiront certaines des nouvelles capacités. Par la suite, il faudra compter encore un certain nombre d'années avant que le programme dans son intégralité commence à porter ses fruits.

Un peu plus tard, il y aura la question de l'architecture. L'espace réseau et l'infrastructure dont nous disposons actuellement n'ont pas nécessairement été conçus en tenant compte des considérations de protection et de défense. Ces éléments sont ajoutés avec le temps, dans certains cas. Il nous arrive, dans le but d'améliorer nos opérations et de les rendre plus conformes, de procéder à des installations qui aident les commandants et le personnel à comprendre leur environnement et à faire leur travail.

Étant donné ce que nous savons maintenant, à l'avenir, nous concevrons dès le départ une infrastructure plus solide et nous veillerons à intégrer les outils nécessaires pour qu'il soit plus facile d'en assurer la protection.

Nous déployons beaucoup d'efforts dans ce programme. Nous avons de nombreux défis à relever, vous avez entièrement raison ce sur point.

Le sénateur Day : J'ai la tête pleine étant donné tout ce qui vient d'être dit. Je vous remercie d'être venu nous éclairer un tant soit peu. Dans le document que je parcours, j'examine les différentes relations qui existent.

Premièrement, pouvez-vous me dire si le MDN est desservi par Services partagés Canada ou si, au MDN, les gens qui travaillent dans le domaine de la technologie de l'information ne font pas partie de Services partagés Canada?

Bgén Loos : Le général Mazzolin pourra prendre la parole après moi, parce que Services partagés Canada fait partie de l'approche intégrée de l'organisation.

Dans mon exposé, je n'ai pas insisté sur le fait que, pour nous, le cyberenvironnement ne se limite pas strictement à notre espace réseau du point de vue militaire. En effet, au-delà de l'espace réseau, il englobe nécessairement tout ce qui est transmis sur une radiofréquence, tout ce qui est reçu sur nos capteurs et nos systèmes-capteurs, remis aux décideurs et envoyé aux unités ou aux groupes qui doivent passer à l'action. Tout cela fait partie du cyberdomaine ou cyberenvironnement et va très certainement au-delà des compétences de Services partagés Canada.

We also look at our command and control systems at "secret" and higher as weapons systems, as a means we need for effecting command and control and for carrying out operations. That is necessarily something that we have to ensure and have controls over. That is currently a dividing line in the effort.

The other thing I would say is that Shared Services Canada has a remit to deliver us a certain range of services and capability for commodity IT, email and data centres, but it is still our job to integrate that into a whole, fused picture. We use those systems as well to support operations, to support the function of command. It is still important to us what is going on with the services that are delivered by Shared Services Canada, or if there are other defensive services provided by Communications Security Establishment Canada. We need to fuse that together and present a coherent picture so that commanders understand what is up, what is down, where we are being attacked today, if we are, what we can do to mitigate that and how we can work around that.

I know it is a swept-up effort within the information management group to deal with the transition of Shared Services Canada being stood up and taking over responsibility for some of those services..

Brig.-Gen. Mazzolin: Brigadier-General Loos has covered it very well. What I would offer is that the Shared Services Canada initiative, to which we have devoted a significant amount of effort in terms of partitioning out the respective resources that are transferred over to us to ensure those we retain within the National Defence, actually presents an opportunity for us.

The commodity-based information management and information technology, which SSC is responsible to manage, still captures a significant portion of what we consider to be command and control infrastructure networks. Virtually everything we do within National Defence impacts on our ability to conduct operations.

I guess the partition line that we have tried to respect is one that we retain within the department, and it allows us to focus on those networks in the classified environment that are integral to supporting our deployed communications, command, control, computing, intelligence, surveillance and reconnaissance operations. To that end, we have undertaken a significant effort to try to understand the delineation point. We recognize that even in the corporate environment, which facilitates military operations, the application environment, which is specific to DND, the data and the information that resides in the networks that are provided by SSC and that we use are what we are trying to focus on and ensuring and developing our specific network environment to be able to protect the information and facilitate operations in cyberspace.

Senator Day: You have a larger role than just DND in terms of protecting information and cyberspace, and that is for Canada. Canada's defence requires you to play that broader role; does it not?

En outre, nous considérons que nos systèmes de commande et de contrôle de niveau secret ou supérieur à secret sont en fait des systèmes d'armes. Nous estimons qu'il s'agit d'outils dont nous avons besoin pour assurer le commandement et le contrôle, et pour effectuer nos opérations. Nous devons nécessairement contrôler ces systèmes. Il y a là une ligne de démarcation.

J'ajouterai qu'il incombe à Services partagés Canada de nous desservir pour ce qui est des produits de technologie de l'information, du courrier électronique et des centres de données, mais nous sommes responsables d'assurer l'intégration de tous ces éléments. Ces systèmes viennent appuyer les opérations et la fonction de commandement. Tout ce qui touche les services fournis par Services partagés Canada, ainsi que les services de défense du Centre de la sécurité des télécommunications Canada, est important pour nous. Nous devons intégrer ces différents éléments de manière à présenter aux commandants un portrait global de ce qui se passe afin qu'ils puissent déterminer d'où viennent les attaques, le cas échéant, les mesures d'atténuation et les correctifs à apporter.

Je sais qu'au sein du groupe de gestion de l'information, la transition en cours constitue un travail magistral, notamment en ce qui concerne les nouvelles responsabilités dans le cadre de l'initiative Services partagés Canada.

Bgén Mazzolin : Le brigadier-général Loos a bien répondu à la question. J'ajouterais que l'initiative Services partagés Canada — à laquelle nous avons consacré des efforts considérables pour ce qui est de diviser les ressources qui nous sont transférées de manière à protéger celles que nous avons au ministère de la Défense nationale — représente une occasion pour nous.

Les produits de technologie de l'information que Services partagés Canada est responsable de gérer englobent une part importante de ce que nous considérons comme des réseaux d'infrastructure de commandement et de contrôle. Pratiquement tout ce que nous faisons à la Défense nationale se répercute sur notre capacité de mener des opérations.

Nous tentons de respecter cette ligne de démarcation au ministère, ce qui nous permet de nous mettre l'accent sur les réseaux, dans un contexte classifié, qui sont essentiels pour soutenir, en déploiement, les communications, le commandement, le contrôle, les services informatiques, le renseignement, la surveillance et les opérations de reconnaissance. Nous nous sommes efforcés de comprendre où était la démarcation. Même dans l'environnement informatique ministériel — l'environnement d'applications qui appuie les opérations militaires, qui est propre à la Défense nationale —, nous essayons de nous concentrer sur les données et les renseignements des réseaux fournis par Services partagés Canada et de bâtir notre propre infrastructure de réseaux pour pouvoir protéger les renseignements et faciliter les opérations dans le cyberespace.

Le sénateur Day : Votre rôle de protection de l'information et du cyberespace dépasse le cadre du ministère de la Défense nationale et s'étend au Canada. La défense du Canada exige que vous assumiez ces fonctions élargies, n'est-ce pas?

Brig.-Gen. Loos: I would say that at this point, no, sir, that has not been laid out for us as a broader role. Certainly, we see ourselves as part of the whole-of-government team to respond to security instances that reach a scope and scale, but in terms of protecting government systems, that is CSEC's role. In terms of reaching out and down to provinces, territories and critical industries, that is Public Safety's role to lead and coordinate.

We are certainly interested in all of that. There is military nexus there, as I have said, in terms of mission assurance and understanding what is going on for if and when it becomes a national security issue for which the military should have a voice in providing advice and contributing to the fight.

Senator Day: I would like to get a feeling for the role of the electronic warfare group, your relationship with them and your relationship with the communications and electronics establishment in Kingston within the military. You have discussed Australia, New Zealand, the U.K. and the U.S. and how you cooperate with them. What about the countries from NATO that have gone into the Estonian research establishment for cyber and the lessons we have learned from that Estonian cyber attack? Can you talk about that? I want to get a feeling for your role within those various parameters.

Brig.-Gen. Loos: I will let you take the electronic warfare part.

Brig.-Gen. Mazzolin: There are a number of questions there in terms of trying to characterize the extent capability. The principle operational entity within the CF at this point is the Canadian Forces Information Operations Group, part of which involves the Canadian Forces Electronic Warfare Centre, which provides support from an electronic warfare perspective in terms of supporting our tactical platforms. The CFIOG looks after our military-specific signals intelligence, network defence operations and electronic warfare capabilities, which basically comprise what we look at operating in the cyber environment and in the terms I think you are referring to.

We work in close collaboration with our international partners, again, in terms of a lot of the doctrine, the tactics, techniques and procedures and also in terms of interoperability with our partners. When the Canadian Forces deploy internationally as part of coalition operations, our deployed platforms have to work in close proximity and in conjunction with our allies. To that end, it is very important that our systems are interoperable.

You mentioned the school in Kingston. I believe you are referring to the School of Communications and Electronics. Again, fundamental in terms of being able to develop a military capability, education, training, professional development and doctrine are absolutely integral to that. A significant amount of effort is being devoted towards developing the school's capacity to be able to do that, to provide that capability.

Bgén Loos : Je vous dirais que non, monsieur, à l'heure actuelle, il n'est pas prévu que nous jouions un plus grand rôle. Évidemment, nous considérons que nous faisons partie intégrante de l'équipe pangouvernementale qui s'occupe des cas de sécurité d'une certaine ampleur et envergure, mais c'est au Centre de la sécurité des télécommunications Canada qu'il revient de protéger les systèmes gouvernementaux. Pour ce qui est de la coordination avec les provinces, les territoires et les industries essentielles, c'est le ministère de la Sécurité publique qui est responsable.

De toute évidence, nous nous intéressons à ce qui se passe. Comme je l'ai dit, il y a tout de même un lien avec l'armée, sur le plan de l'assurance des missions, et nous devons comprendre les enjeux au cas où un problème de sécurité nationale exigerait que l'armée offre des conseils et contribue aux efforts de lutte.

Le sénateur Day : J'aimerais avoir une idée des attributions du groupe de la guerre électronique, de vos liens avec lui et de vos liens avec l'établissement de l'électronique et des communications de Kingston dans le contexte de l'armée. Vous avez parlé de l'Australie, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis et de votre collaboration avec ces pays. Qu'en est-il des pays membres de l'OTAN qui ont vu à la création d'un centre de recherche sur la cyberdéfense, situé en Estonie? Quelles leçons avons-nous tirées de la cyberattaque contre l'Estonie? Pourriez-vous nous en parler? J'aimerais comprendre votre rôle à l'intérieur de ces divers paramètres.

Bgén Loos : Je vais vous laisser parler de la guerre électronique.

Bgén Mazzolin : Vous avez posé beaucoup de questions sur l'étendue de la capacité. Actuellement, la principale entité opérationnelle au sein des Forces canadiennes est le Groupe des opérations d'information, dont fait partie le Centre de guerre électronique des Forces canadiennes, lequel soutient nos plateformes tactiques dans une perspective de guerre électronique. Le Groupe des opérations d'information s'occupe du renseignement militaire d'origine électromagnétique, des opérations de défense des réseaux et des capacités en matière de guerre électronique. Voilà l'essentiel de notre travail dans l'environnement cybernétique. Je pense que c'est ce dont vous parliez.

Nous travaillons en étroite collaboration avec nos partenaires internationaux pour ce qui touche à la doctrine, aux tactiques, aux techniques et aux procédures, ainsi qu'à l'interopérabilité. Lorsque les Forces canadiennes sont déployées à l'étranger pour participer à des opérations au sein d'une coalition, leurs plateformes doivent être utilisées conjointement avec celles des alliés. C'est pourquoi il est crucial que les systèmes soient interopérables.

Vous avez fait allusion à l'école de Kingston. Je crois que vous faites référence à l'École de l'électronique et des communications. Pour le développement des capacités militaires, l'éducation, la formation, le perfectionnement professionnel et la doctrine sont fondamentaux. On consacre beaucoup d'efforts afin de rendre l'école plus à même de fournir cette capacité.

The Chair: Thank you very much. Senator Nolin, you are next.

[*Translation*]

Senator Nolin: A number of my concerns have been addressed. General Loos, correct me if I am wrong, but is your field of work already being practiced in a theatre of operations? Given the reaction speed needed to deal with the enemy in this case, the normal reactions of a defence system, even though we are talking about an abnormal world, will not work. You will have to react very quickly. If we take the example of Estonia, the systems stopped working in a matter of hours.

My question is the following: how are your services integrated into the joint forces? What level of efficiency is there in the chain of command to ensure that reaction speed is at the heart of your superior's concerns?

Brig.-Gen. Loos: If I may, I will respond in English in order to express myself better.

Senator Nolin: Of course.

[*English*]

Brig.-Gen. Loos: There are a couple of ideas there. You are absolutely correct regarding the daily activity — if you want to characterize it as a battle — dealing with events in terms of probes and malicious activity. It is here, absolutely.

In terms of trying to deal with what is coming at us, it is absolutely correct that, from a technological perspective, the intent is to try to deal with it at network speed. It is why one of our fundamental areas of examination is how we can do better with situational awareness. It comes back to instrumenting networks and talking a bit about how we do better at that. It is how you build in up-front the security and the defensive systems so that you can get a better appreciation of what is going on faster with information technology infrastructure information, what is up, what is down, security event information, so the sensors you have instrumented your networks with tell you what is going maliciously, as well as operational information, operations and exercises that are using those systems to carry out operations. That is part of it.

Other partners in government are working in capabilities to get us closer to being able to deal with threats in real-time. That is part of it.

Organization and structure are absolutely factors that will come into our analysis to say what is good, better and best in terms of how we are organized.

Senator Nolin: I must tell you that the answer you gave to my colleague is a bit troubling because it is a work-in-progress, and you are counting in years to get a result. That is where my concerns are.

La présidente : Je vous remercie beaucoup. Sénateur Nolin, vous êtes le suivant.

[*Français*]

Le sénateur Nolin : Plusieurs de mes préoccupations ont été discutées. Général Loos, est-ce que je me trompe ou votre champ d'activité s'exerce déjà dans un théâtre d'opération? Compte tenu de la vitesse de réaction nécessaire pour faire face à l'ennemi, s'il se présente, les réactions normales d'un système de défense, même s'il s'agit d'un monde anormal, seront hors d'ordre. Vous allez devoir réagir très rapidement. Si on reprend l'exemple de l'Estonie, en quelques heures, les systèmes ont arrêté de fonctionner.

Ma question est alors la suivante : comment vos services s'intègrent-ils avec les opérations interarmées? Quelle efficacité retrouve-t-on dans la chaîne de commandement pour s'assurer que la vitesse de réaction soit au cœur des préoccupations de vos supérieurs?

Bgén Loos : Si vous me permettez, je vais répondre en anglais afin de mieux m'exprimer.

Le sénateur Nolin : Absolument.

[*Traduction*]

Bgén Loos : Vous abordez plusieurs éléments. Vous avez tout à fait raison quant aux activités quotidiennes de surveillance des actes malveillants et des tentatives de sondage des systèmes. On peut parler de bataille. Absolument.

En effet, d'un point de vue technologique, le but est de contrer les menaces à la vitesse des réseaux. Un des principaux points que nous examinons, c'est la manière d'améliorer notre connaissance de la situation. Cela nous ramène à la configuration des réseaux et à son amélioration. La façon dont on bâtit les systèmes de sécurité et de défense au départ permet de comprendre mieux et plus vite ce qui se passe grâce à la technologie et à l'infrastructure de l'information, de suivre les tendances, de recueillir des données sur les incidents compromettant la sécurité. Les capteurs dont sont dotés les réseaux détectent les actes malveillants. Ces systèmes servent aussi pour les renseignements opérationnels, les opérations et les exercices. Cela en fait partie.

D'autres partenaires gouvernementaux cherchent à améliorer la capacité afin de nous aider à contrer les menaces en temps réel. C'est un autre aspect des efforts déployés.

L'organisation et la structure sont sans aucun doute des facteurs dont nous tiendrons compte dans les analyses nous permettant d'évaluer l'organisation des opérations.

Le sénateur Nolin : Je dois dire que la réponse que vous avez donnée à mon collègue est un peu inquiétante; il semble s'agir d'un effort de longue haleine qui produira seulement des résultats dans plusieurs années. Voilà ce qui m'inquiète.

Brig.-Gen. Loos: Yes, but today we have an organization that is charged with the defence of our networks and carrying out network operations. It works under General Mazzolin's command and control. The information operations group, our network operations centre, carries out that responsibility today. They have a chain of command, but they are responsive to and work directly with our strategic joint staff as well as our joint operational commander to share that information that is deemed critical in real time. We have invested already cadres of personnel to start normalizing that and bringing that into those operational headquarters and into our strategic joint staff. That exists today. Is it what we will have at the end of this process? It is probably not. We have work to do, but we have some of those things in place.

Part of normalizing this is allowing operational commanders to understand the environment and then to pose their questions, what we call commander's critical information requirements. What does a commander wish to know about, in this case, the cyber environment? The folks who are working on network operations and defence will then have that list and be able to respond to it, to ensure that the commander and his staff have what is available to help them shape operations.

[*Translation*]

Senator Nolin: As far as defence of the continent is concerned, Canada and the United States developed NORAD a number of years ago. Do you foresee—as soon as possible I hope—given the importance of a quick response when it comes to cyber defence, developing an approach with the Americans that is similar to the one used for NORAD? In other words, one that goes beyond the chain of command and implements a command unit that is agile and capable of reacting quickly?

[*English*]

Brig.-Gen. Loos: I think we are probably treading a little bit into policy questions beyond my current remit.

Senator Nolin: That is fine.

Brig.-Gen. Loos: I do believe we have gained much benefit from our approach in defence of the continent in NORAD, for those reasons and for those areas that are considered strategic in nature, to make sure the right questions get escalated to the right levels for decision.

Do I believe that will be part of our future? I think it will be part of our future, but I cannot tell you right now what that constellation will be. Is it just defence? I think it is a whole-of-government answer.

Bgén Loos : C'est vrai, mais nous avons maintenant une organisation responsable de veiller à la défense de nos réseaux et au bon déroulement des opérations réseau. Elle relève du commandement et du contrôle du général Mazzolin. Le Groupe des opérations d'information, notre centre d'opérations réseau, assume aujourd'hui cette responsabilité. Il suit une chaîne de commandement, mais il peut aussi travailler directement avec l'État-major interarmées stratégique ainsi qu'avec le commandant des opérations interarmées afin que l'information jugée essentielle puisse être mise en commun en temps réel. Nous avons déjà chargé divers effectifs d'entamer la normalisation des opérations en les intégrant au quartier général et au sein de l'État-major interarmées stratégique. C'est ce qui se passe actuellement. Le résultat final sera-t-il différent? Fort probablement. Il nous reste du travail à faire, mais certaines structures ont déjà été établies.

Un aspect des efforts de normalisation consiste à permettre aux commandants opérationnels de comprendre l'environnement et de poser des questions afin de satisfaire à ce qu'on appelle les besoins essentiels du commandant en information. Qu'est-ce qu'un commandant pourrait bien vouloir connaître au sujet de l'environnement cybernétique? Les gens responsables des opérations et de la défense réseau seront ensuite en mesure de répondre aux questions du commandant afin que son personnel et lui aient toute l'information nécessaire à la préparation des opérations.

[*Français*]

Le sénateur Nolin : En matière de défense du continent, le Canada et les États-Unis ont développé NORAD depuis plusieurs années. Envisagez-vous qu'un jour, le plus rapidement possible j'espère, on puisse développer avec les Américains la même approche compte tenu de l'importance de la réaction rapide en matière de défense cybernétique; le même type d'approche développé avec NORAD? Autrement dit, qu'on aille au-delà de la chaîne de commandement et qu'on puisse mettre en place une unité de commandement qui soit agile et capable de réagir rapidement?

[*Traduction*]

Bgén Loos : Je crains qu'on aborde des questions stratégiques qui échappent à mon mandat actuel.

Le sénateur Nolin : Peu importe.

Bgén Loos : J'estime effectivement que nous avons beaucoup bénéficié de l'approche adoptée par le NORAD pour la défense du continent, approche qui permet de faire en sorte que les questions essentielles parviennent aux paliers concernés, dans certaines circonstances et pour certaines raisons considérées stratégiques, aux fins de prises de décisions.

Maintiendrons-nous cette approche à l'avenir? Je pense que oui, mais je ne suis pas en mesure de vous brosser un portrait complet. Sera-t-elle limitée au ministère de la Défense? Je pense qu'elle sera appliquée à l'ensemble du gouvernement.

The Chair: That is fair. We have seen indications that both the President and the Prime Minister have identified that as an area of joint concern under perimeter security and under the question of shared borders. You are right; it is for others to answer.

Senator Mitchell: This is really interesting, and you are explaining it very well. As I am listening to your presentations, it is clear that what you are always talking about — and I do not mean this in any pejorative sense — is defence, so we are defending against these attacks. By definition, it means that some other country, some other entity, is viewing cyber elements as a weapon. Are we looking at weaponizing from the other side, in a sense, or are we simply looking at it as defence; or are we in a new era of warfare, attack and retaliation, where you actually have to look at these cyber considerations not in defensive capability or posture but in attacking posture, that new wars will be fought on those grounds?

Senator Day: Sort of like a good defence is an offence.

Senator Mitchell: It is a weapon in the arsenal that others are using, but do we have it, and should we, or can you say?

Brig.-Gen. Loos: I can say a little bit, but perhaps not as much as you would like.

What I would say is that it is true that there are many nations around the world that are looking at the cyber domain as a domain for military operations and looking at what is in the art of possible for offensive capabilities or, rather, whether you consider it to be offensive or just to deliver effects. If you can accomplish something in your military mission without using kinetic means, which causes less collateral damage but delivers the same end result from a military perspective, then I think many countries are looking at that. Certainly there are many potential adversaries out there that have demonstrated they are prepared to use capabilities to further their own national ends, and that is available in the open press.

Regarding our own ambition, we see that this domain is absolutely one within which we have to be able to operate competently. While our priority is on defence and situation awareness, we have to ensure that we retain the ability to continue to use the cyber environment for purposes to support operations, at a minimum. We have to be able to command and control. We have to be able to connect with sensors and shooters. We talk about being able to assure our own mission, to be able to continue to operate and manoeuvre freely in the cyber environment, but I cannot really speak much beyond that.

Senator Mitchell: You start to imagine a new cold war era where you have mutual virtual deterrents, because they are afraid of what we could do to their cyber configuration as much as we are afraid of what they could do to ours.

La présidente : Votre réponse est acceptable. Le président tout comme le premier ministre se sont tous deux dits préoccupés par cette question dans les dossiers de la sécurité du périmètre et de notre frontière commune. Vous avez raison; c'est une question qu'il faudrait adresser à quelqu'un d'autre.

Le sénateur Mitchell : Ce sujet est fort intéressant et vous l'expliquez très bien. J'ai vite compris, en écoutant votre exposé, que vous parlez toujours de défense et de notre capacité de repousser d'éventuelles attaques — ne pensez surtout pas que je vous fais un reproche. Cela signifie donc qu'un autre pays, une autre entité, envisage des armes cybernétiques. Cherchons-nous, de notre côté, à mettre au point de telles armes, ou nous concentrons-nous seulement sur la défense? Sommes-nous à l'aube d'une nouvelle ère de guerres cybernétiques, où l'on doit penser non seulement aux moyens de se défendre mais aussi aux moyens de passer à l'attaque?

Le sénateur Day : La meilleure défense consiste à attaquer, en quelque sorte.

Le sénateur Mitchell : D'autres pays ont de telles armes à leur disposition. Les avons-nous au Canada? Devrions-nous les avoir? Êtes-vous en mesure de nous le dire?

Bgén Loos : Je peux vous en dire quelques mots, mais sûrement pas autant que vous l'auriez espéré.

Il est vrai que beaucoup de pays du monde cherchent à exploiter les capacités offensives de l'informatique dans le cadre d'opérations militaires ou encore à déterminer s'il existe un potentiel à cet égard ou si elle sert seulement à produire certains effets. Si l'informatique a le potentiel de permettre à une organisation d'atteindre son objectif sans employer des moyens cinétiques, et donc en minimisant les dommages collatéraux, je suppose que beaucoup de pays s'y intéressent. On peut certainement lire dans la presse publique que nombre d'éventuels adversaires ont démontré leur disposition à exploiter de telles capacités au service de leurs intérêts nationaux.

Pour revenir à nos propres intentions, il est indéniable que nous devons être en mesure d'être compétents dans le domaine. Nous avons beau nous concentrer sur la défense et la connaissance de la situation, nous devons également nous assurer de maintenir notre capacité d'utiliser les moyens cybernétiques à notre disposition pour, à tout le moins, appuyer nos opérations. Le commandement et le contrôle sont essentiels. Nous devons pouvoir communiquer avec nos éléments de détection et de tir. Il est question d'assurer le succès de notre mission, de pouvoir opérer et manœuvrer librement dans l'environnement cybernétique; je ne peux pas vraiment me prononcer sur autre chose.

Le sénateur Mitchell : On s'imagine une nouvelle guerre froide, où toutes les parties s'arment de mesures de dissuasion virtuelles car elles craignent toutes les dégâts cybernétiques que l'autre pourrait causer.

Brig.-Gen. Mazzolin: The only adjunct I would mention is that, given the topical nature of cyber, there is a tendency to look upon it as a separate, discrete form. We are indicating that in the context of a contemporary progressive military that is responsible for being able to assert will across the various global commons — air, land and sea, and now cyber — one aspires to being able to provide a range of options to operational commanders and, by extension, our national will to be able to provide a calibrated response to any attack, incursion or activity by a hostile entity.

Bgén Mazzolin : J'aimerais ajouter qu'étant donné sa nouveauté relative, on a tendance à voir l'informatique comme quelque chose de distinct. À notre avis, toute organisation militaire moderne et progressiste responsable d'affirmer sa volonté dans divers environnements — l'air, la terre, la mer et maintenant l'environnement cybernétique — se doit d'offrir toute une gamme d'options aux commandants opérationnels et de permettre à notre volonté nationale de motiver une réponse sur mesure à toute attaque, intrusion ou activité entreprise par une entité hostile.

Senator Mitchell: This raises an interesting question. If another country came and bombed the factory and created a good deal of damage by doing that, it is clearly an act of war. However, now another country could come and meddle with the technology of that factory, do every bit as much damage, send trains off tracks, ending up in huge economic implications, and maybe killing people. Would we view that as an act of war? If so, it speaks to your point about what is a proportionate response to that and whether we have the mechanisms to do a proportionate response to that, which might not be flying over and bombing them. It is an interesting question, how the world is changing and how our perceptions will change, or you could change.

Le sénateur Mitchell : Voilà qui soulève une question intéressante. Si un pays étranger largue des bombes sur une usine et cause des dégâts considérables, il ne fait aucun doute qu'il s'agit d'un acte de guerre. Cependant, si un pays étranger s'en prend aux systèmes informatiques de cette usine et cause tout autant de dégâts en faisant dérailler des trains, entraînant des répercussions économiques et peut-être même des morts, s'agirait-il là d'un acte de guerre? Dans l'affirmative, cela revient à ce que vous avez dit à propos de ce qui constituerait une intervention proportionnelle, puisqu'elle ne consisterait pas nécessairement à envoyer un avion là-bas larguer des bombes; vous avez aussi parlé de la question de savoir si nous avons les moyens d'effectuer de telles interventions. C'est une question intéressante; le monde évolue constamment et nos perceptions changent également.

Brig.-Gen. Loos: I am not sure whether that was a question, but let me respond.

Bgén Loos : Je ne suis pas sûr qu'il s'agissait d'une question, mais je répondrai quand même.

I believe it is entirely possible to view cyber activities that yield effects as an act of war. You will find a growing consensus, certainly among Western, like-minded nations. They are looking at this from an effects perspective. The growing legal interpretation, under the law of armed conflict, is whether the effects are such that you cause significant damage — there is always a range of interpretation for "significant" — or injury or loss of life. Ultimately the question of whether it is an armed attack that necessitates a response will always be a political question, whether it is NATO Article 5 or any other response. It will ultimately come back to a political appreciation of whether that was severe enough to merit a response.

À mon avis, une activité cybernétique qui produit des résultats peut effectivement être perçue comme un acte de guerre. De plus en plus de pays —surtout dans l'Ouest, où les perspectives nationales se ressemblent — s'entendent à ce sujet. Ils s'intéressent principalement aux effets produits. Dans le droit des conflits armés, est considérée comme un acte de guerre toute activité dont les effets causent des dégâts importants, des blessures ou des morts; bien évidemment, ce qui constitue des dégâts importants prête encore à interprétation. Au bout du compte, la question de savoir s'il s'agissait d'une attaque armée justifiant une intervention est politique, qu'il s'agisse ou non d'une intervention de l'OTAN en vertu de l'article 5. Il reviendra aux sphères politiques de déterminer si la gravité de l'attaque justifie une intervention.

Certainly there is a growing consensus among the legal folks who are looking at this. Back to an earlier question on Tallinn, one of the great benefits of the efforts at the NATO Cooperative Cyber Defence Centre of Excellence is their work in exposing these ideas and drawing in consensus on how we could and should view these activities. The belief is that international law is actually good enough to consider some of these things if you look at it from an effects perspective and what effect was delivered and whether it was severe enough.

C'est le consensus croissant dans le milieu juridique. Pour revenir à la question de Tallinn, le plus grand succès du Centre d'excellence en cyberdéfense de l'OTAN repose sur la diffusion de ces idées et la création d'un consensus sur l'interprétation de ces activités. On estime que le droit international convient parfaitement si l'on s'en tient aux effets produits et à leur gravité.

The Chair: The issue, of course, is authorship, figuring out who did it.

La présidente : Bien évidemment, tout revient à trouver l'entité responsable.

Senator Dawson: I was in Tallinn, and we did a study. I will not repeat the fact that we do not have a digital plan for Canada. We do not have one for the whole country. Therefore, it is quite

Le sénateur Dawson : J'ai visité Tallinn dans le cadre d'une étude que nous avons effectuée. Je ne répéterai pas le fait que le Canada n'a aucun plan pour l'amener à l'âge du numérique. Nous

obvious that we have problems with digital literacy. Not only are we ignorant about cyber attacks, but we are basically ignorant of cyberspace. We are not educating our young people. Technology is overtaking us.

The question would basically be, as far as Tallinn is concerned, that they could react because they had the digital strategy. They knew what they were doing in the digital world. They invented Skype.

How can you play your role if the rest of the country, the provinces and the private enterprises, are not intertwined with you to be sensitive to not only the text but also the whole literacy part of the Internet, how it should be better planned by governments, plural, because it does concern the provinces as much as the central government? Is the rest of the government playing a role to support you in your efforts? Yes or no?

Brig.-Gen. Loos: If I can paraphrase, I think you are asking me whether the government is doing a good enough job on the cyber file.

Senator Dawson: All governments, the provinces, et cetera.

Brig.-Gen. Loos: Honestly, I do not think I am in the best vantage point to offer an opinion on that. Certainly, I do know that Public Safety has the explicit lead for coordinating with other levels of government and with critical infrastructure.

As I mentioned before, you are absolutely right: There is a military nexus there; there is an interest because they have to understand their role. When it is time for operations — even if it is domestic response aid to civil power operations — if the power is out, it affects military operations. If the transportation system is down, then it will effect military operations. We have an interest, and we have to have a seat at the right whole-of-government tables. For what it is worth, we have something to offer at those whole-of-government tables because we are versed in dealing with security situations of a scope and scale that are multivariate, with many different activities going on, and we can bring planning expertise to the table, if and when it is required, to deal with something coming out.

Do we need industries to be better aware of what is going on? Absolutely. Public Safety has that remit. From what I know and from recent reports from the Auditor General, progress is being made.

The Chair: We had testimony on that last week. There are industry groups feeding in and vice versa. The point that we have all seen written about a lot is that we all have to take more responsibility for this and ensure that we are taking some precautions when we use these things and when we go to the bank because every piece of this puzzle counts.

n'avons aucun plan national. Il est donc plutôt évident que nos compétences numériques laissent à désirer. Non seulement comprenons-nous mal les cyberattaques, nous comprenons mal le cyberespace en général. Nous n'éduquons pas les jeunes. La technologie nous dépasse.

Au bout du compte, si le centre à Tallinn a pu intervenir, c'est parce qu'il avait une stratégie numérique. Il savait ce qu'il faisait dans le monde numérique. C'est là qu'on a inventé Skype.

Comment pouvez-vous jouer votre rôle si le reste du pays, les provinces et les entreprises privées, ne collaborent pas avec vous afin de mieux comprendre les rouages d'Internet, ce qui permettrait également aux gouvernements — car les provinces sont également concernées, pas seulement le gouvernement central — d'améliorer leurs efforts de planification? Le reste du gouvernement vous appuie-t-il dans vos efforts? Oui ou non?

Bgén Loos : Autrement dit, vous me demandez si le gouvernement en fait assez dans le domaine.

Le sénateur Dawson : Tous les gouvernements, y compris provinciaux et autres.

Bgén Loos : Honnêtement, je ne pense pas être bien placé pour m'exprimer là-dessus. Ce que je sais, c'est que le ministère de la Sécurité publique a la première responsabilité pour ce qui est d'assurer la coordination avec d'autres ordres de gouvernement et avec l'infrastructure essentielle.

Je répète que vous avez tout à fait raison : les militaires sont bel et bien concernés, car il est dans leur intérêt que tout le monde comprenne son rôle. Lorsque vient le moment de passer à l'action, même s'il s'agit d'une opération locale d'aide au pouvoir civil, toute panne de courant affectera les opérations. De même, toute perturbation dans le système de transport affectera les opérations. Il est dans notre intérêt d'assister aux réunions regroupant l'ensemble des instances gouvernementales. Pour ce que ça vaut, nous avons quelque chose à contribuer à ces réunions, car nous sommes habitués à répondre aux situations de sécurité de portée et d'ampleur variables en coordonnant toute une gamme d'activités distinctes; nous pouvons mettre à contribution notre expertise en matière de planification, au besoin, pour répondre à toute éventualité.

Faut-il davantage sensibiliser les industries? Absolument. Cela fait partie du mandat du ministère de la Sécurité publique. D'après ce que je sais et selon de récents rapports du vérificateur général, on fait des progrès à cet égard.

La présidente : Le comité a entendu un témoignage à ce sujet la semaine dernière. Certains groupes industriels interviennent et vice-versa. L'argument qui revient souvent est qu'on doit tous assumer une plus grande responsabilité à cet égard et s'assurer de prendre certaines précautions lorsqu'on effectue des activités en-ligne ou des transactions bancaires; tout le monde a un rôle à jouer.

I want to thank you both very much for giving your testimony today and for being careful. We know when you had to because there are some large issues at stake here. Our thanks to Brigadier-General Greg Loos and Brigadier-General Roberto Mazzolin. I am sure that we will talk to you again in the future.

Ladies and gentlemen, we continue with this session of the Standing Senate Committee on National Security and Defence. Last week at our meeting, Public Safety department officials told us a bit about the cyber security role of the Communications Security Establishment Canada. Today, we will learn more about CSEC and all of the acronyms that we are coming to learn and love on this committee. CSEC is a stand-alone agency that reports to the Minister of National Defence. CSEC is our ultra-secret foreign signals intelligence agency. It protects the federal government's electronic information and communications system and provides specialized advice within the federal government. It is a huge job, getting larger all the time. To shed a little more light on this today, we are joined by John Forster, Chief of CSEC, and Toni Moffa, Deputy Chief, IT Security.

John Forster, Chief, Communications Security Establishment Canada: Thank you, Madam Chair. I have distributed a copy of my remarks, but, in the interests of time, I may skip parts of it and try to leave as much time as possible for questions. Thank you for the invitation to be here today. It is a pleasure for me as the chief of the Communications Security Establishment Canada, or CSEC, your favourite acronym. In the short time I have been chief — I was appointed in February — I have to say that I am tremendously amazed and pleased to be the leader of an organization with such tremendous capabilities and dedicated people.

[*Translation*]

Today, I would like to briefly go over who we are, what we do, and how we contribute to the security and safety of Canada. After which, I would be happy to take your questions.

[*English*]

CSEC has a three-part mandate: first, to collect foreign signals intelligence in accordance with the government's intelligence priorities; second, to provide advice, guidance and services to help protect the electronic information and information infrastructure of importance to the government, which is sort of the key part of our mandate that interests you in terms of your work on cyber security; third, to provide technical and operational assistance to our federal law enforcement and security partners.

Je tiens à vous remercier de votre témoignage aujourd'hui et de la prévoyance dont vous faites preuve. Nous sommes conscients que vous n'aviez pas le choix, étant donné l'importance des enjeux en cause. Nous remercions également le brigadier-général Greg Loos et le brigadier-général Roberto Mazzolin. Je suis certain que nous aurons l'occasion de vous parler à nouveau.

Mesdames et messieurs, nous poursuivons cette séance du Comité sénatorial permanent de la défense et de la sécurité. Lors de notre rencontre de la semaine dernière, des représentants du ministère de la Sécurité publique nous ont brièvement parlé du rôle du Centre de la sécurité des télécommunications Canada en matière de cybersécurité. Aujourd'hui, nous allons en entendre un peu plus au sujet du CSTC et de tous ces acronymes que ce comité doit apprendre à connaître et à aimer. Le CSTC est un organisme indépendant qui relève du ministère de la Défense nationale. Il s'agit de l'organisme ultrasecret de cryptologie, qui protège le système d'information électronique et de communication du gouvernement fédéral et qui fournit à ce dernier des conseils spécialisés en la matière. Il s'agit d'un mandat énorme, qui ne cesse de s'élargir. Pour nous éclairer un peu plus sur le sujet, John Forster, chef du CSTC, et Toni Moffa, chef adjointe responsable de la sécurité des technologies de l'information, sont avec nous aujourd'hui.

John Forster, chef, Centre de la sécurité des télécommunications Canada : Merci, madame la présidente. J'ai distribué une copie de mon témoignage mais il se pourrait que j'en saute des passages, par souci de rapidité, afin de laisser le plus de temps possible pour les questions. Je vous remercie de votre invitation; je suis heureux d'être ici à titre de chef du Centre de la sécurité des télécommunications Canada, ou CSTC, votre acronyme préféré. Je dois dire que, pendant la courte période qui s'est écoulée depuis ma nomination au poste de chef du CSTC, en février, j'ai été particulièrement ravi et fier de diriger cet organisme, qui peut compter sur des capacités impressionnantes et sur un personnel dévoué.

[*Français*]

Tout d'abord, je me propose de vous dire quelques mots sur les raisons d'être du SCTC, sur ses activités et sa contribution au maintien de la sécurité et de sûreté du Canada. Par la suite, je serai disposé à répondre à vos questions.

[*Traduction*]

Le mandat du CSTC consiste à accomplir les trois fonctions suivantes : premièrement, collecter des renseignements électromagnétiques étrangers, conformément aux priorités gouvernementales en matière de renseignements, établies annuellement par le gouvernement; deuxièmement, fournir des conseils, des avis et des services pour aider à protéger les renseignements électroniques et l'infrastructure d'information, qui sont importants pour le gouvernement du Canada; et troisièmement, fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice du mandat qui leur est conféré par la loi.

I would like to start off by saying explicitly that our legislation prohibits CSEC from directing our activities at anyone in Canada or at Canadians anywhere in the world.

[*Translation*]

We have strict policies, procedures, and review mechanisms that ensure that the privacy of Canadians is protected and that the activities of CSEC are lawful.

[*English*]

The most notable of our mechanisms is the external, independent CSE Commissioner, the Honourable Robert Décary, a retired federal court judge, whose office has full authority and complete access to review any aspect of our operations for lawfulness. In every public report on the activities that he and previous commissioners have reviewed over 16 years, CSEC has always been found to be lawful. Last December, we became a separate agency. We were formerly part of National Defence, and we are very much still a part of the National Defence portfolio and family. We work closely with National Defence and the forces, and we report to the Minister of National Defence.

In terms of our organization, our operations, let me explain briefly what it is we do. I trust that the committee understands there will be limits on what I can say in a public forum due to the sensitive nature of our work.

The Chair: Indeed we do.

Senator Dallaire: We are most disappointed about that.

Mr. Forster: So noted. The first part of our mandate is for signals intelligence. We collect foreign signals intelligence, which often can include decrypting information, today's equivalent of code breaking. We produce intelligence that responds to the annual priorities of the government. The government sets the priorities and we work within those. We work with our allies in counterterrorism and other threats and with the forces in their missions abroad, such as in Afghanistan, and provide information to the Government of Canada for policy development, decision making, advance warning, counter measures and forensics on cyber threats.

[*Translation*]

These activities have helped to identify threats to Canada and Canadians beyond our borders, protect the lives of our brave men and women of the Canadian Forces serving abroad, and ensure that senior government decision-makers operate with the best available information.

Il est important de souligner d'emblée qu'en vertu de la loi, quiconque se trouve dans les limites territoriales du Canada ne peut être la cible des activités du CSTC. Il en va de même pour tous les Canadiens, peu importe où ils se trouvent dans le monde.

[*Français*]

Nos politiques, procédures et mécanismes d'examen sont des plus stricts, ce qui nous permet de protéger la vie privée des Canadiens et de mener nos activités en toute légalité.

[*Traduction*]

Le plus remarquable de ces mécanismes est sans doute le Bureau du commissaire du CSTC dirigé par l'honorable Robert Décary, ancien juge de la Cour fédérale, qui a le pouvoir et les accès requis permettant de vérifier si les activités du CSTC sont conformes aux lois. Au cours des 16 dernières années, aucun des rapports d'activités annuels déposés par les commissaires du CSTC n'a fait état d'irrégularités. En décembre dernier, le CSTC est devenu un organisme autonome. Auparavant, le CSTC faisait partie du ministère de la Défense nationale; nous sommes toujours partie intégrante du portefeuille et de la famille de la Défense nationale. Nous collaborons étroitement avec le ministère de la Défense nationale et les Forces canadiennes, et nous relevons du ministre de la Défense nationale.

Quant à notre organisation et nos opérations, permettez-moi de vous expliquer ce que nous faisons. Le comité comprendra que je dois respecter certaines limites concernant ce qui peut être dévoilé en public étant donné la nature sensible de notre travail.

La présidente : Effectivement, nous comprenons.

Le sénateur Dallaire : Nous en sommes très déçus.

M. Forster : C'est noté. Le premier volet de notre mandat consiste à faire la collecte de renseignements électromagnétiques étrangers, ce qui nécessite souvent le décryptage d'information, qui correspond à ce que l'on appelle le « cassage de code » aujourd'hui. Nous fournissons des renseignements, conformément aux priorités annuelles du gouvernement en matière de renseignements. Le gouvernement établit les priorités et nous les respectons. Nous collaborons avec nos alliées dans la lutte contre le terrorisme, ou contre toute autre menace, et avec les Forces armées canadiennes dans le cadre de leurs missions à l'étranger, comme en Afghanistan, par exemple. Nous fournissons au gouvernement du Canada des renseignements qui contribuent à l'élaboration de politiques et la prise de décisions, ainsi que des avertissements, des contre-mesures et l'expertise judiciaire en matière de cybermenaces.

[*Français*]

Ces activités ont permis d'atteindre les objectifs suivants : identifier les menaces pesant sur le Canada et les Canadiens se trouvant à l'étranger, protéger la vie des hommes et des femmes des forces canadiennes qui sont en mission à l'étranger, veillez à ce que les principaux décideurs du gouvernement disposent des meilleures informations possible.

[*English*]

The second part of our mandate, and of interest to this committee, is the information protection aspect. I should point out how challenging and increasingly vital this part of our work has become in the last several years. The growth of the Internet and associated computer and communications technology has been quite astonishing in the past decade. Today over 2 billion people use the Internet, visiting 500 million websites. In 2011 the monthly amount of global traffic was 327 times what it was 10 years earlier in 2000. By 2020 the number of devices used on the Internet will exceed 16 billion, so there will be more mobile devices than people.

Canadians have embraced this technology and are very active and keen users of it, with 81 per cent of Canadians online. The average Canadian spends 45 hours a month surfing the net — probably your kids and grandchildren do considerably more; the rest of us bring the average down, I am sure — generating $15 billion of sales online. Globally, the Internet provides a staggering $570 billion in commerce.

While this explosive growth in communications technology has been revolutionary, it provides a new conduit for malicious activities that can threaten Canadians and their government. Threat actors targeting Canada are increasingly using the Internet as a medium of choice, and threat actors online range in sophistication from the amateur and the curious, to organized criminals, to foreign states that can and do use the Internet for a wide variety of malicious purposes.

Our role is to protect against sophisticated cyber threats that target the government's systems and information. Specifically, we identify potential cyber threats to the government's systems, help departments harden networks, monitor systems for cyber threats, block threats when we can, and help mitigate any potential impact.

Like many defence versus offence situations, our adversaries are constantly changing and improving their methods and technology. Our challenge at CSEC is to remain on the cutting edge of technology to stay ahead of them.

The third element in our mandate is to support federal law enforcement and security agencies in the lawful pursuit of their mandates. We may provide technological advice and assistance to them under their authority, often when they have a warrant or a court order to do so.

[*Traduction*]

Le deuxième volet de notre mandat, d'un intérêt particulier pour le comité, concerne la protection de l'information. D'abord, permettez-moi de souligner à quel point cet aspect de notre travail est devenu de plus en plus difficile et important au cours des dernières années. La croissance de l'Internet, la multiplication des ordinateurs et l'essor des technologies de communication a été fulgurante au cours des 10 dernières années. À l'heure actuelle, on estime à plus de 2 milliards les internautes qui visitent les quelque 500 millions de sites sur le web. En 2011, le trafic mondial sur Internet était 327 fois plus important qu'en 2000. D'ici 2020, le nombre de dispositifs utilisés sur Internet dépassera les 16 milliards, ce qui signifie qu'il y aura plus d'appareils mobiles qu'il y aura d'habitants sur la planète.

Les Canadiens sont particulièrement friands de ce type de technologie, puisque 81 p. 100 d'entre eux utilisent l'Internet. En moyenne, les Canadiens passent 45 heures par mois sur Internet. Vos enfants et petits-enfants y passent plus de temps, j'en suis certain; vous et moi faisons sans doute baisser la moyenne. Les ventes en ligne génèrent plus de 15 milliards de dollars au Canada. À l'échelle mondiale, le commerce en ligne a enregistré des ventes astronomiques totalisant 570 milliards de dollars.

Cette croissance explosive dans le domaine des technologies de communication n'est rien de moins que révolutionnaire; elle a néanmoins créé de nouvelles vulnérabilités par rapport aux activités malveillantes qui menacent les Canadiens et leur gouvernement. Les auteurs de menaces qui ciblent le Canada ont de plus en plus recours à l'Internet. Leur compétence en ligne varie grandement, allant du simple amateur aux organisations criminelles et aux États étrangers qui utilisent l'Internet pour mener une foule d'activités malveillantes.

Notre rôle consiste à protéger les systèmes et l'information du gouvernement contre les cybermenaces sophistiquées qui les visent. Plus particulièrement, le CSTC identifie les éventuelles cybermenaces qui pourraient cibler les systèmes du gouvernement du Canada, il aide les ministères à renforcer leurs réseaux, il surveille les cybermenaces pouvant peser sur les systèmes du gouvernement, il neutralise les menaces s'il y a lieu, et il contribue à l'atténuation de leurs répercussions, le cas échéant.

Comme dans la plupart des situations où il faut se défendre contre des attaques, on voit les adversaires améliorer ou changer continuellement leurs méthodes et les technologies qu'ils emploient. Notre défi consiste à nous tenir à la fine pointe de la technologie de façon à toujours devancer nos adversaires.

Le troisième volet de notre mandat consiste à fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de la sécurité et de l'application de la loi, aux fins de l'exercice des fonctions qui leur sont conférées par la loi. Nous leur fournissons de l'aide et des conseils en matière de technologie, ce qui peut nécessiter l'émission de mandats judiciaires.

[*Translation*]

I should stress that all the activities I just described rely on our partnerships, both domestic and international. Partnerships are essential to what we do.

[*English*]

Domestically, among the most important partners of CSEC are the Department of National Defence and the Canadian Forces, CSIS, RCMP, Foreign Affairs, the Privy Council Office, Public Safety Canada and CBSA. As I mentioned, we work closely with National Defence and the forces to ensure that their systems are protected and that their information needs are met.

We also work closely on cyber-defence responsibilities under the leadership of Public Safety Canada. With the implementation of the Cyber Security Strategy announced in 2010, there is a whole-of-government approach to cyber. As my colleague Graham Flack explained last week, Public Safety is the overall policy lead, as well as serving as the primary interface with other governments, the private sector and the public.

Our role is focused on the first objective of the strategy, which is to protect government systems. We use our unique mandate and our knowledge to discover, detect and respond to cyber threats against the government.

Since 2011, the Cyber Threat Evaluation Centre, or CTEC, has been responsible for receiving reports of suspected cyber activity within the Government of Canada. We are the operational nexus for cyber defence for government systems.

I should note that all government departments and agencies, as you heard from Brigadier General Loos, have a responsibility to protect their systems as well as Shared Services Canada, which is now providing services to a number of departments to ensure their IT systems are protected and robust. We provide advice and support to those efforts.

Internationally, CSEC relies heavily on our cryptological counterparts in the Five Eyes: the United Kingdom, the United States, Australia and New Zealand.

[*Translation*]

We work very closely with our Five Eyes partners to share intelligence, track common threats and tackle technological challenges. These international relationships are vital to the everyday operations and success of CSEC in providing value to the Government of Canada. These relationships give us access to intelligence and technology that would otherwise not be available

[*Français*]

J'aimerais préciser que toutes les activités que je viens de décrire misent sur nos partenariats nationaux et internationaux. Les partenariats sont les plus importants pour le travail que nous faisons.

[*Traduction*]

Au pays, le ministère de la Défense nationale, les Forces canadiennes, le Service canadien du renseignement de sécurité, la Gendarmerie royale du Canada, les Affaires étrangères, le Bureau du Conseil privé, Sécurité publique Canada et l'Agence des services frontaliers du Canada figurent parmi les plus importants partenaires nationaux du CSTC. Comme je l'ai dit plus tôt, le CSTC collabore étroitement et régulièrement avec le ministère de la Défense nationale et les Forces canadiennes pour veiller à ce que leurs systèmes soient protégés et que leurs besoins en matière d'information soient comblés.

Sur le plan des responsabilités touchant à la cyberdéfense, nous travaillons très étroitement avec certains ministères, sous la gouverne du ministère de la Sécurité publique. Grâce à la mise en œuvre de la Stratégie de cybersécurité du Canada annoncée en 2010, il existe une véritable approche pangouvernementale en la matière. Comme mon collègue, Graham Flack, l'a expliqué la semaine dernière, Sécurité publique Canada est le principal responsable en matière de politiques et sert de principal intermédiaire entre les gouvernements, le secteur privé et le public.

Le rôle du CSTC consiste principalement en la réalisation du premier objectif de la stratégie, à savoir la sécurisation des systèmes du gouvernement. Forts de notre mandat et de nos compétences uniques, nous sommes en mesure de découvrir, de détecter et de contrer les cybermenaces qui planent sur les systèmes et les réseaux du gouvernement.

Depuis 2011, le Centre d'évaluation des cybermenaces du gouvernement du Canada (CECM-GC), reçoit des rapports faisant état de cyberactivités pouvant avoir lieu au sein des systèmes du gouvernement du Canada. Le CSTC est donc le centre opérationnel de la cyberdéfense pour le gouvernement du Canada.

Il est également important de souligner, comme l'a fait le brigadier-général Loos, que les ministères et organismes du gouvernement, par l'intermédiaire de Services partagés Canada, sont tenus responsables d'assurer la protection et la robustesse de leurs systèmes de TI. Et le CSTC est en bonne posture pour leur offrir l'expertise et les conseils dont ils ont besoin.

Le CSTC s'appuie largement sur ses homologues de la cryptologie chez ses partenaires de la collectivité des cinq, à savoir le Royaume-Uni, les États-Unis, l'Australie et la Nouvelle-Zélande.

[*Français*]

Nous sommes en contact permanent avec nos partenaires de la collectivité des cinq pour échanger des renseignements, surveiller les menaces communes et résoudre les difficultés en matière de technologie. Les relations avec les partenaires internationaux sont essentielles à la bonne marche des opérations du CSTC qui sont grandement favorisées par le gouvernement et nous donnent accès

to us, as it would not be financially feasible for Canada to develop such capabilities alone. We estimate that the government's $387 million annual investment in CSEC provides access to a $15 billion global partnership represented by the Five Eyes.

[*English*]

The demand for information in the government is growing, both getting it and protecting it, and it is our mission to do both. Information is our business. We continue to gather intelligence to help decision makers safeguard Canadians and promote Canadian interests, while at the same time protecting information entrusted to government from cyber threats.

[*Translation*]

That is why CSEC must constantly continue to develop our own capabilities to ensure that we are properly positioned to combat these threats and protect Canada and Canadians.

[*English*]

Thank you for your attention. Ms. Moffa and I look forward to your questions.

The Chair: I will give you a test case here and see what you feel free to talk about. Say there is a 17-year-old radical hacktivist in a Western country who has been able to hack into the Department of Finance Canada. You become aware of this because of your domestic and international sources. What happens?

Mr. Forster: Our role in CTEC is to monitor government networks. You have to think of it in two sets. We work with international partners to collect intelligence and share information about threats. We then use that and monitor government networks. When we detect incidents, then we work with Treasury Board, which puts out guidelines and standards for government systems; Shared Services Canada, because they now have consolidated the core computer operations for about 45 departments, so it is easy for us to work with them to help; and other departments. We will advise other departments about threats. We will advise them on how to help mitigate the impact and how to get the systems back up and running as soon as possible.

The Chair: You might be the first line, the actual detector?

Mr. Forster: We may be but not always.

à des renseignements et des technologies dont le Canada ne pourrait disposer puisqu'il n'aurait pas les moyens ni matériel ni financier d'appuyer de telles capacités à lui seul. Nous estimons que les quelque 387 millions de dollars que le gouvernement investi annuellement dans l'activité du CSTC mène dans le cadre de la collectivité des cinq lui donnent accès à une infrastructure et des services dont la valeur s'élève à 15 milliards de dollars.

[*Traduction*]

Les besoins du gouvernement en matière d'information ne cessent de croître, tant sur le plan de la collecte que de la protection des renseignements. Il incombe au CSTC de répondre à ces besoins. Le renseignement, c'est l'affaire du CSTC. Nous continuerons donc à collecter des renseignements sur lesquels les décideurs du gouvernement pourront s'appuyer pour protéger et promouvoir les intérêts des Canadiens, tout en protégeant contre les cybermenaces l'information dont le gouvernement a la responsabilité.

[*Français*]

C'est la raison pour laquelle le CSTC doit continuellement perfectionner ses propres capacités s'il veut avoir les moyens de contrer les menaces et de protéger le Canada et les Canadiens.

[*Traduction*]

Je vous remercie de votre attention. Mme Moffa et moi serons heureux de répondre à vos questions.

La présidente : Je vais vous donner un exemple afin de voir ce dont vous êtes libre de discuter. Disons qu'un jeune cybermilitant radical âgé de 17 ans et qui habite un pays occidental arrive à s'introduire dans le système du ministère des Finances du Canada. Vos sources canadiennes et étrangères vous informent de la situation. Que se passe-t-il?

M. Forster : Le rôle du CSTC consiste à surveiller les réseaux du gouvernement. Il faut voir notre tâche en deux parties. En collaboration avec nos partenaires internationaux, nous recueillons et partageons des renseignements au sujet des menaces. Nous utilisons ensuite ces informations pour surveiller les réseaux gouvernementaux. Lorsque nous détectons des incidents, nous travaillons avec le Conseil du Trésor, qui publie des lignes directrices et des normes pour les systèmes gouvernementaux. Nous collaborons aussi avec Services partagés Canada; il nous est facile de les aider, parce qu'ils ont consolidé les activités informatiques de base de 45 ministères. Nous aidons d'autres ministères également : nous les renseignons au sujet des menaces, nous les conseillons sur la manière d'atténuer leur impact et sur la façon de remettre leurs systèmes sur pied le plus rapidement possible.

La présidente : Il est donc possible que vous soyez les premiers à détecter la menace?

M. Forster : Oui, mais ce n'est pas toujours le cas.

[*Translation*]

Senator Dallaire: You said that the government establishes your priorities annually. Can you tell me which government entities give you these priorities? Are they the same entities that fund your operations?

[*English*]

Mr. Forster: The priorities are established by cabinet, so they decide what the government's intelligence priorities are. They do not fund us. We are funded through appropriations like any other department in the Government of Canada.

Senator Dallaire: When you mentioned government, you meant cabinet gives you your priorities. What happens if Google goes rogue? It can digitize everything that is out of print and there is no structure, so the information can be manipulated. Would that fall into your realm or someone else's?

Mr. Forster: I will speak to my realm, which is to protect the Government of Canada's systems and information regardless of where the threat would come from, whether it is from a state actor, hacker group or whomever. Our mandate in law is to help the government protect its information and the systems that are important to the government.

Senator Dallaire: Senator Wallin raised the fact that we just passed a law on anti-terrorism where a Canadian who goes to a country to train to be a terrorist is susceptible to Canadian law and goes through our whole process. You said you do not monitor Canadians beyond our borders. However, if a Canadian is involved in subversive operations, would you be getting that information through your colleagues that would be coming in as one of intelligence sources available?

Mr. Forster: I am not allowed, by law, to direct my activities to Canadians anywhere in the world. I target foreigners, not Canadians. There is a protocol between us and our Five Eyes partners. We do not target each other's citizens regardless. I would no more target an American than they would a Canadian.

Senator Dallaire: Thank you very much.

[*Translation*]

Senator Nolin: In his recent report, the Auditor General of Canada addressed your information sharing mechanisms with your Canadian partners.

[*Français*]

Le sénateur Dallaire : Vous avez dit que le gouvernement vous donne vos priorités annuellement. Êtes-vous en mesure de me dire quelles sont les entités du gouvernement qui vous donnent ces priorités? Est-ce que ce sont ces mêmes entités qui financent vos opérations?

[*Traduction*]

M. Forster : Les priorités sont établies par le Cabinet, qui décide quelles seront les priorités du gouvernement en matière de renseignements. Notre financement ne provient pas du Cabinet. Nous sommes financés par l'entremise de crédits, tout comme les autres ministères du gouvernement du Canada.

Le sénateur Dallaire : Lorsque vous avez parlé du gouvernement, vous vouliez dire que c'est le Cabinet qui détermine vos priorités. Que se passe-t-il lorsque Google fait des siennes? On peut l'utiliser pour numériser tous les ouvrages épuisés, et il n'y a aucune structure en place, alors l'information peut être manipulée. Est-ce que ce genre de choses relèverait de votre compétence ou de celle de quelqu'un d'autre?

M. Forster : Je parlerai de mon domaine, c'est-à-dire la protection des systèmes et de l'information du gouvernement du Canada, quelle que soit l'origine de la menace, qu'il s'agisse d'une entité d'État, d'un groupe de pirates informatiques ou de n'importe qui d'autre. Notre mandat législatif est d'aider le gouvernement à protéger ses renseignements et les systèmes qui sont importants pour lui.

Le sénateur Dallaire : Le sénateur Wallin a dit que nous venons de promulguer une loi antiterroriste selon laquelle un Canadien qui se rend à l'étranger pour s'entraîner en vue de commettre des actes de terrorisme peut être ciblé aux termes de la loi canadienne et être soumis à toutes nos procédures. Vous avez dit que vous ne surveillez pas les Canadiens à l'étranger. Cependant, si un Canadien participait à des opérations subversives, vos collègues feraient-ils partie de vos sources de renseignements à cet égard?

M. Forster : La loi m'interdit de cibler des Canadiens n'importe où dans le monde. Je cible des étrangers, et non des Canadiens. Notre collaboration dans le cadre de la collectivité des cinq est régie par un protocole. Nous ne ciblons pas les citoyens de nos pays respectifs, quelles que soient les circonstances. Je ne ciblerais pas davantage un Américain que les États-Unis ne cibleraient un Canadien.

Le sénateur Dallaire : Merci beaucoup.

[*Français*]

Le sénateur Nolin : Dans son récent rapport, le vérificateur général du Canada s'est intéressé à vos mécanismes de partage avec vos partenaires canadiens.

First, I would like to know what mechanisms are in place for sharing this information. Then, I will come back to the Auditor General. My question is on the nature of the mechanisms. I do not want to get into the details. I just want to know how it works.

Mr. Forster: Certainly.

[*English*]

I will speak briefly and perhaps Ms. Moffa can add in some of the details. Looking at an incident that happened early in 2010 or 2011, the Auditor General found that we needed to share information more quickly. They found it took us a week or so. Since that time we have made progress. One of our concerns must always be the security of the information we provide because it is highly classified, highly sensitive top secret information. We have obligations to our partners who provide it to protect it.

Certainly since that incident we share information with CCIRC, which is the public safety office that works with the private sector and provinces. They have an employee that sits inside our government CTEC centre so we are able to share information more quickly. We have a network between Treasury Board, Shared Services Canada and ourselves to distribute information to government departments extremely quickly through bulletins and emails, et cetera.

Toni Moffa, Deputy Chief, IT Security, Communications Security Establishment Canada: When we have a department that has become a victim, first and foremost we get on the phone quickly with them and deal with their particular situation. As the situation involves other government departments, we pay them visits and explain what they can do to mitigate against what we are seeing. First and foremost is the victim themselves.

Senator Nolin: Have you informed the Auditor General of the steps you have taken, and is he satisfied with that?

Mr. Forster: Yes, we explained our role and development since then. He was commenting on how that particular event unfolded.

Senator Nolin: Was it only one event?

Mr. Forster: His observation was related to that event and we explained how we work now and are trying to share information.

Senator Nolin: Is he satisfied with that?

Mr. Forster: He has never personally told me he is satisfied.

The Chair: I think that was stated in these reports.

Mr. Forster: I do not want to paraphrase him incorrectly, but he made an observation that there that been recent improvements in that vein.

Dans un premier temps, je voudrais savoir quels sont les mécanismes en place pour partager cette information? Ensuite, j'en viendrai au vérificateur général. Ma question concerne seulement la nature des mécanismes; je ne veux pas savoir les détails, mais plutôt comment cela fonctionne.

M. Forster : Certainement.

[*Traduction*]

Je vais en parler brièvement, et peut-être que Mme Moffa peut ajouter quelques détails. En se penchant sur les circonstances entourant un incident qui s'est produit au début de 2010 ou de 2011, le vérificateur général a appris que nous avions mis environ une semaine à partager l'information, et il a déterminé qu'il fallait le faire plus rapidement. Depuis ce temps, nous avons fait des progrès. Nous devons toujours nous soucier de la protection des renseignements que nous fournissons, car ce sont des renseignements hautement classifiés, très sensibles et très secrets. Nos obligations envers nos partenaires nous forcent à protéger les renseignements qu'ils nous fournissent.

Il est évident que depuis cet incident, nous partageons l'information avec le CCRIC, l'organisme de sécurité publique qui travaille avec le secteur privé et les provinces. Il y a un employé du CCRIC au Centre d'évaluation des cybermenaces du gouvernement, alors nous avons pu partager l'information plus rapidement. Il y a un réseau qui relie le Conseil du Trésor, Services partagés Canada et notre organisme pour que nous puissions communiquer l'information très rapidement aux ministères par le biais de bulletins, de courriels, et cetera.

Toni Moffa, chef adjointe, Sécurité des TI, Centre de la sécurité des télécommunications Canada : Lorsqu'un ministère a été victime d'une menace, nous commençons par communiquer avec lui rapidement par téléphone, et nous remédions à la situation. Lorsque la situation concerne d'autres ministères, nous leur rendons visite et nous leur expliquons ce qu'ils peuvent faire pour se prémunir contre les problèmes que nous voyons. Nous intervenons d'abord et avant tout auprès des victimes.

Le sénateur Nolin : Avez-vous informé le vérificateur général des mesures que vous avez prises, et en est-il satisfait?

M. Forster : Oui, nous lui avons expliqué notre rôle et les progrès réalisés depuis ce temps. Ses remarques portaient sur la façon dont cet incident en particulier s'est déroulé.

Le sénateur Nolin : A-t-il parlé d'un incident seulement?

M. Forster : Ses remarques concernaient cet incident, et nous lui avons expliqué comment nous travaillons désormais, et comment nous essayons de partager l'information.

Le sénateur Nolin : Est-il satisfait de cette réponse?

M. Forster : Il ne m'a jamais dit en personne qu'il est satisfait.

La présidente : Je crois que cela a été mentionné dans ces rapports.

M. Forster : Je ne veux pas le citer de façon erronée, mais il a fait des remarques selon lesquelles il y avait eu des améliorations à ce chapitre.

Senator Nolin: Now it is on the record.

The Chair: I think he commented on the clarity and distinction between your responsibilities and CSEC.

Senator Lang: I want to compliment Mr. Forster. Prior to coming to your position now, you were involved in the design and delivery of many government infrastructure stimulus programs under the Economic Action Plan. From where I come from, I can say it was very well done. If you can take any of that credit, you should.

An area of concern is the technology, where we purchase the technology, where it is manufactured and the implications thereof when we buy it.

I notice that we are now saying you must be Canadian for principal jobs for building the new federal email system; you have to have Canadian citizenship. Are we looking at a situation down the road where, in order to ensure that all our technology is fully understood but cannot be interfered with by other international states, we are looking at manufacturing that type of equipment here in North America as opposed to going beyond?

Mr. Forster: Not necessarily as a requirement. I will ask Ms. Moffa to speak to this.

One of our roles is to evaluate equipment and systems and provide advice to Shared Services Canada, which is procuring it across the government, about how to best protect it.

Ms. Moffa: We have several evaluation programs for commercial products that the government procures for their own systems, and particularly in the security aspects of those products. We have programs that look at the security claims and evaluate products to ensure they live up to the claims before being deployed into the government systems. Certainly with Shared Services Canada and the consolidation of government IT enterprise, security becomes even more important. We are putting all our eggs in one basket and we want to ensure we build security in from the outset. All of the components of infrastructure that we are moving toward with Shared Services Canada require extra looks at security. It has become more important to us, yes.

Senator Lang: If we get a chip made outside the country and it comes in and goes through the process you have outlined, what comfort can I take as a Canadian that the information that eventually goes into that chip cannot easily go back to the country that built it? Is there a mechanism built in so that cannot happen from a security point of view?

Le sénateur Nolin : Voilà qui est maintenant dit de manière officielle.

La présidente : Je crois que ses remarques portaient sur le fait d'établir clairement la différence entre vos responsabilités et celles du CSTC.

Le sénateur Lang : Je tiens à féliciter M. Forster. Avant d'occuper votre poste actuel, vous avez participé à l'élaboration et à la mise en œuvre d'un grand nombre de programmes gouvernementaux de stimulation des infrastructures dans le cadre du Plan d'action économique. Je crois que vous avez fait du très bon travail. Vous devriez accepter le mérite qui vous revient.

Il faut tenir compte de la technologie, de l'endroit où on l'achète, de l'endroit où elle est fabriquée, et des circonstances entourant son achat.

Je constate qu'on dit maintenant que pour effectuer les tâches principales associées à la création du nouveau système de courriel fédéral, il faut être citoyen canadien. Peut-on envisager de fabriquer ce type d'équipement en Amérique du Nord plutôt qu'ailleurs afin que toute notre technologie soit bien comprise, et que d'autres pays ne puissent pas nuire à son fonctionnement?

M. Forster : Ce n'est pas nécessairement une exigence. Je vais demander à Mme Moffa d'en parler.

Un de nos rôles consiste à évaluer l'équipement et les systèmes, et à donner des conseils sur la meilleure façon de les protéger à Services partagés Canada, l'organisme responsable de les acheter pour l'ensemble du gouvernement.

Mme Moffa : Nous utilisons plusieurs programmes afin d'évaluer, entre autres, les paramètres de sécurité des produits commerciaux que le gouvernement achète pour ses propres systèmes. Nous utilisons des programmes pour évaluer les produits afin de déterminer s'ils sont conformes aux allégations en matière de sécurité avant qu'ils soient déployés dans les systèmes du gouvernement. Évidemment, depuis la création de Services partagés Canada et le regroupement des services de TI du gouvernement, la sécurité est devenue un aspect encore plus important. Nous mettons tous nos œufs dans le même panier, et nous voulons nous assurer de mettre en place des mécanismes de sécurité dès le début. Avec toutes les composantes de l'infrastructure que nous voulons mettre en place en collaboration avec Services partagés Canada, nous devons accorder une attention particulière à la sécurité. C'est effectivement un aspect qui a pris une plus grande importance pour nous.

Le sénateur Lang : Si nous nous procurons une puce informatique fabriquée à l'étranger, et si nous la soumettons au processus dont vous avez parlé, comment pouvez-vous assurer aux Canadiens que l'information qui y sera stockée ne pourra pas être transmise facilement au pays où la puce a été fabriquée? Est-elle dotée d'un mécanisme qui empêche ce genre d'atteinte à la sécurité?

Mr. Forster: At the moment we focus on equipment that the government will buy for its systems. That is our primary focus. Our goal is not to ensure that your home computer is okay; our role is to help the government to ensure that its equipment and networks are safe and secure.

Senator Lang: I understand that. I am trying to understand this "star wars" that we are now involved with on a day-to-day basis. Looking ahead, when we do buy that chip, that is basically a question of security and whether it will maintain its security. If we are not building it here in North America, it is built somewhere else. I will not say "anywhere else." They will have some information of what that chip is, what is in that chip and how to access that chip. Am I correct in thinking that?

In other words, how do we ensure once it arrives here if we buy it offshore that full security is there and access is not available to other countries because of the technology they have?

Mr. Forster: When we work with Shared Services Canada for procurement, such as the systems put out for tender, our responsibility is to give them advice and to ensure in that process that they buy equipment and systems that we feel we can absolutely trust in terms of security. That is the advice we provide them.

We help them in that procurement. We have worked with them in the one they are doing now, and we will provide that advice to them with regard to their options and equipment they will purchase for government systems.

Ms. Moffa: Perhaps it might help to add that when we do an evaluation of products, we examine them closely. All commercial products have some vulnerability in them, whether deliberately or inadvertently, as part of the product. As we find those vulnerabilities in those products, we look at ways to deal with them, whether they require changes to the products or changes to network configurations and architectures to mitigate some of those vulnerabilities. There are many ways to deal with the vulnerabilities we may find in any particular product — whether that be hardware or software — that the government uses.

It is a difficult question to answer because there are many ways of assessing vulnerabilities and mitigating them. Depending where they fit in the overall architecture of a system, we would provide tailored advice in that regard.

The Chair: Thank you. I realize that is a difficult one to be specific about when the technology is neutral in some cases; it is how you put all the pieces together.

Senator Day: You indicated in your remarks that your annual budget is $387 million per year. Is that correct?

M. Forster : Pour le moment, nous nous concentrons sur l'équipement que le gouvernement achètera pour ses systèmes. C'est notre principale préoccupation. Notre objectif n'est pas de protéger votre ordinateur personnel, mais d'aider le gouvernement à faire en sorte que son équipement et ses réseaux soient sécuritaires et protégés.

Le sénateur Lang : Je comprends cela. J'essaie de comprendre cette guerre technologique à laquelle nous devons maintenant faire face de façon quotidienne. Désormais, lorsque nous achèterons une puce, il faudra veiller à ce qu'elle soit et demeure sécuritaire. Si elle n'est pas fabriquée en Amérique du Nord, c'est qu'elle est fabriquée ailleurs, et je ne veux pas dire n'importe où ailleurs. L'autre pays aura des renseignements sur la nature de cette puce, sur ce qu'elle contient, et sur la façon d'accéder à son contenu. Ai-je raison?

Autrement dit, si nous achetons une puce fabriquée à l'étranger, comment être certain que tous les mécanismes de sécurité nécessaires sont en place, et que d'autres pays ne peuvent pas accéder à l'information grâce à la technologie dont ils disposent?

M. Forster : Lorsque nous travaillons avec Services partagés Canada à des fins d'approvisionnement, comme c'est le cas pour les systèmes faisant l'objet d'un appel d'offres, notre responsabilité est de le conseiller et de faire en sorte que ce processus lui permette d'acheter l'équipement et les systèmes qui nous semblent entièrement dignes de confiance sur le plan de la sécurité. C'est le genre de conseils que nous lui donnons.

Nous aidons Services partagés Canada dans le cadre de ce processus d'approvisionnement. Nous avons travaillé avec l'organisme dans le cadre du processus actuellement en cours, et nous le conseillerons par rapport aux options qui lui sont offertes et à l'équipement qu'il achètera pour les systèmes du gouvernement.

Mme Moffa : Il serait peut-être utile d'ajouter que lorsque nous évaluons des produits, nous les examinons de près. Tous les produits commerciaux présentent certaines lacunes, qu'elles soient voulues ou non. Lorsque nous découvrons ces lacunes, nous essayons de trouver des façons de remédier à la situation, que ce soit en apportant des modifications aux produits ou en modifiant les configurations et les architectures de réseau afin d'atténuer certaines de ces lacunes. Il y a bien des façons de composer avec les lacunes que nous pouvons trouver dans n'importe quel produit utilisé par le gouvernement, qu'il s'agisse d'un matériel ou d'un logiciel.

Il est difficile de répondre à cette question, parce qu'il y a de nombreuses façons d'évaluer les lacunes et de les atténuer. Nos conseils sont adaptés en fonction de la place que le produit occupe dans l'architecture globale d'un système.

La présidente : Merci. Je suis consciente qu'il est difficile de répondre à cette question de façon précise, puisque dans certains cas, ce n'est pas la technologie qui est en cause, mais la façon dont les composantes sont assemblées.

Le sénateur Day : Vous avez indiqué dans votre exposé que votre budget annuel est de 387 millions de dollars par année. Est-ce exact?

Mr. Forster: Yes.

Senator Day: How many employees do you have?

Mr. Forster: We have around 2,000.

Senator Day: Would most of those be on site? You do not have people throughout government departments, like Shared Services?

Mr. Forster: No, we are located on one campus.

Senator Day: Okay. With respect to your comment earlier about targeting, you do not target Canadians externally, and all of your work is offshore. However, if it turns out that your target was communicating with or that part of the communications involved a Canadian but that is not what your target was, you would not cease having that target by reason of a Canadian being involved, would you?

Mr. Forster: Maybe I can describe a bit how that works. In the amendments passed in the 2001 Canadian Anti-terrorism Act that you were looking at, there was an amendment to the National Defence Act, which included changes to our mandate. It recognized a shift from the previous days where you might have a single Cold War target and you were monitoring a communication between a person and a person. Now it is into the world of the Internet where you have large volumes of information.

The act allowed that, in pursuit of a foreign target and foreign intelligence, if we inadvertently collected a communication with a Canadian, we had to do it under a ministerial authorization, and we still have to protect the privacy of that individual. It must meet four conditions: It must be directed at a foreign source; it had to be unable to be reasonably obtained otherwise; it had to have value as foreign intelligence; and we had to take steps to protect privacy. We have detailed procedures that protect the privacy of the information that is reviewed by the commissioner when he looks at our operations.

Senator Day: Thank you. The use of the term "intelligence" implies some analysis of the information and the communications that you have picked up. Is there any situation where you would have a direct feed of information without any analysis to either our foreign partners or to other government departments, or is all of the work that you communicate all intelligence-analyzed communication?

Mr. Forster: We collect and then provide information to federal departments and they then use that in their decision making and policy setting. The government has two areas where it does assessment of intelligence: Within the Privy Council Office, there is the Intelligence Assessment Secretariat, and there is ITAC located at CSIS, which looks at intelligence that could come from

M. Forster : Oui.

Le sénateur Day : Combien d'employés avez-vous?

M. Forster : Environ 2 000.

Le sénateur Day : Est-ce que la plupart d'entre eux travaillent sur place? Est-ce que vos employés travaillent au sein des ministères et des organismes gouvernementaux comme Services partagés?

M. Forster : Non, nous travaillons dans un seul établissement.

Le sénateur Day : D'accord. Pour revenir à votre commentaire sur le ciblage, vous ne ciblez pas les Canadiens à l'étranger, et tout votre travail est lié au renseignement étranger. Cependant, si vous découvriez que votre cible communiquait avec un Canadien, ou qu'une partie des communications concernait un Canadien qui n'est pas votre cible, vous n'arrêteriez pas de surveiller votre cible parce qu'un Canadien est concerné, n'est-ce pas?

M. Forster : Je peux peut-être expliquer un peu comment cela fonctionne. Parmi les modifications apportées par la Loi antiterroriste de 2001 que vous examiniez, il y avait des modifications à la Loi sur la défense nationale concernant notre mandat. Ces modifications tenaient compte des changements qui se sont produits par rapport à autrefois. Par exemple, lors de la guerre froide, on pouvait avoir une seule cible, et on surveillait les communications entre deux personnes. Maintenant, nous sommes à l'ère d'Internet, où il faut composer avec un grand volume d'information.

Lorsque nous voulions obtenir des renseignements sur une cible étrangère, et que nous interceptions par inadvertance une communication avec un Canadien, la loi nous obligeait à obtenir une autorisation ministérielle, et nous devions quand même protéger la vie privée de cette personne. L'interception des renseignements doit respecter les quatre conditions suivantes : l'interception vise des entités étrangères; les renseignements ne peuvent raisonnablement être obtenus d'une autre manière; la valeur des renseignements étrangers justifie l'interception; il existe des mesures pour protéger la vie privée. Nous suivons des procédures détaillées pour protéger la confidentialité des renseignements, et ces procédures font l'objet d'un examen par le commissaire.

Le sénateur Day : Merci. L'utilisation du terme « renseignement » implique une certaine analyse du renseignement et des communications que vous avez interceptés. Existe-il des situations où vous pourriez communiquer directement un renseignement à nos partenaires étrangers ou à d'autres ministères sans devoir l'analyser ou est-ce que tous les renseignements que vous communiquez doivent faire l'objet d'une analyse?

M. Forster : Nous recueillons des renseignements, puis nous les fournissons aux ministères fédéraux, qui les utilisent ensuite pour prendre leurs décisions et élaborer leurs politiques. Il y a deux organismes gouvernementaux qui procèdent à l'évaluation du renseignement. Il y a le Secrétariat de l'évaluation du renseignement du Bureau du Conseil privé, puis il y a le CIET

a variety of sources, human intelligence or electronic, in our case.

Senator Day: Would there ever be a situation where you would communicate intelligence or communication that you have developed directly to a Canadian company? For instance, you might learn about intellectual property being hijacked and stolen, or you might develop some information with respect to a takeover bid that would be of value to the Canadian company.

Mr. Forster: We generally provide intelligence to government departments. If there was a threat to a Canadian company, we would work with CSIS and the RCMP.

Senator Day: Should I play on the word "generally"?

Mr. Forster: No, no intention was implied. We would work with our domestic agencies — RCMP and CSIS — who have that responsibility for domestic.

Senator Day: Thank you.

Mr. Forster: Having said that, just to clarify, in terms of general threat information and advice to industry in the private sector, again, we work through the sector councils that Mr. Flack explained to you last week to help them understand cyber threats and the things they need to do.

Senator Day: This might be information that a particular company would not want shared with all of its competitors in the council, but very important information all the same — intelligence for its own purposes.

Mr. Forster: We would provide information, as I said, to the RCMP if there was criminal activity or to CSIS if there was a threat to national security.

Senator Day: Thank you.

The Chair: Is that again how you would deal with a Canadian bad guy somewhere? Are your rules preventing you from dealing with that directly? Would you just supply others with that information?

Mr. Forster: We would share the intelligence. We would protect the privacy of the Canadian. If the agencies come to us under their lawful mandates to get access to that, then we can provide it under their lawful authority.

The Chair: Thank you. That is clear.

Senator Johnson: Thank you for your presentation. I think there was a lot in there, especially about Canadians spending two days a week surfing the Internet.

You stated specifically three things about your mandate. I am interested in the foreign signals intelligence you collect in accordance with government intelligence priorities. First, can you tell us what you are looking for when you are scanning

du SCRS, qui examine des renseignements pouvant provenir de diverses sources, à savoir des sources humaines ou des sources électroniques, dans le cas qui nous occupe.

Le sénateur Day : Y aurait-il des situations où vous transmettriez directement un renseignement ou des outils de communications que vous avez mis au point à une compagnie canadienne? Par exemple, si vous appreniez qu'il y a eu un détournement et un vol de propriété intellectuelle ou si vous avez des renseignements à communiquer sur une offre publique d'achat qui seraient utiles à cette compagnie.

M. Forster : Nous fournissons généralement des renseignements aux ministères. Si une compagnie canadienne était menacée, nous travaillerions avec le SCRS et la GRC.

Le sénateur Day : Est-ce que je devrais déduire quelque chose de votre utilisation du terme « généralement »?

M. Forster : Non, je ne voulais rien dire par cela. Nous travaillerions avec nos organismes nationaux — la GRC et le SCRS — qui s'occupent des menaces à l'échelle nationale.

Le sénateur Day : Merci.

M. Forster : Cela étant dit, j'aimerais préciser que, pour ce qui est des conseils et des renseignements relatifs aux menaces générales qu'il faut fournir aux compagnies du secteur privé, nous travaillons dans les conseils sectoriels dont M. Flack a parlé la semaine dernière afin de les aider à comprendre les cybermenaces et les mesures qui doivent être prises.

Le sénateur Day : Ce pourrait être des renseignements qu'une compagnie ne voudrait pas partager avec tous ses concurrents au conseil, mais qui sont quand même très importants; des renseignements qui ont leurs propres fins.

M. Forster : Comme je l'ai dit, nous fournirions des renseignements à la GRC en cas d'activités criminelles ou au SCRS en cas de menace à la sécurité nationale.

Le sénateur Day : Merci.

La présidente : Est-ce de cette façon que vous allez vous attaquer à des criminels canadiens? Est-ce que vos règles vous empêchent de vous attaquer directement au problème? Est-ce que vous ne feriez que fournir ces renseignements à d'autres?

M. Forster : Nous partagerions les renseignements. Nous protégerions la vie privée des Canadiens. Si, dans le cadre de leur mandat légal, les organismes fédéraux nous demandent un accès à ces renseignements, nous pourrons accéder à leur demande.

La présidente : Merci de cette explication claire.

Le sénateur Johnson : Merci de votre intervention. Je crois qu'elle fournissait beaucoup de détails, surtout sur le fait que les Canadiens passent deux jours par semaine à naviguer sur Internet.

Vous avez précisé trois choses sur votre mandat. Je veux en savoir plus sur le renseignement électromagnétique étranger que vous recueillez conformément aux priorités du gouvernement en matière de renseignement. Premièrement, pouvez-vous nous dire

foreign signals and what you do with what you find? Second, is your scope as broad as that of the American National Security Agency?

Mr. Forster: In terms of how we operate, as I said, the government sets its priorities for our mandate. If it is counterterrorism or cyber security, our role is to try to provide intelligence and information to the government to assist with that issue. Again, we collect it and we provide it to other departments to help them with their decision making, their actions and so on.

Each of the Five Eyes partners has a different mandate, but we work closely together. We have different structures. Some of us are in different agencies, so I would not want to draw comparisons between them.

Our mandate is as it is defined here, as I have explained.

Senator Johnson: There is a great deal of discussion among our allies, especially the United States, about the need to move from passive to active computer network defence. Can you discuss that, your interpretation of "active network defence" and some of the issues it raises for CSEC?

Mr. Forster: Again, at this point, if you look at our legislation and our mandate, I am an intelligence agency, I have a mandate to collect foreign information and I have a mandate to protect the Government of Canada's networks from people trying to infiltrate it. I do not look at my mandate in terms of defence and offence. My job is to protect those networks and how to protect them, either through verifying the equipment and so on that goes into them, monitoring those networks for threats from a range of actors and then helping the government departments mitigate, correct and repair those systems. I do not have an offensive mandate, if you will.

Senator Johnson: How do you think we stand in the world in this field? Where would you position us comparatively? Are we number one?

Mr. Forster: Canada and CSEC, like others of our agencies, are smaller in size than the U.S. and the U.K. I would like to think our people are second to none and that we have certain capabilities that are world-class, world-leading technology. It is hard to evaluate our agency against some of our much larger partners.

Senator Johnson: I understand. Where do we excel?

Mr. Forster: I have to tell you as a newcomer to this organization for nine months, these people blow my socks off. They are some of the smartest people, not just in the government but also in the country. The technologies they use are leaders in the government. They are amazing people, and it is an amazing organization.

Senator Johnson: That is good to know. Thank you.

ce que vous cherchez quand vous analysez les signaux étrangers et ce que vous faites avec ce que vous trouvez? Deuxièmement, est-ce que la portée de votre mandat est aussi grande que celle de l'agence de la sécurité nationale américaine?

M. Forster : Pour ce qui est de notre fonctionnement, comme je l'ai dit, le gouvernement établit les priorités de notre mandat. Si c'est le contre-terrorisme ou la cybersécurité, notre rôle consiste à fournir des renseignements au gouvernement pour l'aider à régler ce problème. Comme je l'ai déjà dit, nous recueillons les renseignements, puis nous les fournissons à d'autres ministères pour les aider à prendre des décisions et des mesures, entre autres.

Chacun des partenaires des Five Eyes a un mandat différent, mais nous travaillons en étroite collaboration. Nous avons des structures différentes. Certains d'entre nous sont dans des organismes différents. Je ne voudrais donc pas établir de comparaisons entre eux.

Notre mandat est celui que j'ai défini ici.

Le sénateur Johnson : Chez les alliés du Canada, et plus particulièrement les États-Unis, il est beaucoup question du passage d'une défense passive des réseaux informatiques à une défense active. Pourriez-vous parler de votre interprétation de la défense active des réseaux et des problèmes qu'elle pose au CSTC?

M. Forster : Comme je l'ai dit, il est clair en examinant notre mandat et la loi qui nous régit que nous sommes un organisme de renseignement. Notre mandat consiste à recueillir des renseignements étrangers et à empêcher les gens d'infiltrer les réseaux du gouvernement du Canada. Je ne perçois pas mon mandat comme un mandat de défense contre les attaques. Mon travail consiste à trouver des moyens de protéger les réseaux, que ce soit en vérifiant leur équipement ou en vérifiant les diverses menaces auxquelles ils sont exposés, puis en aidant les ministères à atténuer les menaces, ainsi qu'à corriger et à réparer ces systèmes. Je n'ai pas de mandat offensif, si je peux m'exprimer ainsi.

Le sénateur Johnson : À quel rang le Canada se classe-t-il dans ce domaine par rapport aux autres pays? Sommes-nous au premier rang?

M. Forster : Le Canada est plus petit que les États-Unis et le Royaume-Uni. Nos organismes, notamment le CSTC, sont donc eux aussi plus petits que ceux de ces deux pays. J'aimerais croire que personne ne surpasse notre organisme et que nous avons certaines capacités et technologies qui sont imbattables dans le monde. Cependant, il est difficile d'évaluer notre organisme par rapport à ceux de nos plus grands partenaires.

Le sénateur Johnson : Je comprends. Dans quoi excellons-nous?

M. Forster : Je dois dire que je travaille seulement dans cette organisation depuis neuf mois, mais ces personnes m'époustouflent. Je crois qu'elles font partie des personnes les plus brillantes, pas seulement au gouvernement, mais dans tout le pays. Elles utilisent des technologies de pointe au sein du gouvernement. C'est une organisation remarquable formée de gens exceptionnels.

Le sénateur Johnson : C'est bon à savoir. Merci.

The Chair: We heard last week from the CCIRC people that this is a difficult world in which to recruit. It is still new. You want top of the line, the folks who will blow your socks off, but we are still in the process of creating them, if you will. Do you have enough people to recruit from in the pool?

Mr. Forster: Generally speaking, overall, I would say we are in good shape. It is certainly a challenge for all of the agencies, whether it is in the U.K., the U.S., Australia or Canada. You are looking for some of the brightest people with the best technological skills possible. You are competing against the Googles and the Facebooks of the world who may be able to offer slightly more than the Government of Canada.

The Chair: Do you think?

Mr. Forster: Maybe a few better perks, but we also offer some pretty unique things. When you talk to people who work at CSEC, they come and a lot of them stay. You will not find more interesting work anywhere in the country than what these people do.

The Chair: With respect to Senator Johnson's question, you folks have chief responsibility for developing the mitigation strategies, not out there waging cyber war but figuring out what to do as opposed to within each department. You are the brain trust for the mitigation piece.

Mr. Forster: I think Brigadier-General Loos spoke to this in his remarks. You have to think about cyber as a team sport; each of us has responsibilities. Public Safety has the overall policy lead. We play a leadership role in protecting government systems. That does not mean each department is let off the hook — absolutely not. Each and every one of them has a responsibility to protect their networks. If you look at our website, we put up 35 basic steps. If we, Canadians and businesses did just 5 or 10 of those, you would deal with 80 per cent of what is coming at you. We have a responsibility and the private sector and provinces do as well to protect their information and protect their systems.

The government strategy tries to recognize that this is not a Government of Canada issue; this is a Canada issue. You need to provide leadership and coordination in getting everyone on that.

Senator Day: My question relates to your comment earlier about your role on the team. You were part of National Defence and you still report up through National Defence, but you are an agency. What was the reason for creating you as a separate, stand-alone agency? How did that relate to your relationship with the rest of the departments within the Canadian government?

La présidente : La semaine dernière, des représentants du CCRIC ont dit que le recrutement dans ce secteur était difficile. C'est un secteur encore nouveau. Vous voulez des employés remarquables qui vous couperont le souffle, mais nous sommes encore en train de les former. Est-ce que le bassin de recrutement est assez grand?

M. Forster : Dans l'ensemble, je dirais que nous nous débrouillons bien. Le recrutement est certainement un problème pour tous les organismes, qu'ils soient au Royaume-Uni, aux États-Unis, en Australie ou au Canada. Nous voulons recruter les personnes les plus brillantes et celles qui possèdent les meilleures compétences technologiques possibles. Nous faisons concurrence à des compagnies comme Google et Facebook, qui pourraient être en mesure d'offrir un peu plus à leurs employés que le gouvernement du Canada.

La présidente : C'est ce que vous pensez?

M. Forster : Elles offrent peut-être quelques meilleurs avantages, mais nous offrons nous aussi des avantages assez uniques. Beaucoup d'employés du CSTC restent là-bas parce qu'ils font le travail le plus intéressant au Canada.

La présidente : Pour revenir à la question du sénateur Johnson, vous êtes les principaux responsables de l'élaboration de stratégies d'atténuation. Vous ne livrez pas de cyberguerre, mais vous élaborer une stratégie pangouvernementale plutôt que des stratégies distinctes pour chaque ministère. Vous êtes des experts en matière de stratégie d'atténuation.

M. Forster : Je crois que le brigadier-général Loos en a parlé dans son intervention. Vous devez penser à la cybersécurité comme un sport d'équipe où chacun a ses responsabilités. Le ministère de la Sécurité publique est le principal responsable en matière de politiques. Nous jouons un rôle de premier plan dans la protection des systèmes gouvernementaux. Cela ne veut pas dire que les autres ministères n'ont pas leur rôle à jouer à cet égard — pas du tout. Chaque ministère a la responsabilité de protéger ses réseaux. Sur notre site web, nous avons énuméré les 35 étapes de base à suivre. Si les citoyens canadiens et les entreprises suivaient juste cinq ou 10 de ces étapes, ils observeraient déjà une diminution de 20 p. 100 de leurs problèmes de réseau. Tout comme le secteur privé et les provinces, nous avons la responsabilité de protéger nos renseignements et nos systèmes.

Dans la stratégie gouvernementale, on souligne que ce n'est pas un problème qui découle du gouvernement canadien, mais du Canada lui-même. Vous devez faire preuve de leadership et de coordination pour veiller à ce que toutes les personnes assument leurs responsabilités à cet égard.

Le sénateur Day : Ma question porte sur la remarque que vous avez faite plus tôt sur votre rôle dans l'équipe. Le CSTC faisait partie de la Défense nationale, et il relève encore de ce ministère. Cependant, il est maintenant devenu un organisme autonome. Pour quelle raison le CSTC est-il devenu un organisme autonome et distinct? Est-ce que cela avait un rapport avec votre relation avec le reste des ministères du gouvernement canadien?

Mr. Forster: With respect to the history of the organization, it was started in 1946. It was a small, dark corner at the National Research Council, and in the 1970s it moved to National Defence. It has always played an integral role with the forces, helping them protect their communications and information.

The decision recognized two things: First, the agency has a broader mandate with the government as a whole, but it still has a close mandate with the Canadian Forces and the Department of National Defence; second, with cyber becoming more important, it made sense to establish it as a separate, stand-alone agency. We have to work with a range of departments: Treasury Board, Shared Services, and CSIS. We do a lot of work with the service. We have quite a job to do with a number of departments.

Senator Day: Does being an agency make it easier to deal with those other departments?

Mr. Forster: I think it is just recognition of that broader mandate and that the size of the agency has grown to a point where it made sense.

Senator Manning: You mentioned the Five Eyes partners, and the countries are definitely our allies: the United Kingdom, the United States, Australia and New Zealand. You made a comment in your opening remarks about the importance of the partnership because it would be financially unfeasible for Canada to develop such capabilities alone. How did the Five Eyes partners come about? Is any effort being made to include others in the partnership, so that you deal with it from the financial aspect of the information and intelligence that is gathered? Maybe you can explain to us how that works.

Mr. Forster: The origin of the Five Eyes partnership came out of the Second World War. There was very close collaboration, particularly between the United Kingdom and the U.S. in that space. It evolved after the war into a partnership with Australia, New Zealand and Canada being part of that Commonwealth effort.

The partnership there is extremely close. It is not to say that we do not work with other countries or nations or that others do not as well. It is just that the Five Eyes in particular collaborate very closely in sharing both intelligence and information on threats. When you are looking at cyber, part of the value we can bring is that we are sharing information with these other countries on threats and what we are all seeing in the global information infrastructure. That is not to say that we do not work with other countries when and where we need to.

Senator Manning: That segues into my second question. When you go outside the partnership of the Five Eyes, how do you decide or figure out whom to trust when you are sharing information and intelligence? Is it criteria-based? How do you decide that?

M. Forster : En ce qui concerne l'histoire de l'organisme, il a été créé en 1946. Il occupait un petit coin sombre dans les locaux du Conseil national de recherches avant de déménager dans ceux du ministère de la Défense nationale dans les années 1970. Il a toujours joué un rôle essentiel dans les forces en les aidant à protéger leurs communications et leurs renseignements.

Il y a deux raisons pour cette décision. Premièrement, l'organisme a un mandat plus large au sein du gouvernement, mais il a encore un mandat auprès des Forces canadiennes et du ministère de la Défense nationale. Deuxièmement, compte tenu de l'importance croissante de la cybersécurité, il était logique de créer un organisme autonome et distinct. Nous devons travailler avec divers ministères : le Conseil du Trésor, Services Partagés et le SCRS. Nous faisons beaucoup de travail auprès du service. Nous avons tout un travail à faire avec de nombreux ministères.

Le sénateur Day : Est-ce que le fait d'être un organisme distinct facilite votre travail avec les autres ministères?

M. Forster : Je pense que cette décision a seulement été prise pour reconnaître notre plus large mandat et le fait que la taille de notre organisme avait beaucoup augmenté.

Le sénateur Manning : Vous avez mentionné nos partenaires des Five Eyes, à savoir le Royaume-Uni, les États-Unis, l'Australie et la Nouvelle-Zélande. Ces pays sont certainement nos alliés. Au début de votre intervention, vous avez parlé de l'importance de ce partenariat parce qu'il serait financièrement impossible pour le Canada de développer ces capacités tout seul. Comment ce partenariat est-il né? Est-ce que des efforts sont déployés pour inclure d'autres pays dans le partenariat afin de pouvoir se pencher sur l'aspect financier des renseignements recueillis? Vous pouvez peut-être nous expliquer comment cela fonctionne.

M. Forster : Le partenariat des Five Eyes a été créé pendant la Seconde Guerre mondiale. Il y avait une collaboration très étroite dans ce domaine, surtout entre le Royaume-Uni et les États-Unis. Après la guerre, l'Australie, la Nouvelle-Zélande et le Canada, en tant que membres du Commonwealth, ont adhéré au partenariat.

C'est un partenariat très étroit. Cela ne signifie pas que nous ne travaillons pas avec d'autres pays ou que les autres pays ne collaborent pas entre eux. C'est juste que les Five Eyes, en particulier, ont une collaboration très étroite en ce qui a trait à l'échange de renseignements sur les menaces existantes. Un des avantages de ce partenariat de cybersécurité est que nous échangeons des renseignements avec quatre autres pays sur les menaces et les autres choses que nous observons dans l'infrastructure mondiale d'information, ce qui ne veut pas dire que nous ne travaillons pas avec d'autres pays lorsque le besoin s'en fait sentir.

Le sénateur Manning : Ce qui nous mène à ma deuxième question. Quand vous agissez hors du partenariat des Five Eyes, comment décidez-vous ou déterminez-vous à qui vous pouvez faire confiance lorsque vous communiquez des renseignements? Avez-vous des critères? Comment prenez-vous cette décision?

Mr. Forster: It is a decision made about what the government's intelligence priorities are and how we can best fulfill those priorities. If it makes sense to collaborate with another country on a particular aspect to help meet the government's priorities, then you may do that, but it is not exactly a formula and it must be a mutual interest.

Senator Manning: When you are gathering information on threats to our own networks, for example, sometimes you will hear of how many hits were made against the security network today. Is that information public? How many attempts are made on a daily basis to the networks in Canada?

Mr. Forster: We do not make that information public. We are measuring the government's systems, not the country's systems.

Senator Lang: If I could ask a supplementary. Why do we not make it public so that people are aware that this is going on and so that Canadians are aware of how serious this is? We should be following the 35 steps you outlined earlier.

Mr. Forster: The 35 steps are certainly public. We promote them, as does Public Safety.

We are measuring the Government of Canada's systems; we are not measuring what happens in the country. We are not able to do that. It is not part of our mandate.

Senator Lang: Who measures that?

Ms. Moffa: There are companies that put out annual reports about global statistics, such as Symantec, McAfee and others. They have good information resources about what they learn about publicly known threats.

The Chair: Senator Lang's question goes to a point. I guess it is always an issue in the defence department, and certainly the security issue, which is that there is some responsibility to educate and maybe even to shock people into some kind of action, when you lay these statistics out about usage and how much time in a day we use these pieces of equipment, how vulnerable we might be, and the need to not tell them what we know or, maybe more important, tell them what we do not know. That is constantly the juggle, and which one of those things is more problematic?

Mr. Forster: As Ms. Moffa mentioned, a number of the security companies do publish estimates of this sort of activity. For example, McAfee estimates there are 75 million unique pieces of malware floating out in the global Internet, or that botnets create about 89.5 billion unsolicited emails every day. There are estimates out there by private firms for that. We are not monitoring the Internet in Canada; we are monitoring the Government of Canada's systems.

Senator Manning: From your perspective, what is the greatest challenge for this space and for CSEC today?

M. Forster : La décision est prise en fonction des besoins prioritaires du gouvernement en ce qui a trait aux renseignements et des moyens que nous pouvons prendre pour répondre à ces besoins. S'il est logique de collaborer avec un autre pays sur un aspect précis pour répondre aux besoins prioritaires du gouvernement, alors on peut agir ainsi, mais il n'y a pas de formule exacte et il faut qu'il y ait intérêt mutuel.

Le sénateur Manning : Lorsque vous recueillez des renseignements sur les menaces contre vos réseaux, par exemple, vous savez parfois combien d'attaques ont été faites contre le réseau de sécurité un jour donné. Cette information est-elle publique? Combien d'attaques sont faites chaque jour contre les réseaux canadiens?

M. Forster : Nous ne rendons pas cette information publique. Nous surveillons les réseaux du gouvernement, pas ceux du pays au complet.

Le sénateur Lang : J'aimerais poser une question complémentaire. Pourquoi ne pas rendre cette information publique afin que les Canadiens soient au courant de ces attaques et qu'ils sachent à quel point elles sont sérieuses? Nous devrions suivre les 35 étapes que vous avez décrites plus tôt.

M. Forster : Les 35 étapes sont publiques. Nous en faisons la promotion, tout comme le ministère de la Sécurité publique.

Nous surveillons les systèmes du gouvernement du Canada, pas ceux du pays en entier. Nous n'avons pas cette capacité. Cela ne fait pas partie de notre mandat.

Le sénateur Lang : Qui le fait?

Mme Moffa : Des entreprises produisent des rapports annuels sur les statistiques globales, comme Symantec, McAfee et d'autres. Ces entreprises sont bien renseignées sur les menaces connues.

La présidente : Le sénateur Lang soulève un bon point. Le ministère de la Défense doit toujours tenir compte — et c'est une question de sécurité — de la responsabilité de renseigner les gens, voire de les pousser à agir, lorsqu'on publie des données qui font état de notre utilisation quotidienne de cet équipement et de notre vulnérabilité à cet égard, et de l'importance de ne pas leur dire ce que nous savons, ou, plus important encore, de leur dire ce que nous ne savons pas. Il faut constamment tenir compte de ces éléments. Lequel est le plus problématique?

M. Forster : Comme Mme Moffa l'a souligné, certaines de ces entreprises de sécurité publient des données générales sur les activités de ce genre. Par exemple, McAfee estime qu'il y a 75 millions de logiciels malveillants différents qui flottent dans Internet et que les réseaux zombies créent quelque 89,5 milliards de courriels non sollicités chaque jour. Certaines de ces entreprises publient des données là-dessus. Nous ne surveillons pas l'utilisation d'Internet au Canada, mais bien les systèmes du gouvernement fédéral.

Le sénateur Manning : À votre avis, quel est le principal défi pour le cyberespace et le CSTC aujourd'hui?

Mr. Forster: I think the greatest challenge for all of us in this space is to continue to keep up our skills and abilities and to invest in the technology we need to always stay ahead of adversaries that are trying to infiltrate our government's systems. That is what our people do constantly.

You also have to understand that it is not a static space. The things you see today you would not have seen five years ago. People's capabilities are getting better. The technology is always getting better. You always have to be working and developing your capabilities and technology to stay ahead of that.

Senator Dallaire: You collate intelligence and distribute it to agencies inside the country for their action. As an example, approximately how many military are working in CSEC now?

Mr. Forster: Brigadier-General Mazzolin just said there are about 28 military integrees embedded inside CSEC, but then we work very closely with the CFIOG, for example.

Senator Dallaire: You are still under the National Defence Act; am I correct?

Mr. Forster: Yes.

Senator Dallaire: Why not then move you to the Canadian Security Intelligence Service Act, as a branch of them versus a branch of DND, if I can use the term "branch"?

Mr. Forster: The government decided that the agency would not be a branch of the Department of National Defence; it would be a stand-alone agency, similar to CSIS. Our mandate is foreign, and one of our primary partnerships continues to be with the military, as well as other departments.

Senator Dallaire: It is because cyber is total war, so it covers all spectrums now, more and more. I was wondering whether you feel yourself being limited or whether you are covering the whole spectrum of possible threats that are coming against a nation.

Mr. Forster: We are not a military agency; we are an intelligence agency. We will work with Brigadier-General Mazzolin and Brigadier-General Loos and support them as they look at the military capabilities in cyberspace. Do I feel constrained by being in the defence portfolio? Not at all.

Senator Lang: I would like to turn our attention away from the defence department and towards the responsibility to the private sector and their responsibilities vis-à-vis the technology they have been using. Where do these organizations come in? I am primarily thinking about the area of financial institutions and the vulnerability there with respect to the changes they are looking at to protect our financial systems so that we do not get into a situation that obviously could happen if they do not do what the government is doing. I notice the government says they are

M. Forster : Je crois que le plus grand défi pour nous tous dans le cyberespace est de maintenir nos compétences et nos capacités à jour et d'investir dans la technologie dont nous avons besoin pour garder l'avance sur ceux qui veulent infiltrer nos systèmes gouvernementaux. C'est ce que nous nous efforçons de faire de manière constante.

Il faut aussi comprendre qu'il ne s'agit pas d'un espace statique. Ce qu'on voit aujourd'hui aurait été impensable il y a cinq ans. Les capacités sont de plus en plus poussées. La technologie aussi. Il faut constamment améliorer et actualiser ses capacités et ses technologies pour continuer de tenir le haut du pavé.

Le sénateur Dallaire : Vous recueillez des renseignements et les communiquez aux agences canadiennes afin qu'elles prennent des mesures. À titre indicatif, combien de militaires travaillent actuellement au CSTC, environ?

M. Forster : Le brigadier-général Mazzolin vient de dire qu'il y a environ 28 militaires qui travaillent au CSTC. Nous collaborons étroitement avec le CORFC, entre autres.

Le sénateur Dallaire : Vous menez toujours vos activités aux termes de la Loi sur la défense nationale, est-ce exact?

M. Forster : Oui.

Le sénateur Dallaire : Pourquoi n'êtes-vous pas assujetti à la Loi sur le Service canadien du renseignement de sécurité, en tant que division — si vous permettez que j'utilise ce terme — du SCRS au lieu du ministère de la Défense nationale?

M. Forster : Le gouvernement a décidé que nous ne serions pas une division du ministère de la Défense nationale, mais bien une agence indépendante, un peu comme le SCRS. Notre mandat est distinct et nous avons des partenariats, avant tout avec l'armée, mais aussi avec d'autres ministères.

Le sénateur Dallaire : C'est parce que la guerre dans le cyberespace touche de plus en plus d'aspects différents; c'est la guerre totale. Sentez-vous que vos capacités sont limitées ou que vous couvrez tout l'éventail de menaces possibles contre un pays?

M. Forster : Nous ne sommes pas une agence militaire; nous sommes une agence de renseignement. Nous collaborons avec le brigadier-général Mazzolin et le brigadier-général Loos et nous les appuyons dans leur examen des capacités militaires dans le cyberespace. Est-ce que je me sens limité par le fait d'être inclus dans le portefeuille de la Défense? Pas du tout.

Le sénateur Lang : J'aimerais laisser de côté le ministère de la Défense et aborder la question de la responsabilité envers le secteur privé et de ses responsabilités à l'égard des technologies qu'il utilise. Quel est le rôle de ces organisations? Je pense principalement aux institutions financières et à leur vulnérabilité relativement aux changements qu'elles doivent apporter pour protéger nos systèmes financiers, pour éviter une situation qui pourrait facilement se produire si elles ne prennent pas les mêmes mesures que le gouvernement. Le gouvernement intègre et réduit

consolidating, cutting back on data systems and on the overlapping of computer networks. Are these recommendations being put forward in the private sector as well? Are you involved in that?

Mr. Forster: I will ask Ms. Moffa to speak to that. Again, we work through Public Safety, and there is a committee in the financial services industry that they work with to provide that information. Ms. Moffa could maybe talk a bit about that.

The consolidation of systems under Shared Services Canada is actually making our lives and jobs a whole lot easier and better.

Senator Lang: As well as less vulnerable.

Mr. Forster: Yes. I will steal Ms. Moffa's analogy, so I will give her credit for it up front. Which is easier to protect, a house with six windows in it, or 60 houses, some with bars and some without, some with locks and some without? It will be easier for us. When we see something and we need to move quickly to protect systems, we can deal with Shared Services. It covers 45 departments, so it is an efficient and effective means of securing our systems.

Ms. Moffa: As far as the private sector goes, certainly we share with them. Through Public Safety, we share cyber-threat information with them so they can be as informed as we are. We may have some unique information in that regard so that they can better protect themselves. Hopefully that will influence their decisions over how they implement security in their own systems.

Also, all the advice and guidance we provide government on IT security in general is available on our website as well. We have extensive guides and technical standards out there that are available for all to use.

Senator Lang: I just want to go into one other area, and that is the provinces. Are the provinces able to buy into the federal system, with your IT system, and consolidate what they have with respect to basically the direction you are going in the federal government?

Mr. Forster: Obviously they manage their own systems, and, again, Public Safety has that responsibility to work with them. I know a number of provinces are moving in that direction. It is something everybody is doing, not only to lower costs but also to make your systems more efficient. One of the benefits of it is that it will make our job that much easier.

The Chair: Thank you. We did hear testimony on a lot of that last week.

Thank you again to John Forster, Chief, Communications Security Establishment Canada, and to Toni Moffa, Deputy Chief, IT Security.

ses systèmes de données et les chevauchements de réseaux. Est-ce que le secteur privé applique aussi ces recommandations? Prenez-vous part à ces activités?

M. Forster : Je vais laisser Mme Moffa répondre. Je répète que nous collaborons avec le ministère de la Sécurité publique. Il y a un comité au sein du secteur des services financiers qui travaille avec le ministère pour fournir cette information. Mme Moffa pourra vous en dire plus à ce sujet.

L'intégration des systèmes à Services partagés Canada facilite énormément notre travail.

Le sénateur Lang : Et nous rend moins vulnérables.

M. Forster : Exactement. Je vais reprendre l'analogie de Mme Moffa, alors c'est à elle que le crédit revient. Qu'est-ce qui est le plus facile à protéger : une maison à six fenêtres, ou 60 maisons, certaines avec des barreaux et d'autres sans, et certaines avec des portes verrouillées et d'autres sans? C'est plus facile pour nous. Lorsque nous détectons quelque chose et que nous devons intervenir rapidement pour protéger des systèmes, nous pouvons traiter avec Services partagés, qui couvrent 45 ministères. C'est une façon efficace et efficiente de protéger nos systèmes.

Mme Moffa : Nous communiquons avec le secteur privé, c'est sûr. Par l'entremise de la Sécurité publique, nous partageons avec les organisations du privé les renseignements sur les cybermenaces afin qu'elles soient aussi bien informées que nous. Nous pouvons détenir certains renseignements particuliers qui leur permettent de mieux se protéger. Il est à souhaiter que cela aura une incidence sur leurs décisions relatives à la sécurité de leurs propres systèmes.

De plus, tous les conseils que nous fournissons au gouvernement en matière de TI en général se trouvent sur notre site Web. On y trouve des guides exhaustifs et des normes techniques que tous peuvent utiliser.

Le sénateur Lang : J'aimerais aborder la question des provinces. Les gouvernements provinciaux peuvent-ils s'intégrer au système fédéral — votre système de TI — et intégrer leurs systèmes pour suivre la direction prise par le fédéral?

M. Forster : Évidemment, les provinces gèrent leurs propres systèmes. Sécurité publique a la responsabilité de travailler avec elles. Je sais que certaines provinces s'en vont dans cette direction. Tout le monde suit cette tendance, non seulement pour réduire les coûts, mais aussi pour rendre les systèmes plus efficaces. L'avantage pour nous, c'est que cela nous facilite la tâche.

La présidente : Merci. Nous avons entendu des témoignages qui portaient là-dessus la semaine dernière.

Je remercie encore une fois John Forster, chef, Centre de la sécurité des télécommunications Canada, et Toni Moffa, chef adjointe, Sécurité des TI.

That brings an end to our session today here at the Standing Senate Committee on National Security and Defence. We will see you all again next week.

(The committee adjourned.)

OTTAWA, Monday, November 19, 2012

The Standing Senate Committee on National Security and Defence met this day at 4:02 p.m. to examine and report on Canada's national security and defence policies, practices, circumstances and capabilities.

Senator Pamela Wallin (*Chair*) in the chair.

[*English*]

The Chair: This is the meeting of the Standing Senate Committee on National Security and Defence. If I could beg for the indulgence of our guests for a moment, we have a quick minute of business for the committee.

As we all know, we have a new order of reference that has come from the Senate. We also have a very full agenda over the next coming weeks. We will begin the process of collecting all the information we need to try to build a work plan around this ASAP. We need advice on procedure and law and rules of engagement for us and witnesses. We need timelines on internal and external reports that are under way, government legislation and timelines on that, travel and discussions with Internal. We will be doing that research in the near future. We are starting on that process. We will then bring that information to the steering committee, where we will discuss it and come up with a work plan. Then we will make sure that everyone on the committee is fully briefed on not only what the work plan is but also what the rules of engagement will be when we have matters that are of procedural and legal interest. I assure members that we are on the case.

Thank you. We appreciate your giving us a minute to do that business.

Senator Dallaire: Let me intervene at this point to indicate that I have also been spending some time working on this and will be putting together a proposal of study that I hope will be helpful to us all in bringing this together.

The Chair: Thanks. I look forward to that.

The week before last, we focused our attention at this committee on cyberspace and learned in that testimony that it is really now a Canadian military domain, joining land, sea, and air. Today we will look at another realm where our military operates: space, outer space or that place where cyberspace actually works. It is above the earth, above the atmosphere. Joining us are Brigadier-General Pitre, Director General Space, and Colonel André Dupuis, Director of Space Requirements. Welcome to you both. I gather you have opening remarks.

Voilà qui met fin à la séance d'aujourd'hui du Comité sénatorial permanent de la sécurité nationale et de la défense. À la semaine prochaine tout le monde.

(La séance est levée.)

OTTAWA, le lundi 19 novembre 2012

Le Comité sénatorial permanent de la sécurité nationale et de la défense se réunit aujourd'hui, à 16 h 2, pour examiner, en vue d'en faire rapport, les politiques, les pratiques, les circonstances et les capacités du Canada en matière de sécurité nationale et de défense.

Le sénateur Pamela Wallin (*présidente*) occupe le fauteuil.

[*Traduction*]

La présidente : Nous entamons une séance du Comité sénatorial permanent de la sécurité nationale et de la défense. Je prie les témoins d'être indulgents pendant un moment, car nous devons discuter brièvement des travaux du comité.

Comme nous le savons tous, nous avons reçu un nouvel ordre de renvoi du Sénat. Notre emploi du temps sera également très chargé au cours des prochaines semaines. Nous allons amorcer la collecte de toutes les informations dont nous avons besoin pour élaborer un plan de travail dès que possible. Nous devons demander conseil quant à la procédure, à la loi et aux obligations de notre comité et des témoins. Nous avons besoin d'échéanciers pour les rapports internes et externes en cours de production, pour les projets de loi du gouvernement et pour les voyages et les discussions concernant la régie interne. Nous allons bientôt effectuer cette recherche, et le processus s'amorce. Nous fournirons ensuite l'information au comité de direction, où nous en discuterons et établirons un plan de travail. Nous allons veiller à ce que tous les membres du comité connaissent en profondeur ce plan et le mandat concernant les questions de procédure et les questions juridiques. Je vous assure que nous travaillons là-dessus.

Merci de nous avoir accordé une minute pour nos travaux.

Le sénateur Dallaire : Permettez-moi d'indiquer que je consacre aussi du temps à la question et que nous allons proposer une étude qui nous aidera tous, je l'espère, à aller de l'avant.

La présidente : Merci, j'ai hâte d'examiner la question.

Il y a deux semaines, nous avons examiné le cyberespace. Les témoignages nous ont appris que c'est maintenant un domaine militaire qui combine les forces terrestres, navales et aériennes du Canada. Aujourd'hui, nous allons examiner un autre domaine militaire, l'espace, l'espace orbital ou le milieu où le cyberespace prend forme. C'est au-dessus de la Terre et de l'atmosphère. Nous accueillons le brigadier-général Pitre, directeur général Espace et le colonel André Dupuis, directeur du développement de l'espace. Bienvenue à vous deux. Je crois que vous allez présenter des exposés.

Brigadier-General Rick Pitre, Director General Space, National Defence: Thank You. Good evening. My name is Brigadier-General Rick Pitre and I am the Director General Space at National Defence Headquarters. Joining me is Colonel André Dupuis, who is responsible for the planning and acquisition of space systems for the Canadian Forces.

My role is to develop the space-enabled capabilities that have become critical enablers for the operational success of our men and women in uniform.

[*Translation*]

I am very pleased to have this opportunity to provide you some sense of just how important space support is to CF operations.

[*English*]

My organization works in conjunction with the Canadian Space Agency, other government departments and key allies to deliver agile, effective and affordable space support to our military.

I would like to start by setting the broader context of the critical but sometimes unrecognizable role that space-based systems play in a modern society as a whole. You probably would not be surprised that space capabilities today are woven into the very fabric of Canadian society. When you think of environmental monitoring, national resource management, disaster assistance, mitigation, the Internet, telephone systems, search and rescue, GPS navigation, weather forecasting, these are all areas where space systems have dramatically improved our lives and our business.

In the military as well, space is now an indispensible part of how we do business. Space-enabled systems provide intelligence, surveillance, reconnaissance, communications, timing and navigation information.

[*Translation*]

All of that would be difficult and sometimes impossible to obtain through other means.

[*English*]

In some instances, it is very difficult to get into other areas. The pervasive nature of space in both the civilian and military worlds gives our department a unique opportunity. We are able to work with a variety of partners to take advantage of systems that provide useful civil and military capabilities, so-called dual-use systems. These systems allow our forces to access space in a flexible and cost-effective way. I coin this: Smart defence is practical defence.

Brigadier-général Rick Pitre, directeur général Espace, Défense nationale : Merci, bonsoir. Je suis le brigadier-général Rick Pitre, directeur général Espace au quartier général de la Défense nationale. Je suis accompagné du colonel André Dupuis, qui est chargé de planifier l'acquisition des systèmes spatiaux pour les Forces canadiennes.

Mon rôle consiste à mettre au point les capacités spatiales qui sont devenues des atouts essentiels à la réussite opérationnelle de nos militaires, hommes et femmes.

[*Français*]

Je suis ravi de vous présenter un aperçu de l'importance du soutien que l'espace donne aux Forces canadiennes.

[*Traduction*]

Mon organisation collabore avec l'Agence spatiale canadienne, d'autres ministères de l'État et des alliés clés pour fournir à nos forces armées, à un prix abordable, un soutien sous la forme de systèmes spatiaux agiles et efficaces.

J'aimerais tout d'abord décrire le grand contexte où les systèmes spatiaux jouent un rôle déterminant, mais parfois peu reconnu, dans l'ensemble de la société moderne. Vous ne vous étonnerez sans doute pas d'apprendre que les capacités spatiales font aujourd'hui partie intégrante de la société canadienne. La surveillance de l'environnement, la gestion des ressources naturelles, l'aide en cas de catastrophe et l'atténuation des dégâts, Internet et les réseaux téléphoniques, la recherche et sauvetage, la navigation par GPS, les prévisions météorologiques, voilà autant de domaines où les systèmes spatiaux ont considérablement amélioré nos interventions et nos activités.

Par ailleurs, l'espace est aussi un atout indispensable des forces armées, dans la conduite de leurs activités. Les systèmes spatiaux aident les réseaux de renseignement et contribuent aux services de surveillance, de reconnaissance, de communication, de synchronisation et d'information pour la navigation, autant d'éléments qu'il serait difficile, voire parfois impossible, d'obtenir par d'autres moyens.

[*Français*]

Tout cela serait difficile et parfois même impossible à obtenir par d'autres moyens.

[*Traduction*]

C'est parfois très difficile de s'occuper autrement de ces questions. La nature omniprésente de l'espace dans les mondes civil et militaire procure des ouvertures sans pareilles à notre ministère. Nous pouvons travailler avec toute une gamme de partenaires pour profiter de systèmes qui offrent d'utiles ressources civiles et militaires. Ce sont les systèmes dits ambivalents. Ils permettent à nos forces d'accéder à l'espace avec souplesse et d'une façon rentable. Une défense judicieuse est une défense pragmatique.

National Defence is also partnering with our closest military allies, including the U.S., to leverage other unique and important space capabilities.

[*Translation*]

For example, with a relatively small investment, we recently joined the U.S.-led Wideband Global SATCOM program.

[*English*]

We gained immediate access to a worldwide, multi-billion-dollar military communications capability that frankly cannot be matched in any other way. However, there is a flip side to the ever-growing and successful use of space throughout the modern world, and that is that the clamour for access to space-enabled services may in fact endanger our assurance to that access. I will explain that in a moment.

The cliché among space professionals is that space has become congested, competitive and contested.

[*Translation*]

The cliché is true.

[*English*]

There has already been an accidental collision between two satellites in orbit, Iridium 33 and Cosmos 2251, in February 2009. China tested an anti-satellite weapon and successfully destroyed one of its own satellites in January 2007.

As society at large, including the Canadian Forces, makes ever-more effective use of space-enabled capabilities, we must also be increasingly proactive to ensure those capabilities are available when and where we need them.

Having given you some context about the nature of space in our modern world, I would like to discuss some of our specific defence space initiatives. These initiatives directly support the Canada First Defence Strategy mandates, and of course those are to deliver excellence at home, to be a strong and reliable partner in the defence of North America, and to project leadership abroad.

[*Translation*]

In the communications realm, we are proud to have recently secured access to several new strategic communication capabilities.

[*English*]

For instance, the Protected Military Satellite Communication program delivers access to the United States MILSATCOM Advanced Extremely High Frequency, or AEHF, program. This is a targeted and prudent investment that fills our needs for a

Par ailleurs, la Défense nationale s'associe à ses plus proches alliés militaires, y compris les États-Unis, pour tirer profit d'autres capacités spatiales importantes et uniques en leur genre.

[*Français*]

Par exemple, avec un investissement relativement minime, nous avons rejoint récemment le programme américain Wideband Global SATCOM.

[*Traduction*]

Du coup, nous avons acquis un accès à un système mondial de communications militaires de plusieurs milliards de dollars qui n'a tout simplement pas d'équivalent dans le monde. Cependant, il y a une contrepartie à l'utilisation grandissante et fructueuse de l'espace dans le monde moderne. Le désir d'accéder aux services axés sur l'espace risque en fait de mettre en péril cet accès même. Je vais fournir une explication dans un moment.

Les professionnels de l'espace ont adopté un cliché selon lequel l'espace est devenu un environnement encombré et contesté où la concurrence est vive.

[*Français*]

La maxime est donc bien réelle.

[*Traduction*]

Une collision accidentelle s'est déjà produite entre deux satellites en orbite, soit l'Iridium 33 et le Cosmos 2251, en février 2009. La Chine a mis à l'essai une arme antisatellitaire et a réussi à détruire un de ses propres engins spatiaux en janvier 2007.

À une époque où la société dans son ensemble, y compris les Forces canadiennes, utilise toujours plus efficacement les capacités spatiales, nous devons aussi nous soucier de plus en plus de faire en sorte que ces capacités soient accessibles quand et où nous en avons besoin.

Maintenant que je vous ai donné une idée de la nature de l'espace dans notre monde moderne, j'aimerais vous parler de certaines des initiatives de défense dans l'espace. Celles-ci vont directement dans le sens des mandats décrits dans la stratégie de défense Le Canada d'abord. Il faut bien sûr tendre à l'excellence au pays, être un partenaire fort et fiable aux fins de la défense de l'Amérique du Nord et projeter le leadership canadien à l'étranger.

[*Français*]

Dans le domaine des communications, nous sommes fiers d'avoir eu un accès sécurisé à plusieurs des nouvelles capacités de communications stratégiques.

[*Traduction*]

Par exemple, le programme de télécommunications militaires protégées par satellite nous donne accès au programme américain de communications militaires évoluées par satellite MILSATCOM dans la bande de fréquences extrêmement hautes EHF. C'est là un

survivable anti-jam communications capability. It also ensures our interoperability with our closest allies and allows Canada to leverage the entire AEHF system.

The military's "big pipe" broadband needs — we use broadband as well — are also growing. This is driven both by the increased capability of modern sensors and by the increased demand for reach-back on deployed and domestic operations. For example, providing our deployed personnel with access to modern, Internet-based services enables them to connect with their families while in theatre. There is no bigger boost for the morale and performance with this capability.

[*Translation*]

The Canadian Arctic is a national priority.

[*English*]

It is very much a priority, and satellite communications are increasingly connecting the Arctic with the South for both military and civilian users. The temporary outage of the Anik F2 communications satellite in October of last year was in fact a vivid demonstration of the importance of space-based systems to Northern Canada.

However, typical communications satellites cannot provide coverage at extreme northern latitudes. We need innovative and affordable solutions that balance the type of capabilities that SATCOM — satellite communications — offer with other practical solutions.

One promising option is the PCW, the Polar Communications and Weather project, being led by our friends in the Canadian Space Agency. That proposal calls for two satellites to be placed in special orbits that can cover all of Canada's northern territory. Commercial companies are also bringing forward some interesting options to address these requirements, and we are closely monitoring developments in these areas.

In addition to communication, earth observation is also enabled by space. As a three-ocean nation with the longest coastline in the world, Canada needs wide-area surveillance advantages to exercise its sovereignty and custodial responsibilities.

Canada's RADARSAT-1 and RADARSAT-2 systems have been tremendous workhorses in this area. They have mapped the entire globe. They provide critical environmental monitoring as well. We are continuing to invest in maximizing the potential of Canada's space-based radar.

Polar Epsilon is our defence program that allows for the more efficient and timely exploitation of RADARSAT-2 data by our military. Frankly, it has been a huge success in building our maritime picture.

investissement ciblé et judicieux qui répond à un de nos besoins en nous donnant accès à un système serviable de communications antibrouillage. Il nous garantit aussi l'interopérabilité avec nos plus proches alliés et permet au Canada de mettre à profit tout le réseau évolué à EHF.

Les besoins des forces armées dans le domaine des « gros canaux » à large bande augmentent eux aussi. Cela s'explique par la capacité accrue des détecteurs modernes et par la demande plus grande de liaisons avec l'arrière dans le cadre des opérations de déploiement et menées au Canada. Par exemple, en fournissant à nos militaires en déploiement un accès à des services Internet modernes, nous leur permettons de communiquer avec leur famille pendant qu'ils sont dans le théâtre. Rien ne saurait mieux renforcer le moral et le rendement des troupes.

[*Français*]

L'Arctique canadien est une priorité nationale.

[*Traduction*]

C'est très certainement une priorité. Les communications par satellite relient de plus en plus l'Arctique au Sud, pour les usagers tant militaires que civils. La panne temporaire du satellite de communication Anik F2, en octobre 2011, a montré on ne peut plus clairement l'importance que les systèmes spatiaux revêtent pour le Nord canadien.

Cependant, les satellites de communications typiques ne peuvent assurer le service à des latitudes très septentrionales. Il nous faut des solutions novatrices de prix abordable qui permettront de trouver un juste milieu entre les capacités inhérentes aux communications par satellite et d'autres moyens pratiques.

Une option prometteuse réside dans le projet des satellites de télécommunications et de météorologie sur orbite polaire PCW, dirigé par nos collègues de l'Agence spatiale canadienne. Deux satellites seraient placés sur des orbites spéciales qui leur permettraient de balayer tout le Nord canadien. Des entreprises ont aussi formulé d'intéressantes propositions pour répondre à ce besoin. Nous suivons de près tous les faits nouveaux dans ce domaine.

Outre que l'espace favorise les communications, il est aussi utile pour l'observation de la Terre. Comme trois océans baignent le Canada, qui possède le plus long littoral du monde, il lui faut pouvoir surveiller des zones étendues pour exercer sa souveraineté et protéger son territoire.

Les systèmes canadiens RADARSAT 1 et 2 ont été de formidables bêtes de somme dans ce domaine. Ils ont dressé la carte du globe et ils assurent un service essentiel en surveillant l'environnement. Par ailleurs, nous continuons d'investir pour maximiser le potentiel du radar spatial canadien.

Notre programme de défense Polar Epsilon favorise une exploitation plus efficace et rapide des données fournies par RADARSAT 2 par nos forces armées. Et pour tout dire, il a énormément contribué à la définition globale de notre situation maritime.

The RADARSAT Constellation Mission, a Canadian Space Agency-led program, will provide Canada with its third generation of space-based radar. We are working with the space agency to add ship Automatic Identification System, or AIS, receive capability to the RADARSAT Constellation satellites. This has the potential to provide a game-changing improvement in our strategic awareness of Canada's ocean approaches.

We have also seen huge leaps in other earth observation capabilities, from the days when the highest-quality earth observation data could be found only in the most classified military systems. Today we can get excellent imagery from a variety of commercial satellite services.

As I mentioned earlier, space is a congested, contested and competitive environment. We need to be aware of what is happening in space.

The U.S. Space Surveillance Network catalogues and tracks more than 22,000 man-made objects in space, all of them a potential threat. Canada has a stake in this game as well, given its reliance on space and therefore the need to protect its critical assets and infrastructure.

[*Translation*]

We are now poised to launch our first satellite-based, electro-optical sensor system, with the help and expertise of MacDonald, Dettwiler and Associates, a Canadian company.

[*English*]

Called Sapphire, this satellite demonstrates our commitment to making a meaningful and a functional contribution to the larger, international space surveillance network, as well as meeting our own needs.

Furthermore, Sapphire represents a niche contribution to our closest allies that we leverage for privileged access to a range of critical space information.

Search and rescue is another key part of the Canadian Forces' mandate. Fast response times are critical to saving people in distress. That means we need to locate those people as rapidly as possible. This is where the search and rescue satellite program, known as Cospas-Sarsat, comes in. It is an indispensable capability to quickly locate emergency locator transmitter signals. The year 2012 marks the system's thirtieth year of operation, and estimates suggest that it has saved some 31,000 lives.

It will get better with the next generation of search and rescue repeaters poised to launch on the U.S. GPS constellation.

Positioning, navigation and timing, known as PNT, is the last key space system I will mention. I noted earlier that the Canadian Forces operations have come to depend heavily on precise

La mission de la Constellation RADARSAT, programme dirigé par l'ASC, procurera au Canada des radars spatiaux de la troisième génération. Le MDN collabore avec l'agence pour ajouter aux satellites de la constellation une capacité de réception des signaux envoyés par les navires par le Système d'identification automatique SIA. Cela pourrait changer les règles du jeu en ce qui concerne notre connaissance stratégique des approches océaniques du Canada.

Des progrès énormes ont aussi caractérisé l'évolution d'autres systèmes d'observation de la Terre depuis l'époque où seuls les systèmes militaires les plus secrets pouvaient fournir des données de la plus haute qualité. Aujourd'hui, divers satellites commerciaux nous transmettent des images d'une excellente qualité.

Comme je l'ai mentionné plus tôt, l'espace est un environnement encombré et contesté où la concurrence est vive. Nous devons être conscients de ce qui se passe dans l'espace.

Le Réseau américain de surveillance de l'espace catalogue et suit plus de 22 000 objets artificiels dans l'espace; ils représentent tous une menace. Le Canada s'intéresse lui aussi à cet aspect, car il mise beaucoup sur l'espace. Par conséquent, il doit y protéger ses ressources et son infrastructure essentielles.

[*Français*]

Nous sommes maintenant prêts à lancer notre premier satellite équipé d'un système de détection électro-optique avec l'assistance et la compétence de MacDonald, Dettwiler et associés, une compagnie canadienne.

[*Traduction*]

Ce satellite, appelé Sapphire, atteste notre volonté d'apporter une contribution significative et fonctionnelle au grand réseau international de surveillance de l'espace, tout en répondant à nos propres besoins.

En outre, le Sapphire représente une contribution spéciale que nous apportons à nos plus proches alliés et que nous faisons valoir pour obtenir un accès privilégié à toute une gamme de renseignements vitaux sur l'espace.

La recherche et sauvetage constitue un autre volet clé du mandat des FC. Il est vital de réagir rapidement pour sauver des personnes en détresse. Cela signifie qu'il faut les repérer le plus vite possible. C'est dans ce contexte que le programme des satellites de recherche et sauvetage appelé Cospas-Sarsat entre en jeu. Il s'agit d'une capacité indispensable pour repérer rapidement les signaux des radiobalises de repérage d'urgence. Le système fonctionne maintenant depuis 30 ans et, d'après les estimations, il aurait sauvé environ 31 000 vies humaines.

Les résultats s'amélioreront encore plus avec le lancement des répéteurs SAR de la prochaine génération qui sont sur le point d'être placés sur la constellation des systèmes GPS américains.

Les systèmes de positionnement, de navigation et de synchronisation PNT sont les derniers engins spatiaux clés que je mentionnerai. J'ai précisé plus tôt que les opérations des Forces

navigation and timing services from satellites like the Global Positioning System, or GPS, but those services have their vulnerabilities. The GPS signal, like any other signal, is easily prone to interference, accidental or otherwise. Access to GPS is not assured.

[*Translation*]

And so, with our allies, we continue to look at ways to protect this vital service.

[*English*]

Our efforts are focused on identifying emerging threats, developing smart tactics, techniques and procedures to deal with GPS-denied environments, and supporting the research and development of new GPS-related technologies.

Finally, we are now taking the step of standing up the Canadian Space Operations Cell, or CANSpOC, within the Canadian Forces Joint Operations Command Centre. This cell will deliver the critical space enablers to our forces and our strategic partners within government in close cooperation with our allies around the world.

Allow me to offer the simple proposition that space today is everyone's business. Our success in the military and in society at large depends on our effective use of space. It is incumbent on all of us to protect the space environment.

National Defence is playing an important role in this endeavour, to meet the needs of our men and women in uniform, and thereby supporting the broader goals of Canadian society.

I thank you very much for your time in allowing me to address this committee, and I look forward to answering your questions.

The Chair: Thank you very much. We appreciate that overview. It an issue we have talked about a little bit around the edges, so it is very helpful that you are here.

Do we have or is there such a thing as an international code of conduct for behaviour in space? What context are we in? I know we would have relations with allies, but in general is there such a thing?

Brig.-Gen. Pitre: There is. In fact, under the UN mandate there is a code of conduct. Our ADM policy folks tend to be through DFAIT the leads in that environment. That certainly does exist.

The Chair: This is a pretty difficult place when you think about space in general, but space over the Arctic, for example. I have some other questions we will come back to.

canadiennes dépendent désormais beaucoup des services précis de navigation et de synchronisation fournis par les satellites tels que ceux du système de positionnement mondial, ou GPS. Cependant, ces services sont vulnérables à certains égards. Les signaux GPS, tout comme n'importe quel signal radio, sont facilement perturbés par les interférences accidentelles ou autres. L'accès au GPS n'est pas garanti.

[*Français*]

Avec nos alliés, nous continuons de chercher des moyens de protéger ce service essentiel.

[*Traduction*]

Nos efforts portent surtout sur le repérage des menaces éventuelles, sur l'élaboration de tactiques, de techniques et de procédures judicieuses pour intervenir dans les environnements privés de services GPS et sur le soutien de la R-D. concernant les nouvelles technologies GPS.

Enfin, nous franchissons maintenant l'étape clé consistant à mettre sur pied la Cellule des opérations spatiales canadienne CANSpOC dans le Centre de commandement des opérations interarmées des FC. Cette cellule procurera des atouts spatiaux essentiels à nos forces armées et à nos partenaires stratégiques au sein du gouvernement, en étroite coopération avec nos alliés partout dans le monde.

Permettez-moi donc d'affirmer tout simplement qu'aujourd'hui, l'espace appartient à toute l'humanité. Notre réussite militaire et sociale dépend en grande partie de la mesure dans laquelle nous saurons exploiter l'espace judicieusement. Il nous incombe à tous de protéger cet environnement.

Le ministère de la Défense nationale joue un rôle important dans cette entreprise. Il se soucie de répondre aux besoins de nos hommes et femmes militaires et, ce faisant, d'aider la société canadienne à atteindre ses grands objectifs.

Je remercie le comité de m'avoir donné l'occasion de m'adresser à lui. Je me ferai maintenant un plaisir de répondre à vos questions.

La présidente : Merci beaucoup de cet aperçu. Votre présence est très utile, car nous avions seulement abordé la question.

Y a-t-il un code de conduite international concernant les comportements dans l'espace? Nous avons des relations avec nos alliés, mais quel est le contexte général?

Bgén Pitre : Il y a un code de conduite qui relève de l'ONU. Les politiques gérées par nos SMA sont en général établies par le MAECI, qui est le principal responsable dans ce domaine. Un code de conduite existe.

La présidente : L'espace en général est un milieu très difficile, mais pensons à l'espace au-dessus de l'Arctique. J'ai d'autres questions que nous examinerons plus tard.

We will begin our more formal questioning now with Senator Dallaire, whose son joins him today. He is in the audience looking on. I was teasing the senator that this was bring-a-kid-to-work day, but this is a member of the military, so not much of a kid.

Senator Dallaire: Master Seaman Guy Dallaire is sitting there.

The Chair: Welcome.

Senator Dallaire: In 1980, when I was with the Marines, we were talking about space law. I attended your course in Winnipeg on space. You had a space course of a couple of weeks. You have a space program at RMC, a variant of an undergraduate degree in physics for space.

What is the development concept with regard to both classifications in the officer corps and trades in the NCO corps for building our expertise in that dimension?

To follow on, if I may: I am of the school that believes that cyberwar is the new total war. You are a communications instrument. You are observation and intelligence, command and control, all those things. You are right up there as one of those primary target areas. How are we preparing that capability within the forces?

Brig.-Gen. Pitre: That is an excellent question. In fact, I am the product of your question. Back about a year ago, we actually stood up the Director General of Space. Prior to that, it was the Director of Space Development, and the majority of the focus was on force development in terms of developing capability. While a good portion of our force generation is training, and our employment piece was with the United States, it clearly became recognized in the last few years that we had to do that at home, as well.

For instance, the courses that you talk about in Winnipeg and the courses that we attended in Colorado Springs were primarily to service that 30-some-year arrangement where most of our expertise was to the NORAD arrangement. We certainly recognized that we need to have a much more comprehensive, all-encompassing approach to that.

In addition to developing capability, we needed space-smart people, and we also needed them to be employed in ways that we could understand and certainly put to good use here at home.

With the CJOC, the Commander Joint Operations Centre, we have this summer stood up seven of our space operators that will provide initial support to all of our operations in terms of mission planning, weather support, space weather — all of the things that we need now to do in terms of our awareness and how we execute operations abroad. That is a continuing process.

The intent is to move that to potentially 30 individuals who will look at both employment pieces, the generation piece in terms of the educational aspects of it, both, as you said, at RMC and in Winnipeg. There is a space university course program that we have, as well. It is inculcating that. We need space-smart people.

Le sénateur Dallaire va entamer les questions plus formelles. Son fils fait partie du public dans la salle aujourd'hui. J'ai taquiné le sénateur en lui disant que c'était le jour où on amène un enfant au travail, mais son fils fait partie de l'armée et n'est plus un enfant.

Le sénateur Dallaire : Le matelot-chef Guy Dallaire est assis là.

La présidente : Bienvenue.

Le sénateur Dallaire : En 1980, lorsque je travaillais avec les marines, nous parlions du droit de l'espace. À Winnipeg, j'ai assisté au cours de deux semaines sur l'espace. Le programme spatial du CMRC est une variante du diplôme de premier cycle en physique.

Comment les FC renforcent-elles l'expertise des corps et des métiers de sous-officiers dans ce domaine?

Si vous le permettez, je vais poursuivre. Je suis de ceux qui croient que la cyberguerre est une toute nouvelle forme de guerre. Vous êtes un outil de communication, d'observation, de renseignement, de commandement, de contrôle, et cetera. Vous êtes en première ligne concernant ces grands domaines. Comment préparons-nous les capacités dans les forces?

Bgén Pitre : Excellente question. En fait, je suis le produit de votre question. Il y a environ un an, nous avons créé le poste de directeur général Espace, après celui de directeur du développement de l'espace. L'attention était surtout concentrée sur le renforcement des capacités. Même si une bonne partie de nos efforts concernent la formation et que notre travail se faisait avec les États-Unis, c'est devenu clair ces dernières années que nous devions nous pencher là-dessus au pays aussi.

Par exemple, les cours à Winnipeg dont vous parlez et les cours auxquels nous avons assisté à Colorado Springs visaient essentiellement à satisfaire aux exigences de cette entente d'une trentaine d'années, alors que le gros de notre expertise était affecté au NORAD. Nous avons reconnu qu'il fallait adopter une approche beaucoup plus globale, plus inclusive.

En plus de développer une capacité, nous avions besoin de personnes qui connaissaient bien l'espace, et il fallait aussi qu'elles soient employées à des fins que nous pouvions comprendre et qu'elles soient utilisées à bon escient ici, au Canada.

Avec le COIC, le Centre de commandement des opérations interarmées, nous avons créé, cet été, sept postes de spécialiste de l'espace, qui assureront un soutien initial à toutes nos opérations pour ce qui est de la planification des missions, le soutien en météorologie, la météorologie de l'espace — toutes les choses que nous devons faire maintenant pour être bien au fait et exécuter nos opérations à l'étranger. Ce processus se poursuit.

L'intention est d'avoir 30 personnes qui s'occuperont de l'emploi, de l'aspect générationnel, c'est-à-dire de la formation tant au Collège militaire royal qu'à Winnipeg. Nous offrons également un programme de cours universitaires sur l'espace, qui transmet ces connaissances. Nous avons besoin de personnes qui connaissent bien l'espace.

You are absolutely right in the sense that this is the new world in terms of where we are, with both cyber and space. There is that recognition that we need to focus on that. That was the impetus a few years back for the creation of my position and beginning to look at an all-encompassing approach to the development of this capability.

The Chair: Maybe you could take another second and say how space and cyber as domains — or separate areas — are working together. How do those two interact or work?

Brig.-Gen. Pitre: We are neighbours, side by side. We share an office right beside each other. We were both stood up at the same time. While Brigadier-General Loos was working his area of expertise, I was working mine. In trying to understand where those linkages are, I mentioned the protection of capability. Although I will not speak to, for instance, the cyber aspects of it, because that is more his domain, I understand clearly the linkages between the two and making sure we defend that capability, as well.

It is not only about defending infrastructure at physical points, but it is about defending those links. For instance, it could be an IP, Internet protocol, link or it could very well be GPS signals. There is a whole host of areas.

We were stood up at the same time. I must say, though, from a space perspective, I probably have a bit of an advantage in terms of more time, because I actually had a force development capability in place already. We work closely together, as we should. The linkages are clearly understood.

Senator Lang: I would just like to follow up on that line of questioning and ask about your relationship with the Canadian Space Agency. At the outset, you highlighted the fact that the systems allow us intelligence, surveillance, reconnaissance, communication, timing and navigation information. If I could make a recommendation, perhaps what should be stressed also is that it is very important for the minute-to-minute running of our economy. I think it is very important that Canadians be aware of that, because most Canadians are not when it comes to the Internet or surveillance or any of these other elements.

One area I would like to ask about is going back to your relationship with the Canadian Space Agency. My understanding is that they have the intelligentsia, the scientists and the engineers that are all required to run that organization, and they are hard to come by. Once you get them, you want to keep them there, because once you lose them, where do you find someone to replace them?

Just reading your opening remarks, I see that the Armed Forces will be responsible for what they call Sapphire and taking Sapphire and putting it into space. I do not quite understand how that relates to the Canadian Space Agency. I understand that they have that responsibility, and then the responsibility of maintenance in space,

Vous avez absolument raison de dire que nous vivons dans un nouveau monde, quand on songe au cyberespace et à l'espace. Nous reconnaissons que nous devons nous concentrer là-dessus. C'est ce qui a mené, il y a quelques années, à la création de mon poste et ce qui nous pousse à examiner une approche inclusive pour le développement de cette capacité.

Le président : Vous pourriez peut-être prendre une seconde de plus pour expliquer comment l'espace et le cyberespace, qui sont des domaines ou des secteurs distincts, interagissent. Quels sont leurs liens?

Bgen Pitre : Nous sommes des voisins, et nous travaillons côte à côte. Nous occupons le même local. Les deux bureaux ont été mis sur pied en même temps. Alors que le brigadier-général Loos travaillait dans son domaine de compétence, je travaillais de mon côté. Pour comprendre où se situent nos liens, j'ai mentionné la protection de la capacité. Je ne parlerai pas, par exemple, des aspects qui touchent au cyberespace, parce que cela relève davantage de son domaine, mais je comprends clairement les liens qui existent entre les deux et je m'assure que nous défendons cette capacité également.

Il ne s'agit pas seulement de défendre une infrastructure physique, mais aussi de défendre ces liens. Par exemple, il pourrait s'agir d'un protocole Internet, d'un IP, d'un lien, ou encore de signaux GPS. C'est tout un ensemble de domaines.

Nos bureaux ont été créés en même temps. Je dois dire toutefois, pour ce qui est de l'espace, que j'ai peut-être l'avantage d'avoir plus de temps, parce que j'avais déjà une capacité sur le plan du développement des forces. Nous travaillons en très étroite collaboration, comme il se doit. Les liens sont bien compris.

Le sénateur Lang : J'aimerais poursuivre dans cet ordre d'idée et vous poser des questions sur votre relation avec l'Agence spatiale canadienne. Pour commencer, vous avez souligné que les systèmes aident les réseaux de renseignement et contribuent aux services de surveillance, de reconnaissance, de communication, de synchronisation et d'information pour la navigation. Si je pouvais faire une recommandation, je soulignerais aussi que c'est très important pour la direction de tous les instants de notre économie. Je crois qu'il importe que les Canadiens en soient conscients, parce que la plupart ne le sont pas lorsqu'on parle d'Internet, de surveillance ou de tous ces autres éléments.

J'aimerais revenir à votre relation avec l'Agence spatiale canadienne. Je crois comprendre qu'elle a l'intelligentsia, les scientifiques et les ingénieurs qui sont tous nécessaires à son fonctionnement, et ils sont difficiles à trouver. Lorsque vous les avez, vous voulez les garder, parce que s'ils partent, vous aurez du mal à trouver des remplaçants.

Je lis votre déclaration préliminaire et je vois que les forces armées seront responsables de ce qu'elles appellent Sapphire, qu'elles vont prendre le satellite et le mettre dans l'espace. Je ne comprends pas très bien quel est le lien avec l'Agence spatiale canadienne. Je comprends qu'elles ont cette responsabilité et

if there is maintenance to be done. My concern is the duplication perhaps of service, when perhaps it does not necessarily have to happen. Perhaps you could comment on that.

Brig.-Gen. Pitre: Thank you very much for your question. In terms of the relationship with CSA, and to go back to your first question, space is pervasive. My opening remarks talked about the duality of space. Everything we do needs to consider both the military aspect and the larger aspect. Therefore, you are absolutely right, senator, in terms of the economy and other aspects. There are so many different drivers today that space involves; it touches almost everything. I think there is a much better appreciation today of how widespread it really is.

In terms of our relationship with CSA, we work very closely with CSA on a whole host of areas. CSA has the mandate for policy and procedures. Individual organizations within government departments also have the responsibility for developing capabilities, as well. We try to link those as best we can.

Sapphire is about debris mitigation. While it is a military program, the responsibility to protect space is all of our responsibility. Sapphire addresses that. The relationship works in that we are linked military to military through the Space Surveillance Network.

When I said it was a niche capability, it was a niche capability identified with close collaboration with our U.S. partners. A lot of what we do is very much collaborative, not only with our allies but interdepartmentally. Working with CSA and the other government departments is very important. After all, whether it is a Sapphire that goes up or whether it is any other type of system that we rely on in Canada, it is a system that we need to understand what is happening up in space in terms of the debris that is up there — and as I said, moving at 22,000 miles an hour, you can imagine the effect. In fact, I think over the last year, they needed to move the International Space Station some 15 times because of potential collision. Therefore, being aware clearly is important.

The linkage with us is through the American system. We then link interdepartmentally. Everyone has to take advantage. The stewardship belongs to all of us.

Senator Lang: I will go to one other subject quickly. You refer to the Canadian Arctic as a national priority, and that is an area of concern for me. You go on to talk about the Polar Communications and Weather Project, which I believe in some terminology is called "Polar SAT;" is that correct?

Brig.-Gen. Pitre: PCW.

Senator Lang: In launching this particular satellite, will you be purchasing or contracting a portion of the costs of running it? If so, have you come to a conclusion on that?

qu'elles seront chargées de la maintenance dans l'espace, si cette maintenance doit être effectuée. Je me demande s'il n'y a pas dédoublement de service, alors que ce service n'est peut-être pas nécessaire. Vous voudrez peut-être nous dire ce que vous en pensez.

Bgén Pitre : Merci beaucoup de votre question. Pour ce qui est des relations avec l'ASC, et pour revenir à votre première question, l'espace est omniprésent. J'ai parlé de la dualité de l'espace dans ma déclaration préliminaire. Dans tout ce que nous faisons, nous devons tenir compte de l'aspect militaire et de l'aspect plus global. Par conséquent, vous avez absolument raison, monsieur le sénateur, de parler de l'économie et des autres aspects. L'espace implique tellement de facteurs différents; l'espace touche à peu près tout. Je crois qu'on comprend beaucoup mieux aujourd'hui toute sa portée.

Concernant nos relations avec l'ASC, nous travaillons en très étroite collaboration avec l'ASC dans tout un éventail de domaines. L'ASC a le mandat d'établir des politiques et des procédures. Des organisations au sein des ministères ont aussi la responsabilité de développer des capacités. Nous essayons de les relier de notre mieux.

Sapphire vise à atténuer les effets des débris. Bien qu'il s'agisse d'un programme militaire, la protection de l'espace est la responsabilité de tous. Sapphire permet de nous acquitter de cette responsabilité. Les liens sont établis entre les forces militaires grâce au Space Surveillance Network.

J'ai dit qu'il s'agissait d'une capacité spéciale, et cette capacité spéciale a été définie en étroite collaboration avec nos partenaires américains. Nous travaillons très souvent en très étroite collaboration, non seulement avec nos alliés, mais avec les autres ministères. Le travail effectué avec l'ASC et les autres ministères est très important. Après tout, que ce soit Sapphire ou tout autre type de système sur lequel le Canada dépend, nous devons comprendre ce qui se produit dans l'espace et quels sont les débris qui se trouvent là. Comme je l'ai dit, vous pouvez imaginer les effets d'un objet qui se déplace à 22 000 milles à l'heure. En fait, je crois qu'au cours de la dernière année, on a dû déplacer la Station spatiale internationale une quinzaine de fois pour éviter des collisions possibles. Il est donc important de savoir ces choses.

Le lien avec nous passe par le système américain. Nous établissons ensuite un lien avec les autres ministères. Tout le monde doit en profiter. La gouvernance appartient à nous tous.

Le sénateur Lang : Je vais passer rapidement à un autre sujet. Vous avez dit que l'Arctique canadien est une priorité nationale, et c'est un secteur qui me préoccupe. Vous parlez ensuite du projet des satellites de télécommunications et de météorologie sur orbite polaire, qu'on appelle aussi, je crois, Polar SAT; est-ce exact?

Bgén Pitre : Le PCW.

Le sénateur Lang : En lançant ce satellite particulier, allez-vous acheter ou plutôt attribuer un contrat pour partager les coûts de son exploitation? Le cas échéant, êtes-vous arrivé à une conclusion à ce sujet?

Second, how does that relate to the military from the fact that right now — just for viewers' information — we do not have any weather way up in the Arctic and communications are minimal, if at all? This will bring this into play; now we have a method of surveillance that we did not have before. Subsequently, that should cut down the costs of running the military in terms of regular flights to see if there is anyone in our Arctic.

Brig.-Gen. Pitre: I will pass this to my director of space requirements. He knows the technical aspects.

Colonel André Dupuis, Director of Space Requirements, National Defence: Thank you, senator. Excellent question. The Polar Communications and Weather Satellite is in Phase A, which is the definition phase for a satellite system. As far as cost share for the departments goes, it has not been attributed.

National Defence took the lead on the communication piece. Obviously, Environment Canada had the lead on the weather piece, but we did not at any point in time discuss costs or cost share. It is very much at this point a program that, frankly, is the only way to fill all of the department's requirements, but it is not a funded program within the Canadian Space Agency at this point. I think that is probably the best I can say about PCW right now.

Senator Lang: Regarding my second question, let us assume it becomes a reality. That should then reflect back on the costs of how you do your surveillance at the present time because you will have this communications weather satellite that you did not have before. That subsequently should cut back on those costs. Is that correct?

Col. Dupuis: The interesting thing about PCW is that it provides a service that by and large is not available today. Clearly, it would enable better weather forecasting to allow the smarter planning of, for example, air operations, land operations or when ice passage is possible for maritime operations. It is very much tied to how we use RADARSAT Constellation and RADARSAT-2 because it also provides an idea of ice conditions and so on.

Modern communications today are very difficult in the Arctic. For those of you who have ever spoken on a high frequency radio, it is more like screaming into a box and having it scream back at you. This would bring communications in the High Arctic to the standards that we would enjoy around the world. That does not mean we cannot operate in the High Arctic; it is just that we would operate more efficiently. To quantify that efficiency at this point is difficult to do.

Deuxièmement, quel est le lien avec les forces militaires, compte tenu du fait qu'à l'heure actuelle — pour la gouverne de ceux qui nous regardent —, nous n'avons pas de service de météorologie dans l'Arctique et que les communications sont minimales, sinon inexistantes? Voici ce qui est en jeu; nous avons maintenant une méthode de surveillance que nous n'avions pas auparavant. Par conséquent, le projet devrait permettre de réduire les dépenses militaires puisqu'on ne fera plus de vols réguliers pour voir s'il y a quelqu'un dans notre territoire arctique.

Bgén Pitre : Je vais demander à notre directeur du développement de l'espace de répondre. Il connaît les détails techniques.

Colonel André Dupuis, directeur du développement de l'espace, Défense nationale : Merci, monsieur le sénateur. C'est une excellente question. Le projet des satellites de télécommunications et de météorologie sur orbite polaire est en phase A, soit la phase de définition du système. En ce qui a trait au partage des coûts entre les ministères, la question n'est pas encore réglée.

La Défense nationale est responsable du volet télécommunications, et c'est bien sûr Environnement Canada qui s'occupe du volet météorologie, mais nous n'avons pas encore abordé la question des coûts et du partage des coûts. Honnêtement, c'est le seul programme à l'heure actuelle qui réponde à tous les besoins du ministère, mais il n'est pas financé par l'Agence spatiale canadienne. C'est probablement ainsi que je peux le mieux définir le PCW à l'heure actuelle.

Le sénateur Lang : Pour ce qui est de ma deuxième question, présumons que le projet s'est concrétisé. Cela devrait avoir une incidence sur les coûts liés à la surveillance, puisque vous disposez maintenant d'un outil que vous n'aviez pas auparavant, soit un satellite de télécommunications et de météorologie. Cela devrait réduire les coûts, n'est-ce pas?

Col Dupuis : Ce qu'il est intéressant de noter au sujet du PCW, c'est qu'il s'agit d'un service qui, dans l'ensemble, n'est pas offert à l'heure actuelle. Il permettra bien sûr de faire de meilleures prévisions météorologiques pour mieux planifier, par exemple, les opérations aériennes et terrestres, ou encore pour savoir si un passage est libre de glace pour les opérations maritimes. Son utilisation sera liée à celle de la Constellation RADARSAT et de RADARSAT-2 qui nous procurent aussi des renseignements sur l'état des glaces, et cetera.

Les communications modernes sont très difficiles dans l'Arctique. Si vous avez déjà utilisé une radio HF, vous savez que c'est un peu comme crier dans une boîte et recevoir la réponse sur le même ton. Ce projet permettra aux communications dans l'Extrême-Arctique d'être aussi performantes qu'ailleurs dans le monde. Cela ne veut pas dire que nous ne sommes pas en mesure de fonctionner à l'heure actuelle, mais simplement que nous serons en mesure de le faire de façon plus efficace. Malheureusement, nous ne sommes pas en mesure de quantifier ces gains d'efficacité pour le moment.

Brig.-Gen. Pitre: It is too early to tell right now, but one needs to look at all the capabilities. Colonel Dupuis mentioned HF. There is point-to-point line of sight UHF. As we know, all of the communication satellites we have right now tend to be geostationary. In other words, they orbit around the equator. The problem, which is pure physics and the curvature of the earth, is that as you get further north, you cannot reach those northern climes. Having solutions there in the orbit that do, for instance, what they call a "high dwell time," in other words, a satellite that will go very far up and hang up well over the North Pole, and if you use two of them, about 12 for each satellite, you have 24-hour coverage, those are certainly things we are looking at. CSA has the lead on it. They initiated the study back in 2009. We need to look at this in terms of all the capabilities we have currently and where we are going. We need to do this smartly. We need to look at the requirements, the demand and, certainly, the supply curve in terms of when we introduce these things. Clearly, the focus is on being able to operate.

Once again, to your point about the economy, we are not the only ones who operate up there. A lot of activity is up there in environmental and oil exploration, and for all of those aspects, we need to have a good understanding of what the needs are. PCW is but one initiative that a number of organizations are looking at to try to solve or satisfy their problem.

The Chair: Just to be clear on Senator Lang's point, the funding for that would be through the space agency, not through your section.

Brig.-Gen. Pitre: We do not know. That has to be a proposal that someone would present, and then we would look at it. It is not cheap, so clearly we would not necessarily see a single entity, nor would a single entity be the only one that would want this capability.

The Chair: That is a good point.

Brig.-Gen. Pitre: There are the Americans, other allies and, certainly, government that would like this.

The Chair: That is a good point. Thank you.

[*Translation*]

Senator Nolin: Welcome to our committee. General Pitre, I would like to go back to your very brief answer concerning cyberspace.

I understand that your colleague testified before us, but sometimes things fall between the cracks. And so, I would like to hear a much more detailed reply from you concerning the vulnerabilities of the space systems whose integrity is your responsibility. I would like to know about these weaknesses that could develop because of the cyberspace environment. I

Bgén Pitre : Il est trop tôt pour le dire, mais il faut voir nos capacités dans leur ensemble. Le colonel Dupuis a parlé des communications en bandes HF. Il y a aussi celles à portée optique en bandes UHF de lieu à lieu. Comme on le sait, tous nos satellites de télécommunications à l'heure actuelle sont généralement géostationnaires. En d'autres mots, ils sont en orbite autour de l'équateur. Le problème, qui tient essentiellement à la physique et à la courbure de la terre, est qu'il est difficile ainsi d'atteindre les régions nordiques. Si on peut avoir quelque chose en orbite qui nous procure ce qu'on appelle un « temps de tenue élevé », autrement dit, un satellite déployé très haut au-dessus du pôle Nord, et même deux, ayant chacun une période orbitale de 12 heures, on obtiendrait ainsi une couverture de 24 heures. C'est assurément une solution très intéressante pour nous. L'ASC est responsable du projet. Elle a entamé l'étude en 2009. Il faut examiner cela à la lumière de l'ensemble des capacités que nous avons à l'heure actuelle et déterminer l'orientation que nous voulons prendre. Il faut procéder intelligemment. Il faut tenir compte des exigences, de la demande et, bien sûr, du barème d'offres, et choisir le bon moment pour mettre le tout en place. Ce qui prime, bien évidemment, c'est de pouvoir fonctionner.

Encore une fois, pour revenir à votre question au sujet de l'économie, nous ne sommes pas les seuls à être présents dans le Nord. Il y a beaucoup d'activités, que ce soit du côté de l'environnement ou de l'exploration pétrolière, et il faut, dans tous les cas, bien comprendre les besoins. Le PCW n'est qu'une des initiatives envisagées par différentes organisations pour tenter de régler les problèmes auxquels elles doivent faire face.

La présidente : J'aimerais simplement clarifier le point du sénateur Lang, à savoir que le financement proviendra de l'agence spatiale et non pas de votre section.

Bgén Pitre : Nous ne le savons pas encore. Il faut que quelqu'un présente une proposition, puis nous l'examinerons. Comme il est question de gros sous, de toute évidence, il faudra que plus d'une organisation participe, et il y en aura assurément plus d'une qui souhaitera le faire.

La présidente : C'est un bon point.

Bgén Pitre : Cela intéressera certainement les Américains et d'autres de nos alliés, et assurément le gouvernement.

La présidente : C'est un bon point. Merci.

[*Français*]

Le sénateur Nolin : Je vous souhaite la bienvenue à notre comité. Général Pitre, j'aimerais revenir sur votre très courte réponse à propos de l'environnement cybernétique.

Je comprends que votre collègue a témoigné devant nous, mais nous, on déteste, parce que cela peut tomber entre deux chaises. Alors, j'aimerais réentendre de façon beaucoup plus détaillée votre réponse sur les vulnérabilités des systèmes spatiaux dont l'intégrité est votre responsabilité. Je voudrais savoir quelles sont ces fameuses faiblesses qui pourraient se développer à cause de

understand that that is your colleague's responsibility, but you are responsible for these assets, and that is why I would like to hear your comments.

Brig.-Gen. Pitre: If you do not mind, I will reply in English.

Senator Nolin: Yes, please. I wanted to give you a chance to practise your French.

Brig.-Gen. Pitre: Yes, I know. I will alternate.

Senator Nolin: Please go ahead.

[*English*]

Brig.-Gen. Pitre: There are a number of areas that we would see as vulnerabilities. From a cyber perspective, we are just learning what those potential vulnerabilities are. As I said, if it is an IP protocol, for instance, the point-to-point vulnerabilities where information moves, that can be a real challenge. I do not know whether Colonel Dupuis can add anything, but let me highlight the other vulnerabilities that I see as our challenge.

One is, as I said, the PNT, the GPS signal. It is a very weak signal. Let me give you an example of some of the work we are doing. We are doing GPS jamming work, so we are trying to understand how easy it is to jam the signal. Once again, this goes back to a common question from before, namely, how pervasive space is. For instance, the financial sector, the energy sector and navigation all rely to some extent on a timing signal. When you go to the ATM to pull out money and your card does not work, it could be there is no timing signal and they are not synchronized. That could be accidental or it could be nefarious; in other words, something bad could be happening.

With respect to the ability to build a jammer today, in fact, about eight years ago, it was about $150 at Radio Shack — go build yourself a jammer, get on the Internet, 40,000 pages on how to build a jammer. There are probably half a million to a million pages today, and the price is $40. With a very weak signal, we are concerned with the signal and how one protects that. That is one vulnerability right there.

The other vulnerabilities are the physical kinetic vulnerabilities we have. In other words, without the ability to do debris mitigation and understand what is happening, Sapphire looks between 6,000 kilometres and 40,000 kilometres and does a registration of material moving about space. Without that know-how, that knowledge and that space situational awareness, we have bullets out there that can potentially take out systems that we rely on for a good part of what we do.

It used to be redundancy was good enough. In other words, you had the ability to build two of something. Space is expensive, and, in some cases, you may not have a redundant capability. What you will hear quite often is another "r": resiliency. Resiliency is about

l'environnement cybernétique. Je comprends que votre collègue a cette responsabilité, mais vous, vous avez la responsabilité de ces actifs, voilà pourquoi je veux vous entendre.

Bgén Pitre : Si vous permettez, j'aimerais répondre en anglais.

Le sénateur Nolin : Allez-y. Je voulais vous donner une chance de pratiquer votre français.

Bgén Pitre : Oui, je sais. Je vais alterner.

Le sénateur Nolin : Allez-y.

[*Traduction*]

Bgén Pitre : On peut envisager différentes vulnérabilités. Dans le cyberespace, on commence seulement à prendre conscience des vulnérabilités potentielles. Comme je l'ai dit, dans le cas d'un protocole IP, les vulnérabilités de la liaison point à point lors du transfert de l'information peuvent présenter tout un défi. Je ne sais pas si le colonel Dupuis a quelque chose à ajouter, mais auparavant je vais vous parler des autres vulnérabilités qui présentent un défi pour nous.

J'ai déjà parlé de l'une d'elles, le PNT, le signal GPS. Il s'agit d'un signal très faible. Je vais vous donner un exemple de ce que nous faisons. Nous faisons du brouillage GPS pour essayer de savoir si le signal peut facilement être brouillé. On en revient encore une fois à la notion d'omniprésence de l'espace dont il a été question un peu plus tôt. Les secteurs de la finance, de l'énergie et de la navigation, par exemple, sont tous tributaires dans une certaine mesure du signal de synchronisation. Lorsque vous vous rendez à un guichet automatique pour retirer de l'argent et que votre carte ne fonctionne pas, il se peut que ce soit parce qu'il n'y a pas de signal de synchronisation et qu'ils ne sont pas synchronisés. Il se peut que ce soit accidentel, mais il se peut aussi que ce soit un geste malveillant; en d'autres mots, il se peut que quelque chose de grave soit en train de se passer.

Il y a environ huit ans, un brouilleur coûtait environ 150 $ à Radio Shack. Il y avait peut-être 40 000 pages de documentation sur Internet pour apprendre à en construire un. On en trouve sans doute entre un demi-million et un million de pages aujourd'hui, et le coût n'est plus que de 40 $. Lorsque le signal est très faible, c'est préoccupant, et on se demande comment le protéger. C'est une des vulnérabilités à l'heure actuelle.

Nos autres vulnérabilités sont de nature physique et cinétique. En d'autres mots, il faut pouvoir atténuer les effets des débris et savoir ce qui se passe dans l'espace. Le satellite Sapphire enregistre donc le mouvement des objets qui se déplacent à une altitude variant entre 6 000 et 40 000 kilomètres. Sans ce savoir-faire, sans ces connaissances et sans ces informations sur ce qui se passe dans l'espace, il se pourrait qu'un projectile vienne endommager un des systèmes dont nous avons besoin dans presque toutes nos activités.

À une certaine époque, on pouvait s'en remettre à la redondance. Il suffisait donc de construire les éléments en double. Toutefois, le matériel spatial coûte cher et, dans certains cas, on ne peut pas avoir nécessairement une capacité de

understanding the impact, the vulnerability and the ability to mitigate through either tactics, techniques, procedures or finding different ways and streams to move your information. That is the other area of vulnerability we are looking at.

The third one is cyberspace, which we are just beginning to understand. Let me tell you why that is a concern today. It used to be that space was an exclusive club — very few individuals and organizations were involved. That is not true today. Everyone has access to space. Most who have access to space may do so through an IP network or the ability to go that way. If you have enough money to buy, for instance, commercial satellite imagery or you have computer know-how, there is vulnerability there as well.

That is as much as I can offer on the cyber part of it. I do not know whether Colonel Dupuis has anything to add.

[*Translation*]

Col. Dupuis: I could add that beyond the threats the general has told you about, with respect to cyberspace, there is a real possibility that a country could take control of a satellite for their own purposes.

Senator Nolin: Without physically getting near it, they could take control of it from a distance?

Col. Dupuis: That's correct, they could use remote controls to tell the satellite to change —

Senator Nolin: To change its itinerary.

Col. Dupuis: And so, to protect our satellites, we use encrypted schemas. The level of encryption used for the RCM — Radar Constellation Mission — system is level 1 military encryption.

Senator Nolin: For the benefit of the members of the committee, could you explain what that standard is?

Col. Dupuis: That standard is used for the most sensitive Canadian government communications. Nothing protects our systems better than level 1military encryption.

Most companies use a civilian system, which is generally equivalent to the systems used by the banking sector, and they are very good.

Major efforts are made to allow us to control the link between earth and space. General Loos would say that we must also protect the control centre and the antennas. There is a whole other cyber schema beyond the link between earth and the satellites. So that is important. We have thought of that, but of course there is always room for improvement.

redondance. On entend alors souvent parler d'un autre « r », résilience. Ce qu'on entend par résilience, c'est la capacité de comprendre les répercussions et la vulnérabilité, et d'en atténuer les effets en ayant recours à des tactiques, des techniques ou des procédures pour acheminer l'information. Voilà donc une autre vulnérabilité sur laquelle nous nous penchons.

Le troisième élément, c'est le cyberespace, que nous commençons tout juste à comprendre. Et je vais vous expliquer pourquoi il s'agit d'une source de préoccupation aujourd'hui. Autrefois, l'espace était un club très fermé — très peu de gens et d'organisations en faisaient partie. Ce n'est plus le cas de nos jours. L'espace est un lieu auquel tout le monde a accès. La plupart des gens y ont accès par un réseau IP ou peuvent le faire de cette façon. Même si vous êtes assez riche pour vous procurer, par exemple, l'imagerie satellitaire commerciale ou si vous êtes versé en informatique, vous êtes aussi vulnérable.

Voilà tout ce que je peux vous dire au sujet de l'environnement cybernétique. Je ne sais pas si le colonel Dupuis aimerait ajouter quelque chose.

[*Français*]

Col Dupuis : Je pourrais ajouter qu'au-delà des menaces dont le général nous a parlées, du côté cybernétique, il y a une vraie possibilité qu'un pays pourrait prendre contrôle d'un satellite à leurs fins.

Le sénateur Nolin : Sans physiquement s'en approcher, mais en prenant le contrôle à distance?

Col Dupuis : C'est cela, avec des télécommandes pour dire au satellite de changer...

Le sénateur Nolin : Changer de parcours.

Col Dupuis : Alors, pour protéger nos satellites, on utilise des schémas cryptographiques. Le niveau de cryptographie utilisé pour le système RCM — Radar Constellation Mission —, est le niveau 1 militaire.

Le sénateur Nolin : Pour le bénéfice des membres du comité, pouvez-vous expliquer ce que signifie cette norme?

Col Dupuis : Cette norme est utilisée pour les communications les plus délicates du gouvernement du Canada. Aucun système ne protège nos systèmes mieux qu'un niveau 1 militaire.

Mais la plupart des compagnies utilisent un système civil, mais qui équivaut plus ou moins à ce qui est utilisé dans le secteur bancaire, système qui est très bon.

De très grands efforts sont faits pour être capable de contrôler le lien entre la terre et l'espace. Le général Loos nous dirait qu'il faut aussi protéger le centre de contrôle et les antennes. Il existe un tout autre schéma cybernétique au-delà du lien entre la terre et les satellites. Alors c'est important. On y pense mais il est évident qu'il y a toujours du travail à faire.

[*English*]

Senator Nolin: If I may, I have another question on service providers.

[*Translation*]

Colonel Dupuis, MacDonald, Dettwiler and COM DEV are among the main equipment suppliers.

Col. Dupuis: They are the two biggest ones.

Senator Nolin: Are there any others? I am asking because these two main suppliers have laid off workers. Given your responsibility for purchasing, you are probably in a position to tell us what is going on. Is it that you were unable to give them enough work? Have some projects been delayed? What do the smaller ones do?

Col. Dupuis: This is quite a solid industry on the Canadian side. There are MacDonald, Dettwiler, and COM DEV, but there is also Neptec and some small value-added services suppliers, hundreds of them, who are responsible for several billion dollars annually of Canadian revenue, and almost 50 per cent of that is due to exports.

Senator Nolin: You say that we should not jump to conclusions based on the fact that the two largest companies had to downsize their work force and lay off some workers. You do not think we should conclude that this field has become precarious?

Col. Dupuis: I would not draw that conclusion readily without a more detailed study. This is not my area, it falls under Industry Canada, but it needs to be discussed in detail because it is a complex matter.

Senator Nolin: I am taking comfort in the word "solid" that you used.

[*English*]

Senator Day: General, colonel, I need to go back to the beginning here and have an understanding of the relationship between cyberspace and "space" space. You stopped using the word "space" with "cyber" and divided cyberspace into two pieces here, it sounds like. Can you explain the relationship and how you divide up your work?

Brig.-Gen. Pitre: I can explain certainly what I do, which is easiest for me. As I said, most of my work right now is both in the force development, the project, the capability development, force generation — that is training — and force employment.

From that perspective, we are developing capability, whether it is a Sapphire, whether it is the military project RCM — which is Polar Epsilon — or whether it is joint space support capability that allows us to down link commercial satellite imagery. Those are the areas of focus for me.

[*Traduction*]

Le sénateur Nolin : Si vous me le permettez, j'ai une autre question concernant les fournisseurs d'équipements.

[*Français*]

Colonel Dupuis, parmi les principaux fournisseurs d'équipements figurent MacDonald, Dettwiler et COM DEV.

Col Dupuis : Ce sont les deux plus grands.

Le sénateur Nolin : Est-ce qu'il y en a d'autres? Parce que ces deux principaux fournisseurs ont mis à pied des employés. Dans votre responsabilité au niveau des achats, vous êtes certainement à même de nous dire ce qui se passe finalement. Est-ce que vous ne leur en donnez pas assez? Il y a des projets qui ont été retardés? Que font les plus petits?

Col Dupuis : C'est déjà une industrie qui est assez robuste du côté canadien. Il y a MacDonald, Dettwiler, il y a COM DEV, mais il y a aussi Neptec et des petits fournisseurs de services à valeur ajoutée, qui sont dans les centaines, qui sont responsable de plusieurs milliards par année de revenus canadiens dont presque 50 p. 100 sont en exportation.

Le sénateur Nolin : Vous nous dites qu'il ne faut pas se fier sur le fait que les deux plus gros ont dû rationaliser leurs effectifs et libérer certains employés. On ne doit donc pas en déduire que ce secteur d'activité est fragilisé?

Col Dupuis : Il faudrait faire très attention à une conclusion semblable sans faire une étude plus détaillée. Ce n'est pas mon secteur, c'est Industrie Canada, mais il faudrait en discuter en détail parce que ce n'est pas une question très simple.

Le sénateur Nolin : Je m'accroche au mot « robuste » que vous avez utilisé.

[*Traduction*]

Le sénateur Day : Messieurs, je dois revenir à la base; j'ai besoin de comprendre le lien qui existe entre le cyberespace et l'espace. Vous avez cessé d'apposer « espace » à « cyber », et on dirait que vous avez divisé le cyberespace en deux. Pourriez-vous expliquer ce lien et la façon dont vous divisez votre travail?

Bgén Pitre : Je peux certainement expliquer ce que je fais, et ce sera plus facile pour moi. Comme je l'ai dit, la majeure partie de mon travail porte sur le développement des forces, le projet, l'augmentation des capacités, la mise sur pied des forces, soit l'entraînement, et l'emploi des forces.

Dans cette perspective, nous augmentons nos capacités par l'entremise, par exemple, du satellite Sapphire, du projet militaire de la MCR, à savoir le projet Polar Epsilon, ou du projet de soutien spatial conjoint qui nous permet d'obtenir de l'imagerie satellite commerciale par liaison descendante. Voilà les domaines sur lesquels je mets l'accent.

In terms of the relationship between space and cyberspace, we are still trying to figure that out in terms of the vulnerabilities. For me, it is more about the hard-core capabilities, what we are developing.

Senator Day: You initially talked about the very fabric of Canadian society, environmental monitoring, et cetera. You talked about GPS. Is that in its concentration of what happens and what is going on? There are initiatives in other departments of the government previously such as the Canadian Space Agency, and then the private sector was involved. Is the cyber side of things looking after all these activities?

Brig.-Gen. Pitre: No, that is the space area. For instance, when we talk about earth observation or maritime or global domain awareness, the military side of it is maritime or global domain awareness. Earth observation is the duality, the other side, for instance, that our commercial or private entities would be looking at. Weather forecasting, earth observation, ship detection, pollution detection and communications all fall within the space realm.

When it begins to affect, for instance, point to point, the movement of information through protocols, that is cyberspace. Once again, I am getting into an area that is not my specialty. That is why, in fact, we are neighbours, we live side by side, because we need to clearly understand those vulnerabilities.

We are talking about service-oriented areas, which are my focus.

Senator Day: Space-enabled systems all fall under your and the colonel's domain as areas of activity.

Brig.-Gen. Pitre: That is right.

Senator Day: There are some military applications here and there are some dual or joint, as you described in your introductory remarks.

Brig.-Gen. Pitre: That is right.

Senator Day: You mentioned NORAD, and that is another area I wanted you to talk about. We have had an extremely good relationship with our neighbour to the south, the United States of America, in relation to NORAD and aerospace and air space activity and monitoring and defence. There was some talk at one time of our expanding that role into space, but we objected to arming space, whereas the U.S. did not. Can you talk to me now about that fine distinction of being able to defend potential attacks in space and the offensive activity that could take place?

Brig.-Gen. Pitre: Our policy has always been clear in terms of weaponization. It is the peaceful use of space and the application of that.

If I go back to your question about NORAD, since 1958 we have been involved very closely with our U.S. counterparts on the defensive nature. In other words, the integrated threat warning

En ce qui a trait au lien entre l'espace et le cyberespace, nous en sommes encore à essayer de comprendre les vulnérabilités que cela représente. Dans mon cas, il est davantage question des capacités fondamentales et de ce que nous mettons au point.

Le sénateur Day : Vous avez dit au début que cela faisait partie intégrante de la société canadienne, et vous avez notamment donné l'exemple de la surveillance environnementale. Vous savez parler des services GPS. Est-ce que cela englobe ce qui se passe autour? Il y a eu des initiatives d'autres organismes, dont l'Agence spatiale canadienne, puis le secteur privé est entré dans le marché. Est-ce que le secteur du cyberespace s'occupe de ces activités?

Bgén Pitre : Non. Il s'agit du secteur de l'espace. Par exemple, lorsqu'il est question de l'observation de la Terre ou de la connaissance de l'espace maritime ou mondial, c'est la connaissance de l'espace maritime ou mondial qui a un intérêt sur le plan militaire. L'observation de la Terre, par exemple, est l'aspect dont le secteur privé s'occupe. Les prévisions météorologiques, l'observation de la Terre, la détection des navires, la détection de la pollution et les communications appartiennent toutes au secteur spatial.

Lorsque cela commence à concerner, par exemple, les communications par l'entremise de protocoles point à point, cela concerne le cyberespace. Encore une fois, ce domaine n'est pas ma spécialité. Voilà pourquoi nous sommes en fait voisins; nous vivons côte à côte, parce qu'il faut clairement comprendre les vulnérabilités.

Nous parlons de secteurs axés sur les services, et c'est mon domaine.

Le sénateur Day : Les systèmes spatiaux relèvent de vos domaines d'activité.

Bgén Pitre : C'est exact.

Le sénateur Day : Certains systèmes ont des applications militaires, alors que d'autres ont des applications mixtes ou communes, comme vous l'avez décrit dans votre exposé.

Bgén Pitre : C'est exact.

Le sénateur Day : Vous avez mentionné le NORAD, et c'est un autre élément que je voulais aborder. Nous entretenons une excellente relation avec nos voisins américains au sujet du NORAD, des activités aérospatiales, de la surveillance et de la défense. Des discussions ont déjà eu lieu dans le but d'étendre ce rôle à l'espace, mais nous nous sommes opposés à la militarisation de l'espace, contrairement aux États-Unis. Pourriez-vous nous expliquer la distinction très subtile qui existe entre la capacité de se défendre contre de possibles attaques dans l'espace et les initiatives offensives possibles?

Bgén Pitre : Notre politique a toujours été claire en ce qui a trait au déploiement d'armes. Nous visons une utilisation pacifique de l'espace.

Pour revenir à votre question sur le NORAD, depuis 1958, nous collaborons très étroitement avec nos homologues américains en ce qui a trait à la défense. Autrement dit,

and assessment has always been a role, and today we are still involved in that. We have Canadian personnel involved, certainly posted to missile warning sites in that area. Defending, from that perspective, has been something we have been doing for the last 34 years. From that perspective, defending is clearly within our mandate. The weaponization, however, is clear to us. We are a UN signatory to the Peaceful Uses of Outer Space, so there is a clear delineation from our perspective.

Senator Day: What comes to mind with weaponization is putting a laser on a satellite up there and the laser would then be used for offensive purposes. Learning to defend against jamming, for example, you learn how someone else might do it, but you also learn how to do it. They develop a new system; you develop a new system. We exchange ideas with our partners in that regard so we can develop tactical offensive weaponry in that regard, can we not?

Col. Dupuis: Senator, probably the easiest way to wrap your arms around this particular topic is that there are three ways to attack a satellite system. You can attack the satellite which clearly, based on the Chinese ASAT tests, is not a good idea; it causes debris. We talked about attacking the link, which is the ground station to the satellite. If you cannot talk to the satellite, you cannot get information off the satellite, so then you have negated it without causing debris. We do not want to cause debris. The other piece is you could always intervene on the ground. If you had to take out a satellite dish, for example, to keep the enemy from accessing that satellite, that would also work.

There are plenty of GPS jammers, as the general mentioned. There are plenty of people jamming satellite communications today. When we talk about the militarization or the military use of space as opposed to weaponization, we just have to be careful about what we are talking about. I do not think anyone is running off to put weapons in space. That perhaps is possible, but no one does it today. We are talking about using military effect to prevent the use of space, which is maybe a more refined way of looking at the question.

Senator Day: I just want it to be clear that you talk defensively but you are learning to act offensively while learning to act defensively.

Brig.-Gen. Pitre: You certainly understand and learn the offensive capabilities, and clearly if you know black you certainly know white. In understanding how to defend, one would need to understand what types of offensive capabilities are out there. Our focus, certainly from the peaceful use of space, allows us the defence of our systems both on the ground and in space.

Senator Day: That rounds out my question. Thank you very much.

l'évaluation et l'avertissement intégrés des menaces ont toujours été un rôle, et nous sommes encore aujourd'hui actifs à cet égard. Du personnel canadien y participe; des Canadiens se trouvent sur place dans les sites d'avertissement de missiles dans ce secteur. Nous nous occupons de la défense depuis 34 ans; dans cette perspective, la défense fait clairement partie de notre mandat. Par contre, notre opinion est claire au sujet du déploiement d'armes. Le Canada est membre du Comité des Nations Unies pour l'utilisation pacifique de l'espace extra-atmosphérique; la limite est clairement définie, selon nous.

Le sénateur Day : Quand nous pensons au déploiement d'armes, nous avons en tête l'installation d'un laser sur un satellite dans l'espace en vue de l'utiliser à des fins offensives. Lorsque vous apprenez à vous défendre contre le brouillage, par exemple, vous apprenez comment un autre pourrait s'y prendre, mais vous apprenez également comment le faire. Ils mettent au point un nouveau système; vous en élaborez un nouveau. Les idées circulent entre nos partenaires à cet égard en vue de pouvoir mettre au point des armes offensives tactiques, n'est-ce pas?

Col Dupuis : Sénateur, pour l'expliquer le plus simplement possible, il y a trois moyens d'attaquer un système satellite. On peut attaquer le satellite, ce qui n'est vraiment pas une bonne idée, d'après les essais d'armes antisatellites de la Chine, parce que cela crée des débris. Nous avons déjà discuté de l'attaque de la station au sol du satellite. S'il est impossible de communiquer avec le satellite, on ne peut pas obtenir de renseignements. L'appareil a donc été mis hors d'usage sans avoir causé de débris. Nous ne voulons pas en causer. Enfin, nous pourrions toujours mener des opérations terrestres. Si nous voulons empêcher un ennemi d'avoir accès au satellite, nous pouvons détruire l'antenne parabolique. Ce serait efficace.

Comme l'a mentionné le général, il y a beaucoup de brouilleurs GPS. Bon nombre de gens brouillent les communications satellites. Lorsque nous parlons de la militarisation ou de l'utilisation militaire de l'espace, par opposition au déploiement d'armes, il faut faire preuve de prudence concernant ce dont il est question. Je ne crois pas qu'un pays soit empressé de déployer des armes dans l'espace. C'est toutefois possible, mais personne ne le fait actuellement. Nous parlons d'utiliser des effets militaires en vue de prévenir l'utilisation de l'espace, ce qui se veut peut-être une façon plus subtile d'aborder la question.

Le sénateur Day : À titre de précision, vos propos portent sur l'aspect défensif, mais vous apprenez des moyens offensifs, tout en apprenant à vous défendre.

Bgén Pitre : Nous comprenons et apprenons évidemment les capacités offensives; si on connaît l'un, on connaît certainement l'autre. Pour comprendre comment se défendre, il faut comprendre les diverses capacités offensives disponibles. L'utilisation pacifique de l'espace nous autorise à assurer la défense de nos systèmes terrestres et spatiaux.

Le sénateur Day : Cela fait le tour de ma question. Merci beaucoup.

Senator Mitchell: Thank you. I would like to pursue this a little bit further. We saw reports of perhaps Chinese elements hacking into Nortel, stealing proprietary information, building whatever it is they would build and compete with, and look at Nortel. If I can use the word "attack," does that fall under what you are doing?

Brig.-Gen. Pitre: Yes.

Senator Mitchell: What is your relationship with those elements of our cyber?

Brig.-Gen. Pitre: My relationship would be directly through, for instance, Director General Cyber. That is my relationship with him. As we build capability, more robust, and understand those vulnerabilities, I link directly through him. You heard from General Loos two weeks ago, and he explained his relationship with those other organizations.

I should say that interdepartmentally we work closely with each other. When we talk about space capabilities and the interests of NRCan or Public Safety or Transport Canada or the Canadian Space Agency, we all share the same interests and concerns. That same question would apply for those organizations that are focused on the cyber threat itself and how we mitigate.

We talk about mitigation in terms of the resiliency part of it. That is an area we would be very interested in.

Senator Mitchell: Thank you. You mentioned in your opening comments that in the past the highest level, the highest quality of earth observatory technology was military and had a high level of confidentiality. Today, you can go out and buy it from companies; it is commercially available. I would like to explore that a little bit.

What are the risks in depending on the commercial sector, the private sector, to deliver those to you? How do you distinguish those risks? How do you deal with them? What kind of budget does that involve? Do you have enough of that budget?

Brig.-Gen. Pitre: I will start and then let Colonel Dupuis talk about some of the other specifics. There are two sides to that coin. What are the risks to what we call classified technical or national technical? The risks are that not everyone has access to it. That can be a challenge. For instance, if you are in a coalition operation where you have plenty of organizations that do not necessarily have the security classification, you cannot share that information with them. For instance, the Joint Space Support Project actually allows us to download commercial satellite imagery right in theatre, within 30 minutes, provide it to the commander and also share it. It is extremely valuable to be able to do that because the information you may need is very pertinent and important.

Le sénateur Mitchell : Merci. J'aimerais explorer un peu plus le sujet. Des rapports sous-entendent que des Chinois auraient piraté Nortel, volé des renseignements exclusifs, créé quelque chose et fait concurrence à Nortel. Si je peux utiliser le mot « attaque », est-ce que cela relève de ce que vous faites?

Bgén Pitre : Oui.

Le sénateur Mitchell : Quelle est votre relation par rapport à ces éléments relativement à la cybersécurité?

Bgén Pitre : Par exemple, je suis en contact direct avec le directeur général de la cybersécurité. C'est le rapport que j'entretiens. À mesure que nous renforçons nos capacités et que nous comprenons les vulnérabilités, je passe directement par lui. Il y a deux semaines, vous avez entendu le témoignage du général Loos; il avait alors expliqué sa relation avec les autres organismes.

Je dirais qu'il y a une étroite collaboration interministérielle. Au sujet des capacités spatiales et des intérêts de RNCan, de Sécurité publique Canada, de Transports Canada ou de l'Agence spatiale canadienne, nous avons tous les mêmes intérêts et les mêmes préoccupations. La même question s'appliquerait dans le cas des organismes qui mettent l'accent sur les cybermenaces et les façons de les atténuer.

Nous parlons d'atténuation en ce qui a trait à la résilience à cet égard. Il s'agit d'un domaine qui nous intéresserait grandement.

Le sénateur Mitchell : Merci. Dans votre exposé, vous avez dit que par le passé les systèmes militaires fournissaient la meilleure qualité de données en ce qui a trait à l'observation de la Terre et qu'ils étaient des plus secrets. Ces données sont maintenant vendues par certaines entreprises; elles sont disponibles sur le marché. J'aimerais explorer un peu cet aspect.

Si nous dépendons du secteur privé pour nous fournir ces données, quels risques y a-t-il? Comment distinguez-vous ces risques? Comment les abordez-vous? Combien cela vous coûte-t-il? Votre budget est-il suffisant?

Bgén Pitre : Je vais répondre en premier, puis laisser le colonel Dupuis entrer dans les détails. Il y a deux aspects. Quels sont les risques au sujet de ce que nous appelons des données techniques classifiées ou des données issues de moyens techniques nationaux? Le problème est que ce n'est pas tout le monde qui y a accès. Cela peut être un défi. Par exemple, dans le cadre d'une opération de coalition dont certains organismes n'ont pas nécessairement la cote de sécurité, nous ne pouvons pas leur communiquer l'information. Par exemple, le projet de soutien spatial conjoint nous permet en fait de télécharger de l'imagerie satellite commerciale sur le terrain en moins de 30 minutes, de faire parvenir les données au commandant, mais aussi de les communiquer aux autres. C'est extrêmement précieux de pouvoir le faire, parce que l'information dont on peut avoir besoin est très pertinente et très importante.

You have two issues. One is the classification of information you get. If it is from national technical means, it may be difficult. Two, we do not own NTM, national technical means, so having access to that requires us to do other things to ensure we do get access to it. That is the national technical side.

With commercial satellite imagery, or CSI, also known as the program but with a different name, the capabilities have improved tremendously over the last decade. They have gotten to the point where they are extremely good. What are the challenges? The challenges clearly are like any other organization: you may not necessarily have access to it. You have to pay for it as well, and there may be potential times when it may not necessarily serve your purposes, your needs, and so it needs to be more specific. This is the comprehensive approach.

What tools and capabilities can we make use of? We go into our toolbox and look at the specific classified systems that may do specific things. What are the unclassified ones that are very good, that will address others, and how do we use this to do the things we need to do? I do not know if Colonel Dupuis can add anything further.

Col. Dupuis: There is not much more to add to that with the exception that the military brings a very good understanding of the process, to analyze, to build a requirement for the imagery, to order the imagery, to exploit the imagery and to disseminate that imagery. We have done that in the classified realm for a very long time. Commercial systems will allow us to do so down to 50 centimetres, very high resolution, using synthetic aperture radar. You can measure differences in heights of millimetres from one dimension to the next. We can bring to that equation the expertise to exploit that information to then pass them on to our mission partners, whether that is in Afghanistan, the Manitoba floods, firefighting, pollution monitoring or a whole host of things that require what we call the TPED process, the intelligence process, and pushing it to the people who need it. They do not compete; they are complementary. Because the commercial folks are selling to a very large audience, it allows the cost to be quite affordable.

The other part of your question was how we control it. We have a law in Canada called the Remote Sensing Space Systems Act, owned by our friends at DFAIT, and all of our allies who have similar systems have a similar law. It says we will tell you who you can and cannot sell imagery to. In an extreme case, you can say "you cannot sell to them." We do not control every satellite system that is up there; however, we can control most of the allied systems and just say *in extremis*, you are not selling to them.

Brig.-Gen. Pitre: We refer to that as shutter control.

Senator Dawson: Because of the time, I will be very brief. One of the partners you did not mention is NAV CANADA. NAV CANADA has responsibility for flight control, and I am speaking

Il y a deux enjeux. Premièrement, il faut tenir compte de la cote des données obtenues. Si elles sont issues de moyens techniques nationaux, ce sera peut-être difficile. Deuxièmement, les moyens techniques nationaux ne nous appartiennent pas. Pour nous assurer d'y avoir accès, il faut donc prendre d'autres mesures. Voilà pour ce qui est des moyens techniques nationaux.

Dans le cas de l'imagerie satellite commerciale, les capacités se sont grandement améliorées au cours de la dernière décennie. Cette imagerie est rendue extrêmement bonne. Quels sont les défis? Les défis sont clairement les mêmes que tout autre organisme : on n'y a pas nécessairement accès. Il faut également payer, et il se peut que ces données ne répondent pas nécessairement à notre utilisation ou à nos besoins. Il faut que ce soit plus précis. C'est une approche globale.

Quels sont les outils ou les capacités qui peuvent nous être utiles? Nous examinons nos systèmes classifiés qui peuvent accomplir des tâches précises. Quels sont les très bons systèmes non classifiés qui peuvent répondre à nos autres besoins? Comment pouvons-nous nous en servir pour accomplir les tâches que nous devons faire? Je ne sais pas si le colonel Dupuis aurait quelque chose à ajouter.

Col Dupuis : Il n'y a pas grand-chose à ajouter, mis à part que l'armée apporte une très bonne compréhension du processus en vue d'analyser, de générer une demande d'imagerie, de la commander, de la traiter et de communiquer les données. Nous le faisons depuis longtemps en ce qui a trait aux systèmes classifiés. Les systèmes commerciaux nous permettront de le faire jusqu'à 50 centimètres avec une très haute résolution grâce à un radar à synthèse d'ouverture. On peut mesurer le relief au millimètre près. Nous pouvons apporter notre expertise en traitant les données pour ensuite les communiquer à nos partenaires en Afghanistan ou au Manitoba pendant des inondations, ou encore pour combattre des incendies ou surveiller la pollution, ou dans toute autre circonstance qui exige un processus TPED, le processus de renseignement, et la communication de données à ceux qui en ont besoin. Ils ne sont pas concurrentiels; ils sont complémentaires. Étant donné que le secteur privé vend ses données à un vaste marché, les coûts sont très abordables.

L'autre partie de votre question portait sur la façon dont le contrôle s'effectue. Au Canada, nous avons la Loi régissant l'exploitation des systèmes de télédétection spatiale, qui est du ressort de nos collègues du MAECI, et tous nos alliés qui disposent de tels systèmes ont une loi similaire. La loi définit ceux à qui l'imagerie peut être vendue. Dans des cas extrêmes, il est possible d'en interdire la vente à certains. Nous n'avons pas de contrôle sur tous les systèmes satellites dans l'espace; par contre, nous pouvons contrôler la majorité des systèmes alliés et nous pouvons dire, dans des cas extrêmes, de ne pas vendre à certains.

Bgén Pitre : Nous appelons cela le contrôle de l'obturateur.

Le sénateur Dawson : En raison du temps qui avance, je serai bref. Parmi les partenaires que vous n'avez pas nommés, il y a NAV CANADA. NAV CANADA s'occupe du contrôle de la circulation

of inner space. Between cyberspace and outer space, there is the other space where flight control is done more and more by satellite. NAV CANADA is a non-profit organization that had to recoup its costs. Along the border, in the major cities or airports, they have revenues to offset their investments. However, when you talk about the North and control of the airspace, landing and taking off in the North, you have not mentioned the relationship between Defence, NAV CANADA and the local needs. How are they concerned? NAV CANADA is very efficient and modern, but it is totally quasi-dependent on cyberspace. They are all doing everything they can either on the Internet or through your satellites. How do they fit into the picture of partnership and development in trying to facilitate sharing of information?

Brig.-Gen. Pitre: NAV CANADA, through Transport Canada, is our vehicle to deal with their particular needs. In my previous job, I had a lot of experience in dealing with NAV CANADA and the Canadian NORAD Region and their requirements. Transport Canada and Public Safety are typically the venues that we would address to address those particular needs that NAV CANADA would have. Aside from that, interdepartmentally, there are other organizations. I am not sure if NAV CANADA sits on the IMSWG. Their voice is typically Transport Canada. However, the Interdepartmental Marine Security Working Group, for instance, is a vehicle that we have, and there are a number of other interdepartmental organizations as well. NAV CANADA, connected directly through Transport Canada, would be the mechanism through which we would see how their needs and requirements are met.

Senator Dawson: I could go on and on, but thank you.

Senator Dallaire: All three services are using space for a variety of reasons. Are they building capacity to maximize that competency in three services? Is all the space capacity in NDHQ in your office, or is there some other headquarters being considered? Do you have liaison officers or maybe defence scientists in the Canadian Space Agency working with them?

Brig.-Gen. Pitre: How we are moving along developing space expertise and ensuring that it is joint has never been better. My responsibility, as the director general space, is to the Chief of Force Development, Ron Lloyd, through the VCS. I can tell you that, over the last year or two, we have been involved, jointly with the army, navy and air force, in every aspect in areas of space enablers, whether it is communications, with Mercury Global or the Wideband Global satellite system linking directly with our navy; whether it is technical narrow band SATCOM looking at communications on the move for both the army and the air force; or whether it is RCM, the RADARSAT Constellation Mission. The navy is a huge player in that in terms of maritime awareness and the game-changing aspects of being able to not only track and identify but also now, when RCM goes up with three satellites, to

aérienne dans l'espace atmosphérique. Entre le cyberespace et l'espace extra-atmosphérique, il y a un autre espace où le contrôle de la circulation aérienne s'effectue de plus en plus grâce aux systèmes satellites. NAV CANADA est un organisme sans but lucratif qui a dû recouvrer ses coûts. Près de la frontière, dans les villes et les aéroports importants, l'organisme a des revenus qui viennent contrebalancer ses investissements. Toutefois, en ce qui concerne le contrôle de la circulation aérienne dans le Nord canadien, des atterrissages et des décollages, vous n'avez pas parlé de la relation entre le ministère de la Défense nationale, NAV CANADA et les besoins locaux. Comment cela concerne-t-il l'organisme? NAV CANADA est très efficace et très moderne, mais il est pratiquement dépendant du cyberespace. Il fait tout ce qu'il peut sur le web ou par l'entremise de vos satellites. Comment cet organisme s'inscrit-il dans le partenariat et le développement en vue d'essayer de faciliter la communication des données?

Bgén Pitre : NAV CANADA, par l'entremise de Transports Canada, est notre moyen pour aborder ses besoins précis. Dans mon précédent poste, j'ai eu souvent eu affaire avec NAV CANADA et la région canadienne du NORAD et leurs exigences. Nous passons normalement par Transports Canada et Sécurité publique Canada pour aborder les besoins particuliers de NAV CANADA. Il y a également des organismes interministériels. Je ne suis pas certain que NAV CANADA siège au GTISM. C'est normalement Transports Canada qui parle au nom de l'organisme. Cependant, le Groupe de travail interministériel sur la sûreté maritime est l'un des véhicules à notre disposition, mais il y a d'autres organismes interministériels. NAV CANADA, qui a un lien direct par l'entremise de Transports Canada, est le mécanisme par lequel nous nous assurons que les exigences et les besoins de l'organisme sont répondus.

Le sénateur Dawson : Je pourrais continuer indéfiniment, mais je vous remercie.

Le sénateur Dallaire : Les trois services utilisent l'espace pour diverses raisons. Sont-ils en train de développer des capacités pour maximiser cette compétence dans trois services? L'ensemble de la capacité spatiale se trouve-t-il dans votre bureau au QGDN, ou d'autres quartiers généraux sont-ils envisagés? Des agents de liaison ou peut-être des scientifiques de la défense établis à l'Agence spatiale canadienne travaillent-ils avec eux?

Bgén Pitre : La façon dont nous développons les compétences spatiales et veillons à leur mixité n'a jamais été meilleure. En tant que directeur général Espace, je rends des comptes au chef — développement des forces, Ron Lloyd, par l'entremise du vice-chef d'état-major. Je peux vous dire qu'au cours des quelques dernières années, nous avons travaillé conjointement avec l'armée, la marine et la Force aérienne, dans tous les domaines qui facilitent l'utilisation de l'espace, qu'il s'agisse de communications, à l'aide de Mercury Global ou du programme des satellites mondiaux de communications à large bande qui sont reliés directement à notre marine, de communications techniques à bande étroite par satellite qui permettent tant à l'Armée et qu'à la Force aérienne de communiquer pendant qu'elles se déplacent, ou de la MCR, la Mission de la Constellation RADARSAT. À cet égard, la Marine

revisit, on a daily basis, our Arctic approaches so that we can actually prosecute and use all of the capabilities that we have out there. We are working with Defence Research and Development Canada, DRDC, on algorithm work that they are doing on the Synthetic Aperture Radar, for which we are leaders in the world. In fact, our U.S. counterparts have their eyes wide open in terms of the things we are doing regarding maritime domain awareness. We are across the board in many areas. To me, this is an exciting time because we understand now. When we talk about the pervasiveness of space and how reliant we are, we are getting it. We really are.

joue un rôle important, en ce qui a trait à la connaissance du domaine maritime et à la capacité non seulement de suivre les déplacements des auteurs d'infractions et de les identifier, mais aussi, lorsque la MCR sera opérationnelle grâce aux trois satellites, de réexaminer quotidiennement les approches que nous avons adoptées dans l'Arctique, afin que nous puissions ainsi poursuivre ces gens et tirer parti de toutes les capacités dont nous disposons là-bas. Nous travaillons avec Recherche et développement pour la défense Canada, RDDC, à l'élaboration d'algorithmes pour le radar à synthèse d'ouverture, et nous sommes des chefs de file mondiaux dans ce domaine. En fait, nos homologues américains sont ébahis par les choses que nous faisons dans le secteur de la reconnaissance du domaine maritime. Nous sommes actifs dans de nombreux domaines. Selon moi, cette période est excitante parce que nous comprenons enfin de quoi il retourne. Lorsque nous parlons de l'omniprésence de l'espace et de la façon dont nous comptons sur lui, nous comprenons vraiment de quoi nous parlons.

The Chair: I just have two quick points to wrap this up. Is Canada the only Five Eyes partner besides the U.S. with space aspects?

La présidente : Pour conclure cette discussion, il y a deux questions que j'aimerais soulever. Si l'on fait abstraction des États-Unis, le Canada est-il le seul partenaire des Five Eyes à mettre en œuvre des programmes spatiaux?

Brig.-Gen. Pitre: Having actual hardware like RADARSAT in space, I think the answer is yes.

Bgén Pitre : Oui, je pense que nous sommes les seuls à disposer de matériel spatial comme RADARSAT.

Col. Dupuis: The answer is definitely yes.

Col Dupuis : La réponse à cette question est assurément oui.

The Chair: When we were in Washington, this discussion came up. I think you have touched on it briefly, but I will just give you 15 seconds to say it out loud. The U.S. is looking to their partners for niche capability. What is it that we put on the table that no one else has?

La présidente : Lorsque nous étions à Washington, cette question a été abordée. Je pense que vous l'avez effleurée brièvement, mais je vais vous accorder 15 secondes seulement pour en parler à voix haute. Les Américains comptent sur leurs partenaires pour se procurer des capacités-créneaux. Qu'avons-nous à offrir qu'aucune autre nation n'est en mesure d'offrir?

Brig.-Gen. Pitre: Whether it is circumstance or by design, all of us in the world today understand that we need to work together. Everything we do is about collaboration and leveraging. Sapphire was a good example years ago. Today, we are working closely with the Five Eyes and the U.S. through the collaboration in the space exchange of data, where we can bring capability that perhaps others do not or cannot in surveillance of space. Sapphire is one grand example, and RCM will be an example as well.

Bgén Pitre : Que ce soit par coïncidence ou à dessein, de nos jours, tous les pays du monde comprennent que nous devons travailler ensemble. Tous les projets que nous entreprenons dépendent de la collaboration et de l'effet de levier. Autrefois, le satellite Sapphire en était un excellent exemple. Aujourd'hui, nous travaillons étroitement avec les Five Eyes et les États-Unis en communiquant les données que nous recueillons dans l'espace. Dans le domaine de la surveillance spatiale, nous pouvons apporter une capacité que les autres nations peuvent ne pas être en mesure d'apporter. Le satellite Sapphire en est un parfait exemple, tout comme le sera la MCR.

The Chair: That is very helpful. Thank you. I want to thank you both very much for your testimony here today. We appreciate this. Our thanks to Brigadier-General Pitre and to Colonel André Dupuis.

La présidente : Vos observations nous sont très utiles. Merci. Je tiens à vous remercier tous les deux de votre témoignage d'aujourd'hui. Nous vous en sommes reconnaissants. Nous offrons nos remerciements au brigadier-général Pitre et au colonel André Dupuis.

We will switch gears again today and welcome back to the committee a guest that —

Encore une fois aujourd'hui, nous allons changer de sujet et souhaiter de nouveau la bienvenue à un invité qui...

Senator Dallaire: Last time it was a bow tie and now it is a tie.

Le sénateur Dallaire : La dernière fois, il portait un nœud papillon et, aujourd'hui, il porte une cravate.

The Chair: Stay focused, Senator Dallaire.

La présidente : Concentrez-vous, sénateur Dallaire.

The committee made a travel trip this summer to Maritime Forces Pacific, and we were briefed on site there on the Asia-Pacific picture by Dr. James Boutilier. We are pleased to welcome him back today to brief us at committee so it becomes part of our official record as we look at these issues. Dr. Boutilier is a professor at the Centre for Asia-Pacific Initiatives at the University of Victoria and a special adviser on policy at the Maritime Forces Pacific, where we first encountered him. This is in the context of looking at the pivot to Asia, as it is described, in terms of trade, but here at this committee we focus more on the defence and security side of it. I see you brought a document with slides. They will not be up on the screen for our viewing audience to see, but we will walk through it. We invite you to begin. Thank you very much for making this trip. We appreciate it.

Cet été, le comité a visité les Forces maritimes du Pacifique et, sur place, M. James Boutilier nous a donné une séance d'information sur la situation en Asie-Pacifique. C'est avec plaisir que nous l'accueillons de nouveau aujourd'hui, afin qu'il renseigne le comité et que ses propos figurent dans le compte rendu lorsque nous étudierons des questions. M. Boutilier est professeur au Centre for Asia-Pacific Initiatives de l'Université de Victoria et conseiller spécial des Forces maritimes du Pacifique en matière de politiques. C'est en les visitant que nous l'avons rencontré pour la première fois. C'était dans le contexte de l'examen du pivot vers l'Asie, comme il est décrit sur le plan commercial, mais, au sein de notre comité, nous mettons davantage l'accent sur ses facettes relatives à la défense et à la sécurité. Je vois que vous apportez un document contenant des diapositives. Celles-ci ne seront pas projetées sur l'écran et, par conséquent, notre auditoire ne pourra pas les voir. Toutefois, nous les passerons en revue. Nous vous invitons à commencer votre exposé. Nous vous remercions de vous être déplacé pour nous le donner. Nous vous en sommes reconnaissants.

James A. Boutilier, Professor, Centre for Asia-Pacific Initiatives, University of Victoria, Special Advisor (Policy) at the Maritime Forces Pacific, as an individual: Thank you very much, madam chair and distinguished members of the committee.

James A. Boutilier, professeur, Centre for Asia-Pacific Initiatives, Université de Victoria, conseiller spécial (politiques) auprès des Forces maritimes du Pacifique, à titre personnel : Je vous remercie infiniment, madame la présidente, et je remercie également les membres du comité.

While I serve as the Asia-Pacific adviser to the Commander Maritime Forces Pacific, I come before you this afternoon as a long-time student of the Asia-Pacific maritime arena. Quite clearly, the details of Canadian naval policy in the region are the province of the Commander Royal Canadian Navy and his senior colleagues.

Bien que je joue le rôle de conseiller sur l'Asie-Pacifique auprès du commandant des Forces maritimes du Pacifique, je me présente devant vous cet après-midi en ma qualité d'étudiant de longue date de la sphère maritime de l'Asie-Pacifique. Il est clair que les détails concernant la politique navale canadienne dans la région relèvent de la compétence du commandant des Forces maritimes du Pacifique et de ses collègues hauts gradés.

Let me provide one or two quick contextual comments before I go into the main elements of my brief.

Avant que j'aborde les principaux éléments de mon exposé, permettez-moi de vous faire part d'une ou deux brèves observations contextuelles.

I think one can argue that this is the maritime century and that increasingly, interstate affairs will be highly related to affairs at sea, whether it is in the commercial realm or the naval realm.

Je crois qu'on peut soutenir que notre siècle revêt un caractère maritime et que les affaires inter-États seront de plus en plus souvent liées aux affaires maritimes, que ce soit sur le plan commercial ou naval.

Second, I would suggest that naval assets — maritime assets, broadly speaking — will be extraordinarily important in terms of our national welfare.

Deuxièmement, je vous fais remarquer que les actifs navals — en gros, les actifs maritimes — revêtiront une importance primordiale du point de vue de notre bien-être national.

In this presentation, we see that the dramatic, profound and rapid shift in the world centre of economic gravity has been matched by an equally profound shift in the world centre of military and, in this context, maritime gravity. As the first feature of that phenomenon, we see that the old front-line navies have declined dramatically, certainly in their numerical size. One can theologically argue that the individual assets, frigates, submarines, destroyers and so forth are much more capable now than they were 20 or 40 years ago.

Dans ces diapositives, nous observons que le centre de gravité économique mondial s'est déplacé de manière rapide, radicale et spectaculaire et que cette évolution s'est accompagnée d'un déplacement aussi radical du centre de gravité militaire mondial et, dans ce contexte, du centre de gravité maritime mondial. Comme première manifestation de ce phénomène, nous remarquons que les anciennes armées navales de première ligne ont régressé radicalement, et c'est certainement le cas de leurs effectifs. Évidemment, on peut soutenir théoriquement que chaque actif maritime, chaque frégate, chaque destroyer, entre autres, ont plus de capacités maintenant qu'ils en avaient il y a 20 ou 40 ans.

Also, I think — and I do not believe this is a glib response — that you cannot have a destroyer in two places at the same time. There is a quality about quantity. When you were on the West Coast, I cited an example of the Royal Navy, which had 152 frigates and destroyers in 1962; it now has 19. Similarly, when we look at the greatest navy on the face of the earth, the United States Navy, in the mid-1980s, under a forward-leaning Secretary of the Navy, John Lehman and a highly supportive U.S. President, Ronald Reagan, there was a plan for a 600-ship navy. This was a pale imitation of the 6,000 ships in the U.S. Navy in 1945. Nevertheless, a 600-ship navy was suitably impressive. Of course in 1985, 1986, we were starting towards the very height of the Cold War. There were equally impressive statistics with respect to the Soviet Navy not only in the Atlantic, but also increasingly in the Pacific.

Of course, the Cold War came to an end before the 600-ship navy was ever realized, but when we look some 25 or 26 years later at the largest navy on the face of the earth, we would be lucky if we had perhaps 275 ships.

One can quite clearly say that within that context are 11 of the greatest aircraft carriers on the face of the earth, a breathtaking array of operational experience and so forth. However, the fact of the matter remains that as part and parcel of the global shift in maritime power, we can see that the navies upon which we have traditionally depended — and upon which the Royal Canadian Navy has depended and alongside which it has worked — have declined dramatically in size. Indeed, not so long ago, *The Economist* newspaper in the United Kingdom published a graph that showed the Chinese People's Liberation Army Navy surpassing the United States Navy in overall size. Once again, one can argue this is only a gross, and in many ways misleading, comparison on the basis of pure numbers.

What we see in the case of the Chinese navy is that China stands at the heart of the second great wave of globalization and that, in the past 30 years, we have had a stellar increase in Chinese economic capability. Much of this is export-led, and the oceans of the world, which in the Chinese cosmos of the past were seen as barriers are now seen perforce as the roots to opportunity. The untrammelled movement of commercial cargoes out of China and the importation of raw materials and energy into China are critical for sustaining the Chinese economic miracle.

As I suggested to you earlier in the year, we have a profound reorientation of the national axis of interest of Japan, China, and also India, away from China, towards the sea. We have an unprecedented situation in East Asia, powerful navies in India, China and Japan. If you look at the statistics for arms sales, they are compelling and overwhelming in the Asia-Pacific region

De plus, je pense qu'un destroyer ne peut pas se trouver à deux endroits en même temps — et je ne crois pas que ce soit là une affirmation désinvolte. La quantité peut être un gage de qualité. Lorsque vous vous trouviez sur la côte Ouest, j'ai cité l'exemple de la Marine royale qui, en 1962, disposait de 152 frégates et destroyers; elle en possède aujourd'hui 19. De même, lorsque nous examinons la plus importante marine de la planète, c'est-à-dire la marine américaine, nous constatons qu'au milieu des années 1980, sous l'autorité de John Lehman, un secrétaire de l'USN axé sur l'avenir, et de Ronald Reagan, un président des États-Unis coopératif, on planifiait de doter la marine de 600 navires. C'était peu en comparaison des 6 000 navires dont disposait l'USN en 1945. Quoi qu'il en soit, 600 navires représentaient une flotte assez impressionnante. Bien entendu, en 1985 et en 1986, nous dirigions vers le point culminant de la guerre froide. Les statistiques concernant la marine soviétique étaient également impressionnantes non seulement dans l'Atlantique, mais aussi de plus en plus fréquemment dans l'océan Pacifique.

Bien entendu, la guerre froide a pris fin avant que les 600 navires soient construits. Alors, lorsqu'on examine la plus importante marine de la planète quelque 25 ou 26 années plus tard, on s'estime heureux de répertorier peut-être 275 navires.

Bien qu'on puisse affirmer clairement que, parmi eux, se trouvent 11 des porte-avions les plus puissants de la planète et que la marine possède, entre autres, une vaste et stupéfiante expérience opérationnelle, il n'en reste pas moins que, dans le cadre du déplacement de la puissance maritime à l'échelle mondiale, nous pouvons constater que les marines sur lesquelles nous comptons habituellement — et sur lesquelles la Marine royale canadienne compte et avec lesquelles elle collabore — ont énormément régressé. En effet, il n'y a pas tellement longtemps, la revue britannique *The Economist* a publié un graphique qui montrait que l'importance de la marine de l'Armée Populaire Chinoise de Libération surpassait globalement celle de la USN. Encore une fois, on peut soutenir que cette comparaison grossière est fondée exclusivement sur des chiffres et qu'elle est trompeuse à de nombreux égards.

Toutefois, nous pouvons constater que la marine chinoise est au cœur de la deuxième grande vague de mondialisation et qu'au cours des 30 dernières années, la capacité économique de la Chine a connu une croissance fulgurante. Une grande partie de cet essor est engendrée par les exportations, et les océans de la planète qui, dans l'ancien univers chinois, représentaient des obstacles, sont maintenant perçus comme des sources de débouchés. Les cargos commerciaux qui quittent la Chine à un rythme effréné et ceux qui apportent des ressources énergétiques et des matériaux bruts en Chine sont essentiels au maintien du miracle économique chinois.

Comme je vous l'ai fait remarquer plus tôt au cours de l'année, le Japon, la Chine ainsi que l'Inde ont radicalement déplacé leur pôle d'intérêt national de la Chine vers la mer. La situation en Asie de l'Est est sans précédent; l'Inde, la Chine et le Japon possèdent maintenant de puissantes marines. Si l'on étudie les statistiques concernant la vente d'armes, on constate que les chiffres enregistrés

compared with elsewhere in the globe. The dynamic economies of the region have afforded the states opportunity to go upmarket, and expansion of regional navies is very much a feature of what I will call the Indo-Pacific region. Why Indo-Pacific? I think these are two very distinct oceanic regimes, but they have now become inextricably linked by virtue of flows of energy and by the naval ambitions particularly of the Chinese and the Indians. I think we need to think in terms of those two oceans as a grand maritime couplet in terms of larger geo-strategy.

Some would argue that we are witnessing a naval arms race, that we have moved beyond sheer modernization to an action-reaction phenomenon, where the purchases or development of weapons in one country lead to equal developments in neighbouring countries. We can perhaps see this particularly in the realm of submarines. Virtually all the navies of the region have gone upmarket, and a feature of that shift has been the appearance of submarines. Vietnam, for example, acquired six sophisticated Kilo Class submarines from the Russians; the Indonesians acquired submarines from South Korea, which in fact are variants on German 209s, 212s, 214s, and so forth. The Indians with their own indigenous nuclear and conventional program have a significant number of submarines being built in China.

We have in Pentagon parlance a submarine-rich environment in East Asia, at the very time that in broad terms we have lost sight of the submarine threat and of the need to hone our ASW capabilities. I do not direct that reference specifically to the Royal Canadian Navy but to navies in general, because of course in the 1990s, in the post-Cold War era, we saw our principal threats coming in the form of air attack and missiles, but we now find ourselves confronted with well over 200 operational submarines in the Indo-Pacific region, and from an ASW perspective the waters of the region are particularly challenging. They are complex geographically; in many cases they are shallow. New and quiet air-independent propulsion conventional submarines are very difficult to track. This is a source of mounting concern to the United States navy in particular as it begins to move its assets into the region.

I suggest in my presentation that a feature of Asia-Pacific or Indo-Pacific landscape is the dramatic increase in commercial shipping. Indeed, were we to go back to probably the rear pages of *The Globe and Mail* in 1983, almost 30 years ago, we would see a tiny article that suggested that trans-Pacific commercial trade had exceeded that across the Atlantic — almost 30 years ago,

dans la région de l'Asie-Pacifique sont convaincants et impressionnants, comparativement à ceux enregistrés dans les autres régions de la planète. Les économies dynamiques des pays de la région ont donné à ces derniers l'occasion de faire de folles dépenses, et l'expansion des marines régionales fait vraiment partie des caractéristiques de ce que j'appellerais la région indo-pacifique. Pourquoi fais-je allusion à la région indo-pacifique? Je pense que ces deux systèmes océaniques sont très distincts, mais ils sont devenus inextricablement liés en raison des flux de ressources énergétiques et des ambitions navales des Chinois et des Indiens, en particulier. D'un point de vue géostratégique général, nous devons envisager ces deux océans comme un grand duo maritime.

On pourrait soutenir que nous sommes témoins d'une course à l'armement naval, que nous sommes passés de la simple modernisation au syndrome de l'action-réaction et que, par conséquent, l'achat ou l'élaboration d'armements dans un pays entraîne la prise de mesures équivalentes dans les pays voisins. Nous pouvons peut-être le constater, en particulier dans le domaine des sous-marins. Pratiquement toutes les marines de la région ont fait de folles dépenses, et cela s'est traduit par l'apparition de sous-marins. Le Vietnam, par exemple, a acheté auprès des Russes six sous-marins de classe Kilo très avancés; les Indonésiens ont acheté des sous-marins de la Corée du Sud qui sont, en fait, des variantes des modèles allemands 209, 212, 214, et cetera. Grâce à leurs propres programmes d'armement nucléaire et conventionnel nationaux, les Indiens ont commandé en Chine de nombreux sous-marins dont la construction est cours.

Comme le dirait le Pentagone, l'Asie de l'Est est devenue un milieu riche en sous-marins, juste au moment où l'on pourrait affirmer, en termes généraux, que nous avons perdu de vue la menace sous-marine et la nécessité de perfectionner nos capacités de lutte anti-sous-marine. Ma remarque ne vise pas précisément la Marine royale canadienne, mais plutôt les marines en général parce qu'au cours des années 1990, la période qui a suivi la guerre froide, les principales menaces que nous avons observées ont pris la forme de missiles et d'attaques aériennes. Cependant, nous devons maintenant affronter plus de 200 sous-marins fonctionnels dans la région indo-pacifique et, sur le plan de la lutte anti-sous-marine, les eaux de la région sont particulièrement difficiles à manœuvrer. Elles sont complexes sur le plan géographique et, dans bien des cas, peu profondes. De plus, les nouveaux sous-marins conventionnels à propulsion anaérobie sont peu bruyants et très difficiles à repérer. Cela représente une source croissante de préoccupations pour l'USN, en particulier au moment où elle commence à transférer certains de ses actifs dans la région.

Dans mon exposé, je vous fais remarquer que l'une des caractéristiques du paysage de l'Asie-Pacifique ou de l'Indo-Pacifique est l'accroissement spectaculaire des activités commerciales de ses transports maritimes. En effet, si nous consultions les dernières pages des numéros du journal *The Globe and Mail* de 1983, soit des numéros datant d'à peu près 30 ans, nous

ladies and gentlemen. Now it is three and a half times as great as the trade across the Atlantic.

Indeed, if you go to Los Angeles/Long Beach in California, something like 25,000 trailer trucks a day pull away bound for the Costcos and Walmarts of this world, part of the larger relationship between the North American economies and the economies of Asia and, more specifically until recently, of China. The export-led economy of China demanded this sort of shipping capacity.

I suggest in my presentation to you that if we look at the statistics, if we were to look at the year 2002, we would probably find that five or possibly six of the leading ports of the world were in Asia, and now it is eight of the top ten ports in the world, whether it is Singapore, Shanghai, Busan, Kaohsiung in Taiwan and so forth. These are monster ports, which make Vancouver, our largest port, look like a modest backwater.

Singapore moves probably 30 million TEUs, that is to say the conventional 20-foot equivalent units, every year. As a sidebar, it is interesting to note that they have not lost one minute to work stoppages in the past 35 years, which is telling in and of itself. A feature of China's new-found discovery of the sea and of sea power in the broadest sense of the word is that within the next few years China will probably be the largest shipbuilder on the face of the earth.

One can argue that the South Koreans or the Japanese are perhaps somewhat more sophisticated shipbuilders in terms of LNG tankers or cruise ships and so forth, but when it comes to commercial shipping, by and large, it is the Chinese who will come to dominate the landscape. This of course creates the circumstance that enables them to build the Chinese navy and indeed to sell warships to other nations in Asia, for example, Pakistan.

If we go to the junction between the Indian and Pacific oceans, that is to say the Strait of Malacca, an extraordinarily narrow, confined waterway that links the Indian Ocean to the South China Sea, an area that is contested in its own right — of which more in a moment — we see that there are probably upwards of 70,000 ships, large and small, that ply through that strait every year. That number is scheduled to rise to about 140,000 probably by the mid-2020s. It is quite astonishing to imagine that density of traffic anywhere in Canadian waters.

I allude in passing to the importance of Vancouver, and Vancouver's growth continues to be impressive, but by Asian standards Vancouver is still, as I suggest, a very modest port. What we see, of course, is that the evolution of Prince Rupert has begun to amend the overall port capacity, particularly in Western

y trouverions un petit article qui laisse entendre que le commerce transpacifique a supplanté le commerce transatlantique — cela s'est produit il y a presque 30 ans, mesdames et messieurs. Maintenant, il est 3,5 fois plus important que le commerce transatlantique.

En effet, si vous visitez Los Angeles ou Long Beach en Californie, vous observerez quelque 25 000 semi-remorques qui quittent quotidiennement les lieux à destination des Costco et des Walmart de l'univers commercial. Cela s'inscrit dans le cadre de la relation élargie que les économies de l'Amérique du Nord entretiennent avec les économies de l'Asie et en particulier, jusqu'à récemment, avec la Chine. Le fait que son économie est axée sur les exportations a forcé la Chine à développer ce genre de capacité maritime.

Dans mon exposé, je vous fais remarquer que si nous examinions les statistiques, nous constaterions qu'en 2002, cinq et peut-être six des ports les plus importants de la planète se trouvaient en Asie. Aujourd'hui ce sont 8 des 10 principaux ports du monde qui s'y trouvent, que ce soit Singapour, Shanghai, Busan, Kaohsiung, à Taiwan, et cetera. Ces ports sont gigantesques et donnent à Vancouver, notre port le plus important, l'allure d'un modeste port reculé.

Singapore préside annuellement au transport d'environ 30 millions d'EVP, c'est-à-dire des équivalents vingt pieds traditionnels. En passant, il est intéressant de noter qu'au cours des 35 dernières années, aucun arrêt de travail n'a entraîné des pertes de temps dans ce port, ce qui en dit long. Le fait que, d'ici quelques années, la Chine sera probablement le plus important constructeur naval de la planète découle de sa découverte récente de la mer et de la puissance maritime, au sens le plus large des termes.

On peut soutenir que les Japonais et les Coréens du Sud sont peut-être des constructeurs navals un peu plus avant-gardistes, pour ce qui est, entre autres, des méthaniers et des paquebots de croisière, mais, en ce qui concerne la navigation commerciale en général, ce sont les Chinois qui domineront bientôt le secteur. Ces circonstances leur permettent bien entendu de construire la marine chinoise et de vendre des navires de guerre aux autres nations d'Asie, comme le Pakistan.

À la jonction de l'océan Indien et de l'océan Pacifique, il y a le détroit de Malacca, une voie navigable extrêmement exiguë qui relie l'océan Indien à la mer de Chine méridionale, une zone elle-même contestée — dont je parlerai davantage dans un moment —, et que, d'après nos constatations, probablement plus de 70 000 navires de toute dimension empruntent annuellement. On prévoit que ce chiffre passera à 140 000 probablement d'ici le milieu des années 2020. Il serait stupéfiant d'imaginer un trafic d'une telle densité où que ce soit dans les eaux canadiennes.

Je mentionne en passant l'importance du port de Vancouver, dont la croissance est impressionnante. Toutefois, selon les normes asiatiques, Vancouver est toujours, à mon sens, un port très modeste. Bien entendu, nous constatons que l'évolution de Prince Rupert commence à modifier la capacité portuaire globale

Canada, and this is certainly critical as part of the larger maritime landscape in the Indo-Pacific region.

What I would suggest further is that that Indo-Pacific region has become increasingly problematic and brittle as a maritime environment, that, whereas the Atlantic is small, empty, non-confrontational, if we go into the Pacific, we probably see more than 50,000 islands, 70-plus maritime disputes with respect to offshore resources, contested boundaries and ownership of islands. It is an excruciatingly complex region jurisdictionally and geographically. What we see is that many of the interstate disputes are being played out at sea, and in some cases these are deeply disturbing, deeply worrying, cat-and-mouse encounters that involve the loss of life at sea and the exchange of naval gunfire.

What I have before you, of course, is a compelling photo of what was left of the front half of a South Korean corvette sunk in March of 2010 by the North Koreans. I think the evidence is overwhelming that a North Korean submarine engaged in this provocative act of war by torpedoing the Republic of Korea's ship, *Cheonan*. Forty-six sailors died. Of course, it is a measure of the realities of the Korean Peninsula that other than fulminating there was little the South Koreans could do. Were they to react, they were possibly inviting overall peninsular war.

This is only one of many episodes in which ships have been damaged or sunk over the past decade in Asian waters. Nothing comparable exists in the Atlantic or even in the Indian Ocean.

I go on to suggest that there is an array of issues that are particularly compelling, particularly a source of concern.

You will have seen, of course, that there have been major tensions between Tokyo and Beijing over three tiny islets, the Senkaku Islands. One can argue that historically there was a lack of specificity at the end of the Second World War regarding ownership of these islands. If you are able to ensure ownership, then of course that confers upon you, as you are well aware, under the UN Convention on the Law of the Sea, an exclusive economic zone of 200 nautical miles with enormous implications in terms of subsea energy, oil and gas. Of course, if we look at China, for example, we see that in the next 25 to 30 years, 50 per cent of the global demand for oil will come from China alone. Perhaps this will be tempered somewhat by the recent turndown in Chinese economic performance, but what we see is that the Senkakus illustrated here are only part of a much larger array of disputes that involve, for example, Manila and Beijing, in which the Chinese have employed state oceanic administration vessels, which in many cases are nearly the size of our frigates, to advance their interests. One could argue that by holding back the Chinese navy and by using these sorts of semi-military or

du Canada, en particulier dans l'Ouest canadien, ce qui est assurément essentiel dans le contexte du paysage maritime plus vaste de la région indo-pacifique.

En outre, je vous ferais observer que le milieu maritime de la région indo-pacifique devient de plus en plus problématique et fragile. Alors que l'océan Atlantique est restreint, vide et non conflictuel, l'océan Pacifique compte plus de 50 000 îles et donne lieu à quelque 70 conflits maritimes liés à des ressources extracôtières, des contestations frontalières et des différends concernant la propriété de certaines îles. Cette région est extrêmement complexe du point de vue des compétences concernées et de ses caractéristiques géographiques. Nous remarquons que bon nombre des différends qui opposent les États se manifestent en mer et, dans certains cas, cela donne lieu à des parties de chasse extrêmement inquiétantes et troublantes qui entraînent des échanges de tirs d'artillerie navale et des décès en mer.

Ce que je vous présente, évidemment, c'est une photo qui montre de façon incontestable ce qui restait de la moitié avant d'une corvette sud-coréenne coulée en mars 2010 par les Nord-Coréens. Je crois que les preuves nous indiquent clairement qu'un sous-marin nord-coréen a accompli cet acte de guerre provocateur en torpillant le navire de la République de Corée, le Cheonan. Quarante-six marins ont perdu la vie. Bien sûr, cela reflète les réalités de la péninsule coréenne contre lesquelles les Sud-Coréens ne pouvaient à peu près rien faire d'autre que de fulminer. S'ils avaient réagi, ils auraient possiblement déclenché une guerre péninsulaire générale.

Ce n'est que l'un des nombreux épisodes au cours desquels des navires ont été endommagés ou coulés dans les eaux asiatiques durant la dernière décennie. Il n'existe rien de comparable dans l'Atlantique, ni même dans l'Océan indien.

Il y a, à mon sens, de nombreux enjeux qui sont particulièrement importants, qui sont une source de préoccupations.

Vous aurez constaté, évidemment, qu'il existe de fortes tensions entre Tokyo et Beijing au sujet de trois îlots minuscules, les îles Senkaku. D'aucuns diront qu'il n'y a pas eu suffisamment de précisions, à la fin de la Seconde Guerre mondiale, en ce qui a trait à la propriété de ces îles. Si vous êtes en mesure d'en assurer la prise en charge, alors évidemment, cela vous confère, comme vous le savez, en vertu de la Convention des Nations Unies sur le droit de la mer, une zone économique exclusive de 200 milles marins, ce qui a des incidences très importantes sur le plan de l'énergie sous-marine, du pétrole et du gaz. Nous savons, par exemple, que d'ici 25 ou 30 ans, la moitié de la demande mondiale de pétrole proviendra de la Chine seulement. Cela sera peut-être quelque peu atténué par le récent ralentissement de la performance économique chinoise, mais ce que nous constatons, c'est que les îles Senkaku, illustrées ici, ne sont qu'un élément d'une série beaucoup plus importante de conflits qui concernent, par exemple, Manille et Beijing, dans lesquels les Chinois ont utilisé des navires de l'administration des océans qui, bien souvent, font presque la taille de nos frégates, pour servir leurs

paramilitary proxies, they have tried to calibrate the degree of tension between the claimants.

Of course, what is particularly worrisome in a third of the examples I cite is that the Chinese are in the process of offering exploration blocks off Vietnam to international oil companies when those blocks are claimed by the Vietnamese. How these exercises in exploration and exploitation will play out very much remains to be seen. One reason the Vietnamese have acquired submarines is to give the Chinese cause for reflection.

Then we see the whole question of the so-called pivot to Asia. Some would argue we are going through our own pivot here in Ottawa with respect to our newfound interest in the region; this is certainly reflected in the Prime Minister's sorties into Asia. Many in Washington would prefer that the word "pivot" was not used. They would maintain what is happening is that, after Washington's interests were deflected by events in southwest Asia, Iraq and Afghanistan, the Americans are simply reasserting in a more profound manner their interests in the region, that they were always there.

Although I must confess there were anxieties on the part of many of the regional players as to whether they would stay the course, the Americans are now back. This is illustrated powerfully by President Obama's presence in Myanmar — or Burma — and now in Cambodia, and by the fact that Secretary of State Clinton has been extraordinarily active in travelling throughout the region, as have the various defence secretaries, such as Gates and Panetta. If we go back as far as 2006, we see that the quadrennial defence review mandated by Congress pointed to the fact that the future lay in Asia and that the United States Navy should begin to distribute its resources asymmetrically into the region — six carriers, with five in the Atlantic, and perhaps 60 per cent of the United States Navy submarine capability, and so forth.

One important element of all of this is the evolution of what I would call the Washington-New Delhi axis. This may be putting an undue or unfair element of formality — it is not an axis as such. However, the fact remains that the past decade has seen a new relationship emerge between the United States and India, which has enormous implications, and it is primarily maritime in its outlook. We see major exercises in the Indian Ocean involving the Indian navy, the Americans, Australians, Singaporeans and, tellingly, the Japanese.

From the perspective of the Chinese, who would argue that the growth of their navy is absolutely justified and in keeping with the history of other great nations on the rise, Beijing would argue that they are witnessing an unwarranted containment — what I call "containment light." When they look out from Beijing, they see the Americans in South Korea, Japan, Okinawa, Guam, increasingly in the Philippines, Australia, Singapore, conceivably in Burma in the future, certainly in India, Pakistan, even in the central Asian republics, and Mongolia. They would

intérêts. On peut faire valoir qu'en freinant la marine chinoise et en utilisant ce type d'intermédiaires semi-militaires ou paramilitaires, on tente de calibrer le niveau de tension entre les parties concernées.

Ce qui est particulièrement inquiétant dans une partie de ces exemples, c'est que les Chinois sont en train d'offrir à des sociétés pétrolières internationales des blocs d'exploration au large du Vietnam, alors que les Vietnamiens les revendiquent. Il faudra voir comment ces activités d'exploration et d'exploitation vont se dérouler. Les Vietnamiens ont acquis des sous-marins dans le but, notamment, d'inciter les Chinois à la réflexion.

Il y a ensuite toute la question de ce qu'on appelle le pivot vers l'Asie. Certains diront que nous avons notre propre pivot ici à Ottawa en raison de l'intérêt que nous portons depuis peu à la région; cela se reflète dans les sorties du premier ministre en Asie. Il y a bien des gens à Washington qui préféreraient que le mot « pivot » ne soit pas utilisé. Ils maintiendraient qu'étant donné que les intérêts de Washington ont été détournés par les événements qui se sont produits en Asie du Sud-Ouest, en Irak et en Afghanistan, les Américains réaffirment simplement de façon plus définitive leurs intérêts dans la région, et qu'ils ont toujours été là.

Bien qu'il y ait eu des inquiétudes de la part des acteurs régionaux quant à savoir s'ils allaient rester dans la course, les Américains sont maintenant de retour, comme en témoignent de façon éloquente la présence du président Obama au Myanmar, ou en Birmanie, et maintenant au Cambodge, et le fait que la secrétaire d'État Hillary Clinton effectue de nombreux déplacements dans toute la région, à l'instar de divers secrétaires à la Défense, comme Gates et Panetta. Si nous nous reportons à 2006, nous constatons que l'examen quadriennal de la défense mandaté par le Congrès a souligné le fait que l'avenir passe par l'Asie et que la Marine des États-Unis devrait commencer à affecter ses ressources de façon asymétrique dans la région — six porte-avions, dont cinq dans l'Atlantique, et peut-être 60 p. 100 de ses sous-marins, et cetera.

L'un des éléments importants, dans tout cela, c'est l'évolution de ce que j'appellerais l'axe Washington-New Delhi, même si cela peut introduire, indûment ou injustement, une notion de formalité, car il ne s'agit pas d'un axe comme tel. Toutefois, il reste qu'au cours de la dernière décennie, les États-Unis et l'Inde ont établi une nouvelle relation qui a des incidences énormes et dont la perspective est principalement maritime. Il y a des exercices importants dans l'océan Indien, auxquels participent la marine indienne, les Américains, les Australiens, les Singapouriens et, ce qui est révélateur, les Japonais.

Du point de vue des Chinois, personne ne contesterait le fait que la croissance de leur marine est tout à fait justifiée, et conformément à l'histoire d'autres grandes nations en plein essor, les Chinois soutiendraient qu'ils sont témoins d'un confinement injustifié — ce que j'appelle une « optique de confinement ». De Beijing, ils voient les Américains en Corée du Sud, au Japon, à Okinawa, à Guam, de plus en plus aux Philippines, en Australie, à Singapour, vraisemblablement en Birmanie dans l'avenir, assurément en Inde, au Pakistan, même dans les républiques d'Asie centrale, et en

maintain that this is an artifact of the Cold War — that the attitude of the Americans is one in which China's legitimate ambitions are being unfairly checked.

I think what has happened is that Washington has gone to considerable lengths to try to reassure Beijing. However, at the same time, there is a profound substratum of distress in the trans-Pacific relationship, which Washington has not succeeded in dispelling.

A feature of the area is that the Chinese have developed — and it is only one aspect of a much more complex maritime environment — what is called the Dong Feng 21D. This is a ballistic missile that the Chinese maintain they have modified to the degree that when it re-enters the Earth's atmosphere, it is manoeuvrable and can take out a U.S. naval carrier. This, in the iconic words of the great Hollywood movie *Dirty Harry*, is designed to make your day. There are those who are skeptical about China's technical accomplishments in this realm, but many senior officials in the United States Navy are taking this very seriously.

You see references in the literature to the so-called Air-Sea Battle Doctrine. I think this is a murky and ill-defined American doctrine for the moment. Perhaps it suggests the prevalence of common sense that the Americans are in no hurry to put combat forces onto the Asian continent and that in the future, they will have to depend on sea and air capabilities.

The Chinese are pursuing the standard strategy of a weaker naval power in the sense that they are trying to deny access to the Asian coast, to hold U.S. carriers at bay with weapons like the Dong Feng 21, an array of submarines, cruise missiles and so on and so forth.

What we see throughout the region is a profound strategic ambiguity. That is to say that if we go to Australia, we find that China is Australia's number one trade partner in iron ore, uranium, a vast array of other minerals, et cetera, which flow out of this continental storehouse of Australia and underwrite the continued growth of the Chinese economy. However, the great security access for Canberra does not lie to Beijing; it lies to Washington. Therefore, this is a complex and potentially contradictory triangle of power.

If you go to almost every other nation in Asia, you find that China is the number one trade partner, having supplanted the United States in the past 10 to 15 years. However, all of the nations in the region are keeping their powder dry because they do not know China's end game. This is certainly true in India. China is rapidly becoming India's number one trade partner, but if you talk to senior security analysts in New Delhi, there is only one word in their lexicon, and that is "China."

Therefore, there is a profound sense of ambiguity as to what the future holds. Throughout the region, there is a disturbing legacy of history. Whereas in Europe the Germans have moved in a moment of maturity beyond the terrifying legacy of the Hitler era, this is not the case in the Pacific. Still the wounds of World War II are kept alive, either artificially or otherwise; the Japanese have, frankly, been maladroit in their handling of the World

Mongolie. Ils maintiendraient que c'est un vestige de la guerre froide — que l'attitude des Américains contribue à freiner injustement les ambitions légitimes de la Chine.

Ce qui s'est produit, selon moi, c'est que Washington a déployé des efforts considérables pour rassurer Beijing. Or, en même temps, il y a un important fondement de détresse dans la relation transpacifique, et Washington n'a pas réussi à le dissiper.

Dans la région, les Chinois ont développé — et ce n'est qu'un aspect d'un environnement maritime bien plus complexe — ce qu'on appelle le Dong Feng 21D, un missile balistique qu'ils affirment avoir modifié afin qu'il soit manœuvrable lors de sa rentrée dans l'atmosphère terrestre et qu'il puisse éliminer un porte-avions américain. Il est conçu pour causer des dégâts, comme on dit. Certaines personnes sont sceptiques quant aux réalisations techniques de la Chine dans ce domaine, mais de nombreux hauts gradés de la marine américaine prennent la menace très au sérieux.

Dans la documentation, on fait référence à ce qu'on appelle la doctrine de bataille aéronavale. Je crois que c'est une doctrine américaine sombre et mal définie pour le moment. Elle laisse peut-être entrevoir que les Américains ne sont pas pressés d'envoyer des forces de combat sur le continent asiatique et qu'à l'avenir, ils devront compter sur les ressources navales et aériennes.

Les Chinois misent sur la stratégie habituelle d'une puissance navale faible, en ce sens qu'ils essaient de bloquer l'accès à la côte asiatique, de tenir les porte-avions américains en échec avec des armes comme le Dong Feng 21, de nombreux sous-marins, des missiles de croisière, et cetera.

Il y a dans la région une ambiguïté stratégique profonde. En effet, la Chine est le principal partenaire commercial de l'Australie pour le minerai de fer, l'uranium et bien d'autres minéraux, qui viennent de l'entrepôt continental de l'Australie et assurent la croissance continue de l'économie chinoise. Toutefois, le principal accès de sécurité pour Canberra ne se trouve pas à Beijing, mais bien à Washington. Par conséquent, c'est un triangle du pouvoir complexe et potentiellement contradictoire.

La Chine est le principal partenaire commercial de presque tous les autres pays d'Asie; elle a supplanté les États-Unis dans les 10 à 15 dernières années. Cependant, tous les pays de la région sont sur leurs gardes, car ils ne connaissent pas l'objectif ultime de la Chine. C'est certainement vrai en ce qui concerne l'Inde. La Chine devient rapidement le principal partenaire commercial de l'Inde, mais elle constitue également la seule préoccupation des analystes principaux de la sécurité à New Delhi.

Par conséquent, il existe un profond sentiment d'ambiguïté quant aux perspectives d'avenir. Dans toute la région, l'héritage de l'histoire est inquiétant. En Europe, les Allemands, grâce à leur maturité, ont dépassé l'héritage terrifiant de l'ère d'Hitler, mais ce n'est pas le cas dans le Pacifique. Les souvenirs des blessures de la Seconde Guerre mondiale sont toujours vivants; pour tout dire, les Japonais ont bien mal géré le legs de la Seconde Guerre

War II legacy, and the Chinese have been extremely ready to raise the spectre of the rape of Nanjing and other terrible experiences in their interstate relations.

Right across the region there is the problem of history. Uncertainties or debates with respect to history also underpin many of the maritime disputes, with the various players all alluding to their historical claims, none of which could probably stand international legal scrutiny.

One of the great exercises of the region is RIMPAC, the Rim of the Pacific. You may very well have been briefed on the enormity of this exercise — vast armadas of ships and vast arrays of men and women, aircraft, and so forth. I would suggest to you that in the Cold War there was a clear anti-Soviet narrative that underpinned RIMPAC. Now I would suggest that, while it is certainly not expressed in public terms, it is probably an anti-Chinese narrative. Interestingly enough, we see that the Americans have extended an invitation to China to be an observer in RIMPAC in the future.

What are the challenges for Canada? I will leave the specifics of naval policy, as I suggested, to the Commander of the Navy; he is ideally suited to address these issues. However, we see that there is a new and challenging arena, in terms of commercial shipping, defence acquisitions, the growth of navies, unresolved disputes, and setting nations one against another at sea. There are sidebar issues with respect to submarine resources, with respect to fish, with respect to illegal movements of people, piracy and so forth, all of which suggest that we need, as a nation, to pay particular attention to this part of the world.

The great beauty about CPAR, about naval vessels, is that they are superbly nuanced and calibrated agents in the sense that there is no other weapons system that I am aware of which can, in fact, move literally, within minutes, from hosting some diplomatic naval reception to engaging in search and rescue or humanitarian assistance and disaster relief or hunting for pirates and so forth. Naval vessels are by their very nature extraordinarily potent vessels in terms of telegraphing national resolve, and history, I think, has underscored this fact.

Thank you very much.

The Chair: Thank you very much. That was a very complete setting of the stage. Just as we begin our questioning, and I know our time is short today, you sort of left it there. Is it a pivot or reassertion, in your view, on the part of the Americans? What is it for us?

Mr. Boutilier: What is it for us? I think it is first and foremost a reassertion.

The Chair: For Canada as well?

Mr. Boutilier: Yes, and I think that after many years in which Canada was otherwise engaged, Canada has begun to come to grips very recently, within the past year or so within the defence realm in specific terms, to the challenges of Asia. One of the

mondiale, et les Chinois n'attendent que de soulever le spectre du viol de Nanjing et d'autres horribles événements dans leurs relations interétatiques.

Dans toute la région, il y a le problème que pose l'histoire. Les incertitudes ou les débats concernant l'histoire sont aussi à la base de nombreux conflits maritimes, dans lesquels les acteurs font tous allusion à leurs revendications historiques; or, probablement aucune ne pourrait résister à l'examen juridique international.

L'un des excellents exercices de la région est celui du RIMPAC. On vous a sans doute parlé de l'ampleur de cet exercice — de vastes flottes de navires et une grande quantité d'hommes et de femmes, d'avions, et cetera. Je dirais que durant la guerre froide, il y avait un discours clairement antisoviétique qui reposait sur le RIMPAC. Je dirais que maintenant, même si ce n'est pas exprimé publiquement, c'est probablement un discours antichinois. Fait intéressant, les Américains ont invité la Chine à être un observateur lors de futurs exercices RIMPAC.

Quels sont les défis pour le Canada? Je vais laisser, comme je l'ai dit, le commandant de la marine vous parler de la politique navale; il est le mieux placé pour le faire. Cependant, nous constatons qu'il existe un nouvel échiquier intéressant en ce qui concerne la navigation commerciale, les acquisitions militaires, la croissance des marines, les conflits non résolus, et les nations qui s'opposent l'une à l'autre en mer. Il y a des enjeux connexes relativement aux ressources sous-marines, au poisson, au mouvement illégal de personnes et à la piraterie, entre autres, et tous indiquent que nous devons, en tant que nation, porter une attention particulière à cette région du monde.

Le grand avantage du CPAR, des bâtiments navals, c'est que ce sont des systèmes admirablement nuancés et calibrés, en ce sens qu'il n'existe aucun autre système d'armes, à ma connaissance, qui peut passer littéralement, en quelques minutes, d'une réception diplomatique de la marine à une opération de recherche et sauvetage, d'aide humanitaire et de secours aux sinistrés ou de chasse aux pirates. Les bâtiments navals, par leur nature même, sont des navires extrêmement puissants lorsqu'il s'agit de communiquer la détermination nationale, et je pense que l'histoire a mis ce fait en évidence.

Merci beaucoup.

La présidente : Merci beaucoup. C'est une description très complète de la situation. Comme nous débutons notre série de questions, et je sais que notre temps est limité aujourd'hui, puisque vous en êtes en quelque sorte resté là, puis-je vous demander s'il s'agit d'un pivot ou d'une réaffirmation, selon vous, de la part des Américains? De quoi s'agit-il pour nous?

M. Boutilier : Pour nous? Je crois que c'est d'abord et avant tout une réaffirmation.

La présidente : Pour le Canada également?

M. Boutilier : Oui, et je pense qu'après avoir été occupé ailleurs durant de nombreuses années, le Canada a commencé tout récemment, dans la dernière année, plus précisément dans le secteur de la défense, à vraiment saisir les défis auxquels l'Asie est

problems, of course, in Asia, as you can imagine, is that there is no NATO framework. The area is huge geographically. There is no consensus in who constitutes the enemy the way there was in the Cold War. It is a challenging arena in terms of how do we engage.

Senator Dallaire: I notice you mentioned fishing as merely a sidebar, yet in food stocks in Asian countries, fish is a major staple. The fish off our coast are not insignificant in the Pacific and can, in fact, attract significant frictions, let alone all the other dimensions you mentioned of economy, such as movement of fuel from this country and natural resources and stuff coming back.

My point is that the navy has as the Maritime Component Commander the commander of the fleet on the East Coast. The generic threat assessment based on activity, let alone actual articulating of a threat, is the Pacific versus the Atlantic, with the Mediterranean still being a problem. I do not see why the Maritime Component Commander should be on the East Coast. I would contend that more of the lessons to be learned, more of the work and making RIMPAC a more mature exercise are on the West Coast. There is no equivalent to you on the East Coast with the Maritime Component Commander, which is not insignificant. I do not know how much more capacity the Armed Forces or DND possess.

What I am leading to is that it has taken years to build a balance between the two coasts because the poor cousin was always the West Coast. What is behind the reticence of moving more assets to the West Coast and building that capability there in Esquimalt or maybe even taking part in Prince Rupert to building more capacity for the navy?

Mr. Boutilier: That is a very interesting and appropriate question, general. Let me address several aspects of it.

Let me talk momentarily about fish. If we go to Southeast Asia, 80 per cent of the population of 500 million derive their protein from the sea. If you go all the way up the Asian coast, you find that fish stocks are in danger. The catches are declining in size, the number of species is declining and the size of the individual fish is declining.

There is a further element in all of this, and that is that climate change is warming the world's oceans, and fish are beginning to migrate towards the poles. A growing number of tropical nations will find it harder and harder to acquire fish. About 60 per cent of the world's stock of fish is now at or beyond carrying capacity. What you are beginning to see — and this is a real challenge for navies and coast guards — is the fact that illegal and unreported fishing is now increasingly rampant. This is a major threat. Right across the world, we will be faced with the politics of scarcity when it comes to fish stocks.

confrontée. Comme vous pouvez l'imaginer, l'un des problèmes en Asie, c'est qu'il n'y a pas de structure de l'OTAN. La région est immense, sur le plan géographique. Il n'y a pas de consensus pour déterminer qui constitue l'ennemi, comme c'était le cas durant la guerre froide. C'est un secteur où il est difficile de savoir comment nous engager.

Le sénateur Dallaire : J'ai remarqué que vous avez parlé de la pêche comme d'un enjeu connexe; pourtant, le poisson est un aliment de base dans les stocks alimentaires des pays asiatiques. Les poissons au large de nos côtes ne sont pas négligeables dans le Pacifique et cela peut, en fait, créer des frictions importantes, sans parler de tous les autres secteurs de l'économie que vous avez mentionnés, comme le déplacement de carburant à partir de ce pays, les ressources naturelles et les choses qui reviennent.

Ce que je veux dire, c'est que la marine a comme Commandant de composante maritime le commandant de la flotte de la côte Est. L'évaluation générale de la menace en fonction de l'activité, sans parler de l'expression d'une menace, est axée sur le Pacifique par rapport à l'Atlantique, et la Méditerranée est encore un problème. Je ne vois pas pourquoi le Commandant de composante maritime devrait être sur la côte Est. Je soutiens qu'il y a davantage de leçons à apprendre, davantage de travail à accomplir et davantage de maturité à donner à l'exercice RIMPAC sur la côte Ouest. Il n'existe aucun équivalent à ce que vous avez sur la côte Est avec le Commandant de composante maritime, ce qui n'est pas négligeable. J'ignore combien il reste de ressources aux forces armées ou au MDN.

Il a fallu des années pour créer un équilibre entre les deux côtes, car la côte Ouest était toujours considérée comme le parent pauvre. D'où vient la réticence à déplacer davantage de ressources sur la côte Ouest et à renforcer les capacités à Esquimalt ou peut-être même à participer au renforcement des capacités pour la marine à Prince Rupert?

M. Boutilier : C'est une question très intéressante et très appropriée, général. Permettez-moi de l'aborder sous plusieurs aspects.

Je vais parler brièvement de la question du poisson. En Asie du Sud-Est, 80 p. 100 de la population de 500 millions d'habitants tire ses protéines de la mer. Si on remonte la côte asiatique, on constate que les stocks de poisson sont menacés. Les prises diminuent, tout comme le nombre d'espèces et la taille des poissons.

L'autre élément à considérer, c'est que les changements climatiques contribuent à réchauffer les océans de la planète, et les poissons commencent à migrer vers les pôles. Un nombre croissant de pays tropicaux auront de plus en plus de difficulté à trouver du poisson. Environ 60 p. 100 du stock mondial de poissons a maintenant atteint ou dépassé sa capacité de charge. On commence à constater — et c'est un réel problème pour les marines et les gardes côtières — que la pêche illégale et non déclarée est maintenant de plus en plus endémique. C'est une menace importante. Partout dans le monde, nous serons confrontés à la dimension politique de la pénurie de poissons.

That is a source of growing national concern for many nations, particularly in East Asia. If you go to China, for example, you will find 300,000 fishing boats in their fishing fleet. As a sidebar, those boats have, in many cases, been pressed into service as proxies in the disputes over places like the Senkaku. If you look at the final photograph in my handout, you will see a compelling picture of two Japanese coast guard vessels coming to grips with a Chinese fishing boat.

There are some other issues. I will leave the larger policy issue of the balancing of the fleet to the commander of RCN. There are the dictates of geography in the sense of access to the Arctic, for example. Is it easier from Halifax? Is it easier from Esquimalt? If you go from Halifax to the Indian Ocean, you can go all the way to Chennai, or Madras, at one time, on the eastern flank of the Indian subcontinent, and that is the make-and-break point between Halifax, on the one hand, and Esquimalt on the other. One can argue that you can just as effectively service the whole of the Mediterranean, the Horn of Africa and so on from the East Coast as you can from the West Coast.

These are some features of global maritime geography that are worth bearing in mind, I think, when it comes to how ships are deployed. I will leave the specifics because that is really a policy issue that needs to be dealt with, and there are historic reasons why, in fact, the fleets were asymmetric in their size.

Senator Dallaire: You met the threat in the past. This growing threat and uncertainty is now in the West. Why is there that shift? You are an intellectual scientist in providing strategic guidance to these flag officers. Why is that not simply recognized in that action being taken?

Mr. Boutilier: I think that argument has been advanced. The countervailing argument is our NATO commitment and other things — this was certainly borne out in Libya and in the current presence of vessels in the eastern Mediterranean or in the Persian Gulf — and that there were other equally compelling arguments for the maintenance of a presence in the Atlantic. Again, I think that is a policy issue that is best addressed by the commander of the navy.

The Chair: He will be a witness for us soon.

Mr. Boutilier: That is good, and I am sure he will come to grips with that.

Senator Mitchell: With respect to CNOOC buying Nexen, if China is a threat, how does that fit into that?

Mr. Boutilier: This is part of this larger issue of ambiguity. I talked about geostrategic ambiguity. Now we are moving into a commercial, political ambiguity. One can make compelling arguments that China is an unparalleled opportunity. Indeed, one could argue that in the past decade, the world economic vitality would have suffered far more profoundly if it had not

Cela suscite de plus en plus l'inquiétude de bien des pays, en particulier en Asie de l'Est. En Chine, par exemple, la flotte de pêche compte 300 000 bateaux. En complément, ces bateaux, dans bien des cas, ont été mobilisés pour servir d'alliés dans les conflits concernant des endroits comme les îles Senkaku. Si vous regardez la dernière photographie de mon document, vous verrez deux navires de la garde côtière japonaise qui font face à un bateau de pêche chinois.

Il y a d'autres enjeux. Je vais laisser le commandant de la MRC vous parler de la question plus vaste de l'équilibre de la flotte. Il y a les diktats géographiques, par exemple l'accès à l'Arctique. Est-ce plus facile à partir d'Halifax? D'Esquimalt? Si vous partez d'Halifax pour vous rendre dans l'océan Indien, vous pouvez aller jusqu'à Chennai, ou Madras, sur le flanc Est du sous-continent indien, et c'est le point décisif entre Halifax, d'un côté, et Esquimalt, de l'autre. On pourrait dire que l'on peut desservir tout aussi efficacement toute la Méditerranée et la Corne de l'Afrique de la côte Est que de la côte Ouest.

Ce sont des caractéristiques de la géographie maritime mondiale qu'il vaut mieux garder à l'esprit, je pense, en ce qui a trait à la façon dont on déploie les navires. Je n'entrerai pas dans les détails parce qu'il s'agit en réalité d'une question de politique qu'il faut régler, et l'asymétrie de la taille des flottes s'inscrit dans un contexte historique.

Le sénateur Dallaire : Vous avez été confronté à la menace dans le passé. C'est maintenant le monde occidental qui est confronté à cette menace et à cette incertitude croissantes. À quoi ce virage est-il attribuable? Vous êtes un scientifique qui donne des conseils stratégiques à ces officiers généraux. Pourquoi ce fait ne se reflète-t-il pas dans les actions qui sont prises?

M. Boutilier : Je pense que cet argument a déjà été avancé. En contrepartie, il y a notre engagement envers l'OTAN et d'autres facteurs — cela a certainement été confirmé en Libye et par l'actuelle présence de navires dans le secteur oriental de la Méditerranée ou dans le golfe Persique — et il y a d'autres arguments tout aussi convaincants pour le maintien d'une présence dans l'Atlantique. Encore une fois, je pense qu'il s'agit d'une question de politique qui relève davantage du commandant de la marine.

La présidente : Il viendra témoigner au comité sous peu.

M. Boutilier : C'est bien, et je suis certain qu'il abordera le sujet.

Le sénateur Mitchell : En ce qui a trait à l'acquisition de Nexen par CNOOC, si on considère la Chine comme une menace, quel lien doit-on établir?

M. Boutilier : Cela fait partie de la question plus globale de l'ambiguïté. J'ai parlé de l'ambiguïté géostratégique. Nous entrons maintenant dans une ambiguïté commerciale et politique. On peut présenter des arguments forts convaincus selon lesquelles la Chine représente une occasion sans précédent. En effet, on pourrait faire valoir que dans la dernière décennie, la

been for the dynamism of China. We go back to 2001-02 when a major global downturn was anticipated but did not occur as a result of Chinese economic dynamism.

One can make the compelling argument that China is an opportunity. One can make the equally compelling argument that it is a threat. One of the important things to bear in mind is the prevalence and the pervasive presence of the party in China.

It is very much the same as if the Democratic Party in the United States controlled, for example, the appointment of all university presidents, the editors of all newspapers, the presidency or CEO-ships of all major corporations. That reality causes people to be concerned. One can argue that there are checks and balances, and I think that the Chinese have gone to some considerable lengths to try to tailor their offers to meet the realities of the Canadian marketplace.

Of course, this is not the only country where there have been hesitations about Chinese involvement. We can see, back more than a decade ago, Chinese overtures to Unocal in Texas, and that was turned down by Washington.

It becomes even more complex when we move into weapons systems, computer systems and so forth, to what degree we should permit their presence in North America. More and more evidence is forthcoming that hacking attacks and so on originate out of China.

I think clearly the CNOOC-Nexen issue is a decision that must be made at the senior-most levels in the political realm. It is somewhat removed from the maritime realm, other than of course it is part and parcel of China's insatiable demand for energy.

Just to conclude, I would say that the Chinese have embarked on an exceedingly impressive worldwide diversification of energy over the past 15 years, with energy coming out of Iraq, Iran, Angola, Sudan, Central Asia, Russia, Venezuela and Colombia. Their interest in energy in Canada is not surprising in any way. They are eager to, first, meet demand and, second, diversify to the extent that their ship-borne imports of energy will not be confined to one or two, for example, choke points like the Strait of Malacca, where they could be interdicted, one of the reasons for the whole complex energy politics with Central Asia.

Senator Mitchell: The U.S. has an interest in this relationship with CNOOC. In fact, today I read that Senator McCain suggested that the Parliament of Canada should look at this carefully. How intense are they about that, really, and what does that do to our relationship with them?

vitalité de l'économie mondiale aurait été beaucoup plus durement éprouvée, n'eût été le dynamisme de la Chine. Il faut remonter à 2001-2002, alors qu'on avait prévu un ralentissement économique mondial important et qui n'a pas eu lieu en raison de la vitalité économique de la Chine.

On peut faire valoir que la Chine représente une occasion. On peut tout aussi bien avancer qu'elle est une menace. Un des aspects importants qu'il faut garder en tête et la prévalence et l'omniprésence du parti en Chine.

C'est exactement comme si, aux États-Unis, le Parti démocrate contrôlait, par exemple, la nomination de tous les présidents d'université, des rédacteurs en chef de tous les journaux et des présidents ou des présidents-directeurs généraux de toutes les grandes entreprises. Cette réalité soulève des préoccupations chez les gens. On peut faire valoir qu'il y a un système de poids et de contrepoids, et je pense que les Chinois ont fait des efforts considérables pour essayer d'adapter leurs offres aux réalités du marché canadien.

Bien entendu, le Canada n'est pas le seul pays où l'on observe une certaine réticence à l'égard de la participation de la Chine. On a pu voir, il y a plus d'une décennie, un certain intérêt des Chinois envers Unocal, au Texas, ce qui a été refusé par Washington.

Quant à savoir jusqu'à quel point nous devrions accepter leur présence en Amérique du Nord, cela devient encore plus complexe lorsqu'on parle de systèmes d'armement, de systèmes informatiques, et cetera. De plus en plus de preuves tendent à démontrer que le piratage informatique, entre autres, est fait à partir de la Chine.

Je pense certainement que la question liée à CNOOC-Nexen est une décision qui relève des plus hauts dirigeants de la sphère politique. En quelque sorte, ce n'est plus lié au domaine maritime, outre le fait que cela fait évidemment partie intégrante de l'insatiable soif d'énergie de la Chine.

En conclusion, je dirais que ces 15 dernières années, les Chinois ont entrepris à l'échelle mondiale une stratégie de diversification des sources d'énergie extrêmement impressionnante. Leurs sources d'énergie sont l'Irak, l'Iran, l'Angola, le Soudan, l'Asie centrale, la Russie, le Venezuela et la Colombie. Leur intérêt envers les ressources énergétiques du Canada n'a rien de surprenant. D'abord, ils sont soucieux de satisfaire à la demande et, deuxièmement, il veut se diversifier de façon à ce que leurs importations d'énergie par voie maritime ne se limitent pas à un ou deux points de passage obligé, par exemple, comme le détroit de Malacca, où il pourrait faire l'objet d'une interdiction, ce qui est une des raisons qui expliquent la complexité des politiques énergétiques avec l'Asie centrale.

Le sénateur Mitchell : Les États-Unis ont un intérêt dans cette relation avec CNOOC. En fait, j'ai lu aujourd'hui que le sénateur McCain a laissé entendre que le Parlement du Canada devrait étudier la question attentivement. En réalité, la question est de savoir à quel point ils y tiennent et de savoir quelle incidence cela aura sur notre relation avec eux.

Mr. Boutilier: This is straying a long way from maritime issues, I have to confess, but I think there are arguments in some quarters that the Chinese will not forget if we do not embrace their offers. However, these are the hard challenges of the marketplace, I think. I know that other nations, like Australia, are also subject to overtures, although I think probably in broad terms the Chinese have made more headway in Australia in mining and energy than elsewhere.

The Chair: Thank you for keeping that brief and getting us back on focus.

Senator Lang: I will turn back to the maritime issues and the navy and the size of our navy. I am not clear in your presentation here just exactly where you are recommending that the Royal Canadian Navy go in respect of their fleet and what they have. As you know, the government has made a major commitment to revitalize the navy and is in the process of putting that in place.

Taking it from that point of view, are you satisfied that, within the limits of our financial capabilities, we are going in the right direction?

Second, with the four submarines we have, in conjunction with the other 196 or 200 that are in the Pacific, will that suffice from our point of view as a country in the contribution and trying to maintain a presence? In particular, you have referred to the Chinese as a threat a number of times during your presentation. Maybe you would comment on that.

Mr. Boutilier: Once again, I think this is really the province of the commander of the navy. What I would suggest, however, is that our submarines can be seen within the larger context of an arena in which submarines are becoming increasingly prevalent. The fact is that virtually all the nations of the world in that region are moving into the submarine realm. Even Singapore, which has a population equal to metro Toronto, has missile boats, frigates, corvettes and submarines. It also has a budget too large to spend in defence.

If you look at the highly aspirational and ambitious defence plans in Australia, for example, we see that their intention is to increase their number of submarines from 6 to 12. A whole host of issues have affected the Collins Class in Australia, whether it is the availability of crews or technical challenges and so forth. It is a measure of how Canberra sees the nature of the maritime threat that one of the principal areas in which they want to move is to increase submarine capability.

Submarines, I think, will be increasingly part of the currency of the region. I know that in the case of the United States Navy they leased from Sweden a boat and its entire crew to operate on the California coast to begin to give the United States Navy — this was some years ago — experience in anti-submarine warfare. This is a particularly challenging issue.

M. Boutilier : Je dois admettre que l'on se donne beaucoup des questions maritimes, mais je pense que dans certains milieux, on laisse entendre que les Chinois n'oublieront pas si nous n'acceptons pas leurs offres. Toutefois, je pense que ce sont là les conditions difficiles du marché. Je sais que d'autres pays, comme l'Australie, font aussi l'objet de cette ouverture, même si je pense qu'en général, les Chinois ont probablement mieux progressé dans les secteurs minier et énergétique de l'Australie que n'importe où ailleurs.

La présidente : Merci d'avoir été bref et d'avoir recentré la discussion.

Le sénateur Lang : Je vais revenir aux questions maritimes, à la marine et à la taille de notre marine. Je ne suis pas certain de savoir exactement quelles sont, dans votre exposé, vos recommandations quant à ce que la Marine royale canadienne devrait faire en ce qui concerne sa flotte et ce dont elle dispose. Comme vous le savez, le gouvernement s'est engagé formellement à moderniser la marine et s'emploie activement à le faire.

Partant de ce point de vue, avez-vous l'impression que, dans les limites de notre capacité financière, nous allons dans la bonne direction?

Deuxièmement, avec nos quatre sous-marins, en plus des quelque 196 ou 200 autres sous-marins présents dans le Pacifique, cela sera-t-il suffisant pour nous permettre d'apporter notre contribution en tant que pays et d'essayer de maintenir une présence? Je pense en particulier au fait que vous avez parlé des Chinois comme d'une menace plusieurs fois pendant votre exposé. Quels sont vos commentaires à cet égard?

M. Boutilier : Encore une fois, je pense que cela concerne davantage le commandant de la marine. Cependant, je dirais que nos sous-marins peuvent être considérés comme faisant partie du contexte plus large d'un théâtre où les sous-marins jouent un rôle de plus en plus prépondérant. Le fait est que presque tous les pays de cette région se tournent vers les sous-marins. Même Singapour, dont la population équivaut à celle du Grand Toronto, à des navires équipés de missiles, des régates, des corvettes et des sous-marins. Il dispose aussi d'un budget de défense très important.

Lorsqu'on regarde les plans de défense très ambitieux de l'Australie, par exemple, on constate que l'intention des Australiens est d'augmenter le nombre de sous-marins de six à 12. En Australie, les sous-marins de classe Collins ont été touchés par une série de problèmes : disponibilité des équipages, problèmes techniques, et cetera. Le fait qu'une des principales mesures que souhaite adopter l'Australie est d'augmenter le nombre de sous-marins est représentatif de la façon dont Canberra perçoit la nature de la menace maritime.

Je pense que les sous-marins feront de plus en plus partie de la donne dans la région. Je sais que la marine américaine a eu recours aux services d'un navire suédois et de son équipage. L'objectif était de procéder à des exercices le long de la côte de la Californie pour permettre à la marine américaine — c'était il y a quelques années — d'acquérir de l'expérience dans le domaine de la guerre anti-sous-marine. C'est un problème particulièrement difficile.

It is also interesting to see that the Russians, who have some major ambitions in revitalizing their aging fleet, are beginning to move some of their newer generation of boats into the Pacific. Originally, if we were to go back 10 years, they were all to be in the White Sea in the northwestern corner of Russia. Suffice to say, I am sure all commanders would like to have more assets. Within that context, submarines, I think, will be very important.

My general thrust to you all is that in this maritime century navies are going to be critical in advancing the interests of the nations of the region.

Senator Nolin: Thank you, professor, for coming to Ottawa.

Mr. Boutilier: I am flattered.

Senator Nolin: After hearing you in Esquimalt and here, I think it is great.

Canada's interest in trade in the Pacific is no secret. What about the defence alliances? I do not know whether you have written publicly on the subject. I would be interested if you have. What are your views on Canada's interests in developing an alliance, multilateral alliances, similar to what we have in the Atlantic or the Pacific? Should we go bilateral only?

Mr. Boutilier: As I suggested, one of the challenges in the region is there is no equivalent to NATO. There is no framework into which we can plug in terms of our larger effort. I would suggest to you that, over the past 10 years, there has been a compelling shift in attitudes. Whereas, perhaps in the 1990s, we saw it as a uni-polar world with the Americans taking the lead, now our American colleagues are increasingly forthright and candid about the fact that no nation can do it on their own.

If we go back some five or six years, we see the thousand-ship navy concept, which was really a mythological concept. What it did was to place a premium on cooperation. Americans are particularly eager to cooperate with like-minded nations in the region. One of the things that facilitates that, to some degree, is that nations like Japan and South Korea all have, as a common denominator, close association with the United States Navy, for example, over many decades. Thus we find that Australians, New Zealanders, increasingly Singaporeans, Japanese, South Koreans, Canadians, all have some degree of commonality by virtue of having worked closely with the United States Navy.

Il est aussi intéressant de voir que les Russes, qui ont de grandes ambitions en ce qui concerne la modernisation de leur flotte vieillissante, commencent à déplacer vers le Pacifique une partie de leur navire de nouvelle génération. À l'origine, si l'on remonte de 10 ans, tous les navires devaient être déployés dans la mer Blanche, à la pointe nord-ouest de la Russie. Je dirai simplement que je suis certain que tous les commandants aimeraient avoir plus de ressources. Dans ce contexte, les sous-marins seront très importants, à mon avis.

Le message général que je veux vous transmettre, c'est qu'en ce siècle maritime, la marine sera essentielle à la promotion des intérêts des pays de la région.

Le sénateur Nolin : Merci d'être venu à Ottawa, monsieur.

M. Boutilier : C'est un honneur d'être ici.

Le sénateur Nolin : Après vous avoir entendu ici et à Esquimalt, je pense que c'est formidable.

L'intérêt que porte le Canada pour le commerce dans la région du Pacifique n'est pas un secret. Qu'en est-il des alliances de défense? Je ne sais pas si vous avez publié quelque chose ce sujet. Si oui, j'aimerais le lire. À votre avis, dans quelle mesure le Canada a-t-il intérêt à créer une alliance, des alliances multilatérales semblables à ce que nous avons du côté de l'Atlantique ou du Pacifique? Devrions-nous opter seulement pour des alliances bilatérales?

M. Boutilier : Comme je l'ai indiqué, un des problèmes dans la région, ce qui n'a pas d'équivalent à l'OTAN. Il n'y a aucun cadre dans lequel nous pouvons intégrer notre effort global. Je vous dirais qu'au cours des 10 dernières années, il y a eu un changement fondamental des mentalités. Alors qu'auparavant — dans les années 1990, peut-être — nous considérions cela comme un monde unipolaire où les Américains étaient le chef de file, nous constatons maintenant que nos collègues américains font de plus en plus preuve d'ouverture et de candeur quant au fait qu'aucun pays ne peut agir seul.

Si nous retournons en arrière de cinq ou six ans, il y avait le concept des 1 000 navires, qui était plutôt un mythe. En conséquence, on accordait une grande importance à la coopération. Les Américains cherchent surtout à collaborer avec les pays de la région aux vues similaires. Un des éléments qui favorisent cette collaboration, à un certain point, c'est que des pays comme le Japon et la Corée du Sud ont comme dénominateur commun des relations étroites avec la marine américaine, par exemple, et ce, depuis plusieurs décennies. Par conséquent, on constate que les Australiens, les Néo-Zélandais, les Singapouriens — de plus en plus —, les Japonais, les Sud-Coréens et les Canadiens ont dans une certaine mesure des points en commun du fait qu'ils ont travaillé en étroite collaboration avec la marine américaine.

I think Americans would argue, among other things, maintaining peace and stability at sea, addressing an increasing array of challenges like humanitarian assistance and disaster relief in the region, all place a premium on naval collaboration.

I wrote a piece recently, which I anticipate NATO will publish, arguing that cooperation at sea is perhaps one of the ways we can begin to build relationships in East Asia. Of course, the beauty of naval cooperation is that it is — not to put too fine a point on it — out of sight, out of mind. It is not a contentious issue in the sense that land-based operations or exercises are. One can make an argument that there are many issues, whether it is fisheries patrols or search and rescue or humanitarian assistance, as illustrated in the great Indonesian tsunami of 2004, where navies should work together.

Indeed, we have begun to get some movement in that arena with the serendipitous collaboration of an amazing array of vessels off the Horn of Africa in anti-piracy operations. Thus we find Chinese, American, Russian, Singaporean vessels all interacting. The levels of interaction are pretty minimal, to say the least, but it is a start. I have argued that I think we should do everything we can to try to foster greater confidence building and collaboration at sea involving the navies of the region.

I do not see formal alliances appearing at sea any time in the future, but I certainly see that the whole trend in senior naval thinking across the region is to place a premium on collaboration and cooperation.

Senator Nolin: You said you wrote a piece and that NATO will publish it?

Mr. Boutilier: Yes. I was invited by the NATO Defense College to write a piece. They produce a regular series of opinion pieces. One issue that confronts NATO, not to put too fine a point on it, is what is the future of NATO after Afghanistan. Is there a future in Asia? The fact that NATO is in Afghanistan would have been, in the early 1990s, absolutely, utterly unthinkable, but now we see a situation where NATO is looking to recreate itself.

Recently I was in Rome lecturing to an audience of generals, flag officers and ambassadors, and much to my delight, in the audience was a Chinese rear admiral. This is an initiative on the part of the NATO Defense College to reach out, as they have already done to Australians and Japanese and others, the so-called NATO contact nations in Asia, to China. It is very much a work-in-progress, but it seems to me that maritime cooperation

Je pense que les Américains feraient notamment valoir que le maintien de la paix et de la stabilité en mer de même que les opérations visant à régler un nombre croissant de problèmes dans la région — comme l'aide humanitaire et les secours en cas de catastrophe — sont des facteurs qui soulignent l'importance de la collaboration des forces navales.

Récemment, j'ai écrit un article qui sera publié par l'OTAN, je crois, dans lequel je soutenais que la coopération en mer est peut-être pour nous l'une des façons de commencer à établir des relations en Extrême-Orient. Bien entendu, la beauté de la coopération navale, c'est qu'elle est loin des yeux, loin du coeur, pour dire les choses comme elles sont. Ce n'est pas une question controversée comme le sont les opérations ou les exercices terrestres. On peut faire valoir qu'il y a beaucoup de situations dans lesquelles les forces navales devraient collaborer : patrouilles de surveillance des pêches, missions de recherche et de sauvetage ou missions de l'humanitaire. À titre d'exemple, il y a le terrible tsunami en Indonésie, en 2004.

Nous avons en effet commencé à voir une évolution en ce sens avec l'extraordinaire collaboration d'un éventail étonnant de navires au large de la Corne de l'Afrique dans le cadre d'opérations de lutte contre la piraterie. On voit donc une interaction entre des navires chinois, américains, russes et singapouriens. Le niveau d'interaction est plutôt minime, c'est le moins qu'on puisse dire, mais c'est un début. J'ai indiqué que nous devrions faire tout notre possible pour essayer de favoriser, chez les forces navales de la région, une augmentation de la confiance et une meilleure collaboration en mer.

Je ne crois pas que nous verrons un jour la création d'alliances officielles entre des forces navales, mais je constate certainement que dans la région, les officiers supérieurs des forces navales de la région tendent à accorder une grande place à la collaboration et à la coopération.

Le sénateur Nolin : Vous avez dit que vous avez écrit un article et que l'OTAN va le publier?

M. Boutilier : Oui. Le Collège de défense de l'OTAN m'a invité à écrire un article. Il publie régulièrement une série d'articles d'opinion. Un des problèmes auxquels est confrontée l'OTAN, sans insister davantage sur cet aspect, c'est de savoir quel est l'avenir de l'OTAN après l'Afghanistan. A-t-elle un avenir en Asie? Au début des années 1990, une intervention de l'OTAN en Afghanistan aurait été tout à fait impensable, mais nous voyons actuellement une situation où l'OTAN cherche à se réinventer.

Récemment, je suis allé à Rome pour prononcer un discours devant un auditoire composé de généraux, d'officiers généraux et d'ambassadeurs et, à ma grande surprise, un contre-amiral chinois était dans la salle. Il s'agit d'une initiative du Collège de défense de l'OTAN visant à établir des liens avec ce qu'on appelle les pays de contact de l'OTAN en Asie, avec la Chine, comme cela a été fait avec l'Australie et le Japon, notamment. Essentiellement, il

is one of the most promising arenas in which to begin building, softly, softly, a greater sense of community at sea.

The Chair: On that note, are there any other structures? There are lots of Asian trade organizations. Is there any structure? Is RIMPAC actually a structure?

Mr. Boutilier: It is in the sense that it remains a work-in-progress. No sooner has this year's RIMPAC come to an end than they are planning the next one. One structure you may not have encountered in your work is the Western Pacific Naval Symposium. Canada is a full member of that symposium. This brings together the heads of almost all the major navies in the Pacific Ocean. There is an Indian Ocean subset or equivalent, in a way, but this gives a real opportunity for heads of navies to interact, and they are, for example, trying to look at ways to avoid the unpleasant circumstances associated with unexpected encounters or collisions at sea, the sort of thing they did during the Cold War with the Incidents at Sea Agreement with the Soviets. They are also looking at basic, low-level communications documents that would give Western Pacific naval fleets, whether it is China, Australia or Chile, interoperability. Of course, we have had documents of this sort in NATO for decades. The WPNS, as it is called, Western Pacific Naval Symposium, I think is quite promising as a launch point for greater cooperation at sea.

The Chair: We have gone over our time, but I appreciate all of the information you have managed to cram into that brief time. I think we are all better for it. Thank you, Dr. Boutilier, for making this trip and joining us today.

Mr. Boutilier: I am delighted to support you and happy to do so on any other occasion.

The Chair: Thank you so much. We will officially adjourn our meeting.

(The committee adjourned.)

s'agit de quelque chose qui est en cours, mais il me semble que la coopération maritime est l'un des théâtres les plus prometteurs pour commencer à bâtir — doucement, lentement — un esprit communautaire en mer.

La présidente : Cela dit, y a-t-il d'autres structures? Il existe en Asie beaucoup d'organisations commerciales. Y a-t-il des structures? Le RIMPAC est-il une structure?

M. Boutilier : Ce l'est, en ce sens qu'il demeure un exercice en évolution. Dès la fin du RIMPAC de cette année, on a commencé à planifier les prochains. Dans vos travaux, vous n'avez peut-être pas entendu parler d'une structure qui s'appelle le Symposium naval du Pacifique occidental. Le Canada en est membre. On y réunit les dirigeants de presque toutes les forces navales principales de l'océan Pacifique. Il a son pendant ou son équivalent pour l'océan Indien, en quelque sorte. Il offre aux dirigeants des forces navales une véritable occasion d'interagir. On essaie, par exemple, de trouver des façons d'éviter des situations déplaisantes liées à des rencontres imprévues ou des collisions en mer, un peu comme on le faisait pendant la guerre froide dans le cadre du protocole sur les incidents en mer qui a été signé avec les Soviétiques. On se penche aussi sur des documents de communication de base qui permettraient l'interopérabilité des flottes de navires du Pacifique occidental, qu'il s'agisse de la Chine, de l'Australie ou du Chili. Bien entendu, des documents de ce genre existent à l'OTAN depuis des décennies. Le Symposium naval du Pacifique occidental — le WPNS, comme on l'appelle — est, à mon avis, un point de départ plutôt prometteur pour ce qui est d'une plus grande collaboration en mer.

La présidente : Nous avons dépassé le temps imparti, mais je vous remercie de toutes les informations que vous avez réussi à nous fournir pendant ce court moment. Je pense que cela nous sera tous très utile. Monsieur Boutilier, merci d'avoir fait le voyage et de vous être joint à nous aujourd'hui.

M. Boutilier : Je suis heureux de vous aider et c'est avec plaisir que je le ferai à tout autre moment.

La présidente : Merci beaucoup. La séance est levée.

(La séance est levée.)

WITNESSES

Monday, November 5, 2012

National Defence:

Brigadier-General Greg Loos, Director General Cyber, Chief of Force Development;

Brigadier-General Roberto Mazzolin, Director General, Information Management Operations;

Communications Security Establishment Canada:

John Forster, Chief;

Toni Moffa, Deputy Chief, IT Security.

Monday November 19, 2012

National Defence:

Brigadier-General Rick Pitre, Director General Space;

Colonel André Dupuis, Director of Space Requirements.

As an individual:

James A. Boutilier, Professor, Centre for Asia-Pacific Initiatives, University of Victoria, Special Advisor (Policy) at the Maritime Forces Pacific.

TÉMOINS

Le lundi 5 novembre 2012

Défense nationale :

Brigadier-général Greg Loos, directeur général, Cybersécurité, chef, Développement des forces;

Brigadier-général, Roberto Mazzolin, directeur général, Opérations de la gestion de l'information.

Centre de la sécurité des télécommunications Canada :

John Forster, chef;

Toni Moffa, chef adjointe, Sécurité des TI.

Le lundi 19 novembre 2012

Défense nationale :

Brigadier-général Rick Pitre, directeur général, Espace;

Colonel André Dupuis, directeur du développement de l'espace.

À titre personnel :

James A. Boutilier, professeur, Centre for Asia-Pacific Initiatives, Université de Victoria, conseiller spécial (politiques) auprès des Forces maritimes du Pacifique.