TRANSMITTAL SLIP / NOTE D'ENVOI

To / À	Classification
Director	**Unclassified**
From / De	File / Dossier
ADP	900-6-1 (HoC Committees)
Drafting officer / Rédacteur	Date
Policy Coordination	2016 09 30

Subject / Sujet

Director's Appearance at SECU (National Security Framework)

Action / Donnez suite	Priority / Priorité	Deadline / Délai
❑ Signature ❑ Comments / Commentaires X Approval / Approbation ❑ Information	❑ Routine X Urgent ❑ Immediate / Immédiate	**2016 09 30**

Record of Consultation/Approval Rapport de consultation/d'approbation	Consulted Consulter	Concur D'accord		Comments / Commentaires
		Yes Oui	No Non	
Chief, **DG PFR**				Please find enclosed the draft Table of Contents for your briefing binder in support of your appearance at the Standing Committee on Public Safety and National Security and Defence (SECU) on **2016 010 06 from 3:30- 5:30.** The appearance will last two hours. The Minister will appear for the first hour, with you and officials from the RCMP and Public Safety. You and the other representatives will remain at the table to answer questions for the second hour. No opening remarks are required. The briefing binder will be delivered by noon **2016 10 04**.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

HOUSE OF COMMONS STANDING COMMITTEE ON PUBLIC SAFETY AND NATIONAL SECURITY (SECU)

6 October 2016, 3:30-5:30

TABLE OF CONTENTS

TAB 1 - **Hot Issues:**

- Information Sharing with GAC
- Number of TRA Measures to Date
- Number of Travelers
- Recent NS Incident
- Human Rights and Information Sharing
- AEN

TAB 2 - **Issue Notes:**

A. National Security Consultations
B. NS Framework
- CSIS' Role
- CSIS' Cooperation with Domestic Partners
- CSIS' Cooperation with Foreign Partners
- Operational cooperation

C. Threat Reduction
- Implementation
- Number of Measures to Date
- Safeguards
- Cooperation with Partners (RCMP, GAC, CSE)
- Warranted Measures
- Non-Warranted Threat Reduction Activities
- Examples of Warranted Activities

D. Countering Radicalization to Violence
- Preventing Radicalization
- Office of Community Outreach and Counter-Radicalization Coordinator

E. Security of Canada Information Sharing Act (SCISA)
- Definitions and Thresholds (SCISA, CSIS Act)
- Safeguards and Accountability
- Implementation
- Experience to date

F. Secure Air Travel Act (SATA)
- CSIS Nominations

G. Accountability
- Relationship with SIRC
- Committee of Parliamentarians
- Allied Countries
- Judicial Authorization
- Inter-Agency Review

H. Lawful Access (Going Dark)
- Impact of "Going Dark"
- Relationship with CSP
- Data Retention
- Encrytption

I. Intelligence as Evidence
- Existing Authorities to Protect Sensitive Information

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

J. SIRC Annual Report 2015-2016
- Certification/Compliance
- Threat Reduction Mandate
- Canadian Revenue Agency
- Dataset Acquisition
- Foreign Fighter Investigation
- Ministerial Notification

K. Terrorism
- Numbers
- Returnees
- Public Threat Report
- Threat Level
- Travel Numbers
- Recent NS Incidents

L. Espionage, Foreign Interference
- Foreign investment
- Foreign Influence
- Insider Threat

M. Cyber Security
- NS Framework – Cyber
- TRA and Offensive Cyber Operations
- Cyber Review

N. Proliferation

O. Foreign Cooperation and Information Sharing
- Ministerial Direction on Information Sharing
- Operations Abroad
- Arrangements with foreign partners
- Implementation of Ministerial Direction

TAB 3 - **CSIS Overview:**

P. CSIS Mandate
- Collect/Investigate/Advise, s.12
- Threat Reduction, s.12.1
- Threats to security of Canada, s.2
- Security Screening, ss.13-15
- Foreign Intelligence, s.16

Q. CSIS Today
- Demographics
- Regional Presence

TAB 4 - **Recent Media Coverage and Trends**

TAB 5 - **Previous Testimony**

R. SECU, 2016 02 23, (TRA and SCISA flagged)
S. Written Response to SECU follow-up on SCISA
T. SECD, 2016 03 07, (TRA flagged)
U. SECU, 2016 03 08, (Supplementary Estimates C)

TAB 6 - **SECU Membership (PS)**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

TRANSMITTAL SLIP / NOTE D'ENVOI

To / À	Classification
Director	**UNCLAS**
From / De	File / Dossier
ADP	900-6-1 (HoC Committees)
Drafting officer / Rédacteur	Date
	2016 10 03

Subject / Sujet

Director's Appearance at SECU: National Security Framework/Green Paper Consultations

Action / Donnez suite	Priority / Priorité	Deadline / Délai
❑ Signature ❑ Comments / Commentaires X Approval / Approbation ❑ Information	❑ Routine X Urgent ❑ Immediate / Immédiate	**2016 10 04 (Noon)**

Record of Consultation/Approval Rapport de consultation/d'approbation	Consulted Consulter	Concur D'accord		Comments / Commentaires
		Yes Oui	No Non	
Chief, **DG PFR**		X		Please find enclosed the briefing binder in support of your appearance, in support of the Minister at the Standing Committee on Public Safety and National Security and Defence (SECU) on **2016 010 06 from 3:30- 5:30** to discuss its study on "Canada's National Security Framework/Green Paper Consultations". The appearance will last two hours. The Minister will appear for the first hour, with you and officials from the RCMP and Public Safety. You and the other representatives will remain at the table to answer questions for the second hour. No opening remarks are required.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

Hot Issues

ISSUE: Has SCISA expanded the scope of information it can collect from Global Affairs Canada? Has CSIS engaged in TRA? How and against what threats? How many Canadians abroad are engaged in terrorist activity? How does CSIS assess human rights issues with respect to its relationships with foreign agencies?

IF PRESSED ON INFORMATION SHARING WITH GLOBAL AFFAIRS CANADA

- **CSIS and Global Affairs Canada have distinct mandates. We report to different Ministers and have our own legislative authorities. Both, however, perform vital functions and work together as appropriate, to protect Canadians and Canada's national interests.**

- **Global Affairs Canada may share information with CSIS, both *proactively* and in response to requests, in accordance with the authorities in SCISA.**

- **This does not, however, in any way expand the Service's authority to collect information. Indeed, the Service must continue to ensure that any information it collects is "strictly necessary" for the purposes of investigating threats to the security of Canada.**

- **Further, nothing in SCISA compels information sharing with CSIS. Global Affairs Canada is responsible for determining whether information may be shared.**

- **CSIS and Global Affairs Canada have established an arrangement that governs the sharing of consular information. The arrangement was established to ensure that the requirements of both parties are clear and that any sharing is done in strict accordance with relevant Canadian legislation and Ministerial Direction.**

- **For example, there could be instances where Global Affairs Canada has obtained threat-related information from an individual seeking consular assistance, particularly in areas that are close to conflict zones. If Global Affairs Canada views the information as relevant to CSIS' mandate, it may decide to proactively share it with CSIS using SCISA.**

IF PRESSED ON THE NUMBER OF TRA MEASURES TAKEN TO DATE

- **The Service has issued some two dozen approvals for threat diminishment measures since the mandate came into effect.**
- **The Service is gaining experience every day in identifying and developing these measures, and assessing their risks and impacts.**

IF PRESSED ON NUMBERS OF TRAVELERS

- **There are approximately 180 individuals abroad for terrorism-related purposes.**
- **Of the approximately 180 travelers, around half were last identified in Turkey, Syria or Iraq. Many extremists groups operating in the region freely traverse between Syria and Iraq; an individual known to be in Syria one day might be in Iraq the next.**
- **I must state that this number also includes individuals who are believed, or suspected, to have died while abroad.**
- **As previously stated, there is not a lot to be gained by reporting frequently on incremental changes in these numbers, which fluctuate constantly.**
- **Nor do numbers of 'travelers' or 'returnees' adequately capture the scale of this threat: individuals who have never travelled – whether they aspire to, have been prevented from travelling or, for a variety of reasons, choose to remain in Canada – and are engaged in threat-related activities at home are not included.**
- **I will remind you, members, that Aaron Driver was a thwarted traveller who was prevented from going abroad.**
- **I should point out that that we remain concerned about the number of individuals that we are not aware of, or about whom we have incomplete information, due to the significant operational challenges associated with such investigations.**

IF PRESSED ON THE AUGUST 10TH AARON DRIVER INCIDENT

- **The Service closely engages with Canadian and international partners in relation to urgent matters of national security.**
- **The incident in Strathroy, Ontario, demonstrates the importance of close collaboration between international and domestic partners.**

- **Ongoing communication and deconfliction between the Service, RCMP and FBI throughout the incident prevented lives being lost.**
- **The Aaron Driver case also highlights the threat of frustrated travellers who turn their attention to conducting attacks domestically.**

IF PRESSED ON HUMAN RIGHTS AND INFORMATION SHARING

- **CSIS opposes in the strongest possible terms the mistreatment of any individual by a foreign agency, and in all situations, we must and do comply with Canada's laws and legal obligations in sharing information with foreign entities.**

- **The human rights reputations of the agencies with which CSIS engages is not something which the Service takes lightly. CSIS must assess and mitigate potential risks of sharing information with foreign entities, always cognizant of the fact that our first responsibility is to the Canadian people and their safety.**

- **CSIS continuously assesses all of its foreign arrangements, including human rights reputations of the country, and more specifically, of the agency with which it has established such arrangements.**

- **As part of this assessment process, CSIS regularly reviews various government and non-government human rights reports and assessments for all countries with which the Service has implemented Ministerially-approved arrangements. We also liaise with allied foreign counterparts in support of such assessments.**

- **In addition to specific protocols for information sharing, the way in which we establish and manage foreign arrangements is designed to mitigate risk.**

IF PRESSED ON ALMALKI, ELMAATI AND NUREDDIN (AEN)

- **The actions of Canadian officials in relation to AEN's detention and mistreatment overseas were the subject of a Commission of Inquiry.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **In 2008, the Commissioner concluded that certain actions by the Service and other departments had indirectly contributed to AEN's detention and mistreatment overseas. Good-faith efforts in exceptionally difficult circumstances were, in some instances, found to be deficient.**

- **I can assure you that CSIS has taken the recommendations from this Commission of Inquiry and modified its governance surrounding information sharing with foreign partners accordingly. SIRC has commented positively on what we have put in place, and on our decision-making in relation to foreign information sharing.**

- **The civil cases between AEN and the Government are a matter before the Courts. To maintain the integrity of the judicial process, I will refrain from commenting any further on this issue.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

Hot Issues

IF PRESSED ON THE EFFECTIVENESS OF PROVISIONS IN BILL C-51

- **The authorities provided for in Bill C-51 have indeed helped the Service investigate and reduce threats to the security of Canada.**
- **Today's threat environment is diffuse, fast, connected and sophisticated. CSIS must rely on the full range of authorities available, including cooperation with domestic and foreign partners, to detect and address threats to the security of Canada.**
- **The Service has taken threat reduction measures on about two dozen occasions since the mandate came into effect. These have both directly and indirectly reduced threats to the security of Canada.**
- **Dealing with emerging threats early on allows us to focus resources on more advanced and imminent threats.**
- **As it relates to information sharing, SCISA provides a clear lawful authority to share information for national security purposes.**
- **Generally, CSIS has observed an increase in proactive disclosures of threat-related information to CSIS, all of which has been shared in accordance with the provisions in SCISA. In all cases, the information was determined to be directly relevant to threat related investigations.**

IF PRESSED ON WHETHER C-51 HAS "PREVENTED" ATTACKS

- **Attacks are prevented by a very wide range of capabilities and authorities, across the Government of Canada, most of which have nothing to do with Bill C-51. C-51 has added some valuable tools to that toolkit.**
- **But the Service has employed its TRA mandate against the terrorist threat to Canada by, for example, taking measures to reduce certain threat actors' access to finances, material and online propaganda that promote and enable terrorist activity.**
- **Nor is the Service's TRA mandate only employed against the terrorist**

threat to Canada; it can be used against all the threats defined in the *CSIS Act*.

IF PRESSED ON INFORMATION SHARING WITH GLOBAL AFFAIRS CANADA

- Global Affairs Canada may share information with CSIS, both *proactively* and in response to requests, in accordance with the authorities in SCISA. This does not, however, in any way expand the Service's authority to collect information. CSIS must continue to ensure that any information it collects is "strictly necessary" for the purposes of investigating threats to the security of Canada.



- Further, nothing in SCISA compels information sharing with CSIS. Global Affairs Canada is responsible for determining whether information may be shared.



- We have established an arrangement that governs the sharing of consular information to ensure any sharing is done in strict accordance with the law and Ministerial Direction.

- For example, there could be instances where Global Affairs Canada has obtained threat-related information from an individual seeking consular assistance, particularly in areas that are close to conflict zones. If Global Affairs Canada views the information as relevant to CSIS' mandate, it may decide to proactively share it with CSIS using SCISA.

IF PRESSED ON NUMBERS OF TRAVELERS

- There are approximately 180 individuals with a nexus to Canada abroad for terrorism-related purposes. Around half of these were last identified in Turkey, Syria or Iraq. I must state that this number also includes individuals who are believed, or suspected, to have died while abroad.

- As previously stated, there is not a lot to be gained by reporting frequently on incremental changes in these numbers, which fluctuate constantly.

- **Numbers of 'travelers' or 'returnees' do not adequately capture the scale of this threat: individuals who have never travelled still may pose a threat. I will remind you, members, that Aaron Driver was a thwarted traveller who was prevented from going abroad.**
- **I should point out that that we remain concerned about the number of individuals that we are not aware of, or about whom we have incomplete information, due to the significant operational challenges associated with such investigations.**

IF PRESSED ON THE AUGUST 10TH AARON DRIVER INCIDENT

- **The Service closely engages with Canadian and international partners in relation to urgent matters of national security.**
- **The incident in Strathroy, Ontario, demonstrates the importance of close collaboration between international and domestic partners.**
- **Ongoing communication and deconfliction between the Service, RCMP and FBI throughout the incident prevented more lives being lost.**

IF PRESSED ON HUMAN RIGHTS AND INFORMATION SHARING

- **CSIS opposes in the strongest possible terms the mistreatment of any individual by a foreign agency, and in all situations, we must and do comply with Canada's laws and legal obligations in sharing information with foreign entities.**
- **The human rights reputations of the agencies with which CSIS engages is not something which the Service takes lightly. CSIS must assess and mitigate potential risks of sharing information with foreign entities, always cognizant of the fact that our first responsibility is to the Canadian people and their safety.**
- **CSIS continuously assesses all of its foreign arrangements, including human rights reputations of the country, and more specifically, of the agency with which it has established such arrangements.**
- **As part of this assessment process, CSIS regularly reviews various**

government and non-government human rights reports and assessments for all countries with which the Service has implemented Ministerially-approved arrangements. We also liaise with allied foreign counterparts in support of such assessments.

- In addition to specific protocols for information sharing, the way in which we establish and manage foreign arrangements is designed to mitigate risk.

IF PRESSED ON MINISTERIAL DIRECTION

- Ministerial Direction clearly states that in sharing information, CSIS must act in a manner that complies with Canada's laws and legal obligations and avoid complicity in mistreatment by foreign entities.

- To do so, CSIS must assess and mitigate potential risks of sharing with foreign entities, as well as the accuracy and reliability of information received.

- We have very specific direction in place to do so, supported by a detailed decision-making process, supported by a senior-level committee that is convened as required. In this year's report, SIRC found the range of participants around the table fostered substantive discussion and provided for a rigorous decision-making process.

- There are also clear requirements to refer such decisions to me if the Committee determines that there is a substantial risk and there is a serious threat of loss of life or injury. These cases are exceptionally rare.

- Exchanges with foreign agencies are also incremental in nature, in order to gauge the reliability of the agency and the usefulness of such an arrangement. Exchanges are also commensurate with the degree of trust established over a period of time and reflective of the political and human rights climate within the country in question.

- That said, if CSIS received information indicating Canadian lives may be at risk, we would be negligent not to assess and attempt to corroborate it in order to prevent a direct and timely security threat,

such as terrorist attack, against Canada or its interests regardless of the information's origins.

IF PRESSED ON ALMALKI, ELMAATI AND NUREDDIN (AEN)

- **The actions of Canadian officials in relation to AEN's detention and mistreatment overseas were the subject of a Commission of Inquiry.**

- **In 2008, the Commissioner concluded that certain actions by the Service and other departments had indirectly contributed to AEN's detention and mistreatment overseas. Good-faith efforts in exceptionally difficult circumstances were, in some instances, found to be deficient.**

- **I can assure you that CSIS has taken the recommendations from this Commission of Inquiry and modified its governance surrounding information sharing with foreign partners accordingly. SIRC has commented positively on what we have put in place, and on our decision-making in relation to foreign information sharing.**

- **The civil cases between AEN and the Government are a matter before the Courts. To maintain the integrity of the judicial process, I will refrain from commenting any further on this issue.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

National Security Consultations

ISSUE: What is the Service's position regarding national security consultations? What are the Service's views on the issues: CSIS threat reduction: SCISA, SATA, Radicalization, Going Dark, Intelligence as Evidence, Terrorist Financing, and Listings?

- **The Government has launched consultations on a wide range of national security issues.**
- **Many of the questions at issue have a direct impact on CSIS operations and, in some cases, the manner in which we fulfill our mandate.**
- **These are important questions and informed public debate is essential.**
- **Though these are rightly a question for the public and Parliament to consider, we welcome the discussion and the opportunity to hear form Canadians on these important issues, many of which are at the heart of what we do.**
- **CSIS remains prepare to support this process, as appropriate, and I am pleased to be here today to answer questions about how we work within the current national security framework.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

NATIONAL SECURITY FRAMEWORK

ISSUE: What is CSIS' role in the national security community? How does CSIS cooperate with domestic and international partners? Is the Service's operational cooperation with partners guided by frameworks or internal policies?

- **CSIS is dedicated to the safety of Canadians and the protection of Canada's national security – a mission that is clearly articulated in our legislation.**
- **Everything we do is anchored in the *CSIS Act*, which sets out clear requirements for the conduct of our operations to investigate and respond to threats.**
- **We are, however, but one element of the broader national security community. This is recognized in our Act, which authorizes the Service to cooperate with domestic and foreign partners.**
- **In fulfilling our respective mandates, each partner has an essential role to play, but cooperation is critical at all phases – investigation, assessment and response.**

IF PRESSED ON CSIS' ROLE IN NS FRAMEWORK:

- **In order to achieve our mission, to protect public safety, we investigate and respond to threats.**
- **The Service collects vital intelligence through a variety of methods, including the use of specific investigative techniques for which judicial authorization is required, and advises Government on threats to the security of Canada.**
- **CSIS collects information and intelligence to meet Government of Canada intelligence priorities. In so doing, we actively cooperate with partners, both to advance investigations and deconflict operations.**
- **In terms of our response, there are always a range of options to consider, often in consultation with partners.**
- **This can include a decision to investigate further, because we need to know more. Or, it could mean sharing information with partners to inform their lawful investigations or enforcement action (eg, citizenship or immigration decisions, Secure Air Travel Act).**

- **In some cases, it may be most appropriate for us to act directly to reduce threat-related activities.**

- **It is important to note that CSIS is not an enforcement agency. We do not have the authority to arrest or detain individuals, nor do we enforce laws or make administrative decisions.**

IF PRESSED ON CSIS' COOPERATION WITH DOMESTIC PARTNERS:

- **Cooperation with domestic partners is critical to the success of the Service's lawful investigations and also serves to enhance advice provided to Government.**

- **Effective and responsible sharing of information between institutions is critical to our ability to protect Canadians.**

- **CSIS information may provide important insight for domestic partners, just as information lawfully collected by other federal departments may be relevant to active CSIS investigations.**

- **We have worked with domestic partners to develop tailored frameworks for cooperation to inform our operational cooperation, and continue to do so as our relationship and requirements evolve.**

IF PRESSED ON CSIS' COOPERATION WITH FOREIGN PARTNERS:

- **CSIS maintains a well-established network of relationships with partners abroad. These relationships are vital to CSIS operations.**

- **Without such collaboration, particularly from our Five-Eyes partners, Canada would suffer significant intelligence gaps.**

- **CSIS maintains more than 300 relationships with foreign agencies in over 155 countries, each authorized by the Minister.**

- **Through such relationships, CSIS advances its own investigations into threats to the security of Canada and gains a greater understanding of the scope and nature of threats.**

IF PRESSED ON OPERATIONAL COOPERATION:

- **We have a regional presence across Canada and strong working relationships with partners.**

- **We cooperate in a multitude of ways, including through a multi-agency approach.**
- **To that end, CSIS is an active participant in inter-departmental initiatives such as the National Security Joint Operations Centre and RCMP-led Integrated National Security Teams, which seek to enhance the Government's response to threat developments.**
- **Though real-time operational cooperation occurs, CSIS, as well as other involved departments, adhere to their mandate, policies and guidelines.**
- **CSIS also works closely with a number of federal, provincial, municipal and territorial departments and agencies to develop and implement mechanisms to respond to emergency situations, including terrorist incidents.**
- **In other cases, we also cooperate one on one with partners.**
- **As an important example, we routinely work with the RCMP and developed a framework for cooperation referred to as "One Vision."**
- **This framework recognizes our distinct mandates and authorities, and provides clear parameters for an effective working operational relationship.**
- **Of note, it was recently revised to reflect CSIS' threat reduction mandate and establishes an enhanced approach to operational cooperation, which shows the mature relationship between our two organizations.**
- **Though I can confirm that CSIS and RCMP engage regularly at both the executive and working levels to ensure decisions prioritize public safety and the broader public interest, I cannot discuss specific cases.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

THREAT REDUCTION ACTIVITY

ISSUE: Has CSIS engaged in TRA? How and against what threats? What are the safeguards and limitations on CSIS' TRA mandate? How has CSIS implemented this new mandate? How do you ensure that CSIS TRA does not impede RCMP investigations or reduce the likelihood of a prosecution?

- **Today's threats are fast, complex and dynamic, and threat actors are highly connected and mobile.**
- **From an operational perspective, recourse to a flexible range of response options is essential in this threat environment.**
- **In fulfilling its mandate, CSIS has developed unique expertise, capabilities and insight into threats.**
- **We face a vastly different threat environment than in the early 1980s, when the CSIS Act was passed, with terrorism as the most prominent threat. This new threat environment requires a stronger and more flexible response.**
- **Both SIRC and the Senate Committee contemplated this mandate in the past, with SIRC assessing that disruption may at times be necessary to protect Canadians. The Senate Committee reached a similar conclusion and suggested that this authority be clarified.**
-

- **While we always consider the range of possible response options, CSIS has used this new mandate to reduce threats to the security of Canada; always in consultation with domestic partners.**
- **SIRC has expressed its satisfaction with the rigorous governance framework that the Service has implemented to operationalize this new threat reduction mandate.**

IF PRESSED ON IMPLEMENTATION OF TRA

- **The Service has developed a robust governance framework to give effect to the requirements set out in law and Ministerial Direction.**
- **Clear direction has been issued to all employees, complemented by formal training which is mandatory for all operational employees.**
- **A risk assessment is undertaken for each threat reduction measure. CSIS works with the Department of Justice to assess the application of Canadian law, including the Charter, and to determine if a warrant is required.**
- **We also consult with partners, as appropriate, including Global Affairs Canada, the Royal Canadian Mounted Police, and the Communications Security Establishment.**
- **Since the amendments to the CSIS Act came into force in June 2015, the Service has approved a number of measures against a range of threats. None have required a warrant.**

IF PRESSED ON THE NUMBER OF MEASURES TAKEN TO DATE

- **The Service has issued some two dozen approvals for threat diminishment measures since the mandate came into effect.**
- **The Service is gaining experience every day in identifying and developing these measures, and assessing their risks and impacts.**

IF PRESSED ON SAFEGUARDS

- **Whereas we require "reasonable grounds to suspect" to initiate a national security investigation, the law requires that we have "reasonable grounds to believe" that a particular activity constitutes a threat to the security of Canada for threat reduction to be undertaken.**
- **The legislation also requires that threat reduction measures be reasonable and proportionate in the circumstances, having regard to the nature of the threat, the nature of the means to reduce the threat, and the reasonable availability of other means.**
- **Certain conduct is prohibited in all circumstances, including causing physical harm. These prohibitions mirror those applicable to law enforcement [as enshrined in the Criminal Code (s.25)].**

- **The Act also provides for a warrant regime, so that judicial authorization is required for any measure that would otherwise contravene the Charter or be contrary to Canadian law.**
- **In these circumstances, a Federal Court judge - not a CSIS employee - will determine whether the measure represents a reasonable limit on the right or freedom as is required**
- **Threat reduction authorities do not equate to police powers. The power to arrest, detain, and enforce the law remain the purview of our law enforcement partners.**
- **The Act also contains new reporting requirements for CSIS and for the review by the Security Intelligence Review Committee on the conduct of threat reduction.**

IF PRESSED ON COOPERATION WITH PARTNERS

- **As you know, in today's global threat environment, national security is necessarily a team effort – which means that CSIS works with many domestic partners.**
- **We operate to protect Canada and Canadian interests, supporting one another while always respecting our distinct mandates.**
- **We have developed tailor-made frameworks with GAC, CSE and the RCMP, which set out clear direction on how we consult on TRA.**

IF PRESSED ON WARRANTED MEASURES

- **Threat reduction measures must be reasonable and proportionate to the nature of the threat. In some cases, this may include a threat reduction measure that requires a warrant.**
- **The authority to seek a warrant therefore provides flexibility in terms of our operational response.**
- **The authorization framework is tailored to reflect requirements specific to the threat reduction mandate.**
- **The *CSIS Act* clearly identifies when CSIS must seek a warrant to reduce a threat and what conditions must be satisfied for the Court to authorize certain measures.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **CSIS would require Ministerial approval before seeking a warrant.**
- **The requirement to seek judicial authorization will allow a Federal Court judge to determine if a proposed measure contravenes the Charter and, if so, to determine whether the measure represents a reasonable limit on the right or freedom, and is therefore in accordance with the Charter as a whole.**

IF PRESSED ON EXAMPLES OF NON-WARRANTED TRA:

It is possible to generally describe examples of non-warranted TRA but caution must be exercised as each measure would be assessed on its own merits to determine the authorization required.

- **Employing human sources to provide a cautionary voice or counter-narrative**
- **Informing a family member or close friend of a prospective terrorist traveller of the individual's intentions, enabling them to intervene to dissuade the person from travelling**
- **Exposing CSIS' interest through interviews with the person, family members or associates in order to dissuade the person from taking certain actions**
- **Advising a hostile foreign intelligence operative, or informing the contacts of a known hostile foreign intelligence officer, that their affiliation is known to authorities**
- **Reporting social media accounts for violation of terms of use to allow Service providers to choose whether to remove the material.**

IF PRESSED ON EXAMPLES OF WARRANTED TRA:

- **It is possible to generally describe examples of TRA requiring judicial authorization, caution must be exercised as each measure would be assessed on its own merits to determine the authorization required.**
- **Intercepting and/or degrading equipment or weapons destined for terrorist or weapons-of-mass-destruction purposes**
- **Modifying or removing threat-related content on an extremist website**
- **Disabling or altering personal electronics (computer, phone) used to support threat activities**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

RADICALIZATION

ISSUE: What is the Service doing about domestic radicalization? What is CSIS doing to stop radicalization? What about the mandated commitment to establish an Office of Community Outreach and Counter-Radicalization Coordinator?

- **The appeal of violent messages from groups like DAESH and Al-Qaeda continue to resonate among some Canadians.**

- **DAESH in particular very effectively employs online fora to justify and incite violence in Western countries and against Western interests abroad.**

- **DAESH has developed a sophisticated social media presence, using supporters and operatives to communicate its message all over the world.**

IF PRESSED ON WHAT CSIS IS DOING TO STOP DOMESTIC RADICALIZATION

- **Given our mandate, we investigate individuals suspected of engaging in terrorist activity, including those who radicalize others, and advise government partners as appropriate. We may also act directly to reduce threats.**

- **Canadians with extremist views who seek to undertake terrorist activity, whether in Canada or abroad, are the most pressing threat Canada faces and as such, are the central focus of CSIS counter-terrorism investigative resources.**

IF PRESSED ON THE GOVERNMENT COMMITMENT TO ESTABLISH AN OFFICE OF COMMUNITY OUTREACH AND COUNTER-RADICALIZATION COORDINATOR

- **Given its mandate, the Service has unique insight into the path a small subset of Canadians follow as they progress from ideological susceptibility to action.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **CSIS works closely with its Government partners, and will support any new initiative, as appropriate.**

- **Countering radicalization to violence is a key national security issue; our response must be one that is based on clear facts and understanding of the evolving threat.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L' INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

SECURITY OF CANADA INFORMATION SHARING ACT

ISSUE: Does the SCISA alter CSIS' mandate? What safeguards are in place to protect the privacy rights of Canadians? Has SCISA expanded the scope of information it can collect from Global Affairs Canada? What has CSIS done to implement the SCISA? What has been CSIS' experience to date?

- **Timely and reliable access to information is critical to the success of the Service's lawful investigations and also serves to enhance advice provided to Government.**

- **Information lawfully collected by other departments can be directly relevant to an active CSIS investigation and a reliable source of information.**

- **The SCISA does not in any way alter CSIS' mandate, nor does it expand the range of threats CSIS is authorized to investigate.**

IF PRESSED ON INFORMATION SHARING WITH GLOBAL AFFAIRS CANADA

- **CSIS and Global Affairs Canada have distinct mandates. We report to different Ministers and have our own legislative authorities. Both, however, perform vital functions and work together as appropriate, to protect Canadians and Canada's national interests.**

- **Global Affairs Canada may share information with CSIS, both *proactively* and in response to requests, in accordance with the authorities in SCISA.**

- **This does not, however, in any way expand the Service's authority to collect information. Indeed, the Service must continue to ensure that any information it collects is "strictly necessary" for the purposes of investigating threats to the security of Canada.**

- **Further, nothing in SCISA compels information sharing with CSIS. Global Affairs Canada is responsible for determining whether information may be shared.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **CSIS and Global Affairs Canada have established an arrangement that governs the sharing of consular information. The arrangement was established to ensure that the requirements of both parties are clear and that any sharing is done in strict accordance with relevant Canadian legislation and Ministerial Direction.**

- **For example, there could be instances where Global Affairs Canada has obtained threat-related information from an individual seeking consular assistance, particularly in areas that are close to conflict zones. If Global Affairs Canada views the information as relevant to CSIS' mandate, it may decide to proactively share it with CSIS using SCISA.**

IF PRESSED ON DEFINITIONS AND THRESHOLDS (SCISA, CSIS ACT):

- **Public Safety and the Department of Justice would be better placed to respond to questions on specific provisions of SCISA, including the definition of "activities that undermine the security of Canada".**

- **Let me reiterate, though, that this definition does not affect the definition of threats to the security of Canada for the purpose of CSIS investigations nor does it alter or expand the Service's mandate or its authority to collect information.**

- **CSIS' activities, including the collection of information, continue to be governed by the CSIS Act, which explicitly prohibits the investigation of lawful protest and dissent – SCISA does not change that.**

- **SCISA provides an explicit authority for Government departments to share information with designated recipients where relevant to activities that undermine the security of Canada.**

- **CSIS is designated as a recipient institution, given that its duties and functions – to investigate threats to the security of Canada – are aligned with the definition of "activities that undermine the security of Canada" in the SCISA. This means that departments have a clear, explicit authority to share information with CSIS under SCISA where it is relevant to its mandate.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **While CSIS' duties and functions are captured within this definition, thereby enabling CSIS to be designated as a recipient, any collection of information by CSIS must comply with obligations under the CSIS Act – that is, CSIS is authorized to collect information only to the extent that is strictly necessary to investigate threats to the security of Canada.**

IF PRESSED ON SAFEGUARDS AND ACCOUNTABILITY

- **The SCISA does not compel departments and agencies to share information.**

- **How and what information is shared under this new Act is carefully assessed by the originator and the recipient. Originators maintain discretion on whether to share and how information can be shared.**

- **All the activities undertaken by CSIS in the pursuit of its mandate continue to be consistent with Canadian law, including the *Charter of Rights and Freedoms* and *Privacy Act*. Our activities are also reviewed by the Security Intelligence Review Committee.**

IF PRESSED ON IMPLEMENTATION

- **CSIS has adopted a strategic approach to implementing SCISA by engaging partners on a priority basis. These partners were identified based on operational needs and requirements.**

- **This practical approach considers the particularities of each relationship, including legal and policy considerations. It has also allowed CSIS to review current relationships, identify opportunities for improvement and ensure relationships are adapted as necessary.**

- **CSIS has signed one SCISA-specific arrangement with Global Affairs Canada and adopted related protocols.**

IF PRESSED ON EXPERIENCE TO DATE

- **While I can't speak to specific details, I can tell you that CSIS works in close collaboration with its partners to protect Canada's national security and our national interests.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **CSIS and its partners continue to review existing relationships and how best to integrate SCISA to ensure that all relevant legal, policy, privacy and operational considerations are assessed to support responsible information sharing.**

- **CSIS can, however, confirm it has received information that has been shared in accordance with SCISA.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L' INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

SECURE AIR TRAVEL ACT

ISSUE: What is CSIS' role in the Passenger Protect Program? Does CSIS nominate all individuals known to be abroad?

- **The *Secure Air Travel Act* (SATA) is an additional tool that may be used to prevent travel for terrorist purposes.**
- **The SATA expanded the Passenger Protect Program to address both threats to transportation security and the prevention of travel by air for the purposes of committing certain terrorism offences.**
- **CSIS participates in the Public Safety-led Passenger Protect Advisory Group, which is responsible for reviewing nominations and recommending individuals for listing or de-listing.**
- **The Advisory Group regularly reviews the SATA list and updates it as needed. CSIS' participation is limited to recommending individuals for listing or de-listing to the SATA list.**
- **We do so in accordance with the threshold established by Government.**

IF PRESSED ON CSIS NOMINATIONS

- **CSIS cannot comment on the number of individuals it has nominated for security and privacy reasons.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

ACCOUNTABILITY

ISSUE: What is the status of the Service's relationship with SIRC? What is the Service's position regarding enhanced review? Will the Service be willing to work with the National Security and Intelligence Committee of Parliamentarians, should it be created? Why is Canada the only Five-Eyes country without a Parliamentary committee to oversee CSIS, as well as other national security agencies and departments? Could inter-agency review address existing gaps in the review of such agencies and departments?

- **CSIS recognizes the importance of independent review in maintaining Canadians' trust in Canada's national security community.**
- **We have a well-established and effective relationship with our existing review body, the Security Intelligence Review Committee (SIRC), and the Federal Court plays an important role in authorizing investigative activities, as required.**
- **In addition, I am accountable to the Minister for the conduct and management of the Service, which includes compliance with directions issued by the Minister in accordance with the Act.**
- **Enhancements to this review system, including the proposed National Security and Intelligence Committee of Parliamentarians, will be properly decided by Parliament.**
- **CSIS will, of course, respect and fully cooperate with any additional review regime put in place. We will also continue to make ourselves available to Parliamentary committees.**

IF PRESSED ON THE RELATIONSHIP WITH SIRC

- **CSIS and SIRC have established an effective, professional and productive relationship.**
- **The Service values SIRC's reviews and recommendations. CSIS gives serious consideration to SIRC's findings which, on many occasions, have had a direct impact on CSIS policies and practices.**

IF PRESSED ON THE COMMITTEE OF PARLIAMENTARIANS

- **The establishment of a National Security and Intelligence Committee of Parliamentarians is a matter of public policy currently being considered by Parliament.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- I will therefore leave it up to Parliament to debate and determine the structure and functions of this new review body.

- CSIS will, of course, cooperate fully with whatever Parliament deems appropriate.

IF PRESSED ON PARLIAMENTARY REVIEW IN ALLIED COUNTRIES

- I am aware of parliamentary review committees in allied countries based on Westminster-style governance systems.

- Review Committees in these countries draw on Parliamentarians from both Houses to review information provided by departments and agencies belonging to their country's national security community and present reports which are laid before Parliament.

- I would note, however, an important distinction. Many of those countries operate in a system of Ministerial Direction, in which intrusive operations, are authorized by Ministers and then subject to Parliamentary review.

- In Canada, these activities are authorized by the judiciary.

IF PRESSED ON JUDICIAL AUTHORIZATION

- The Federal Court plays a critical role in reviewing and deciding on the Service's warrant applications to investigate threats to Canada's national security.

- The court warrant process, which is set out in legislation, is rigorous.

- In each case, the application of Canadian laws, including the *Charter*, is thoroughly assessed. Each warrant application is approved by the Minister.

- After its review, the Court may, if satisfied that all the statutory requirements have been met, issue a warrant.

IF PRESSED ON INTER-AGENCY REVIEW:

- Existing review bodies, such as SIRC, are not currently authorized to review issues beyond their specific agency of focus and have limited authority to collaborate with one another.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **Past Commissions of Inquiry have raised this issue.**
- **Such questions are a matter of public policy. As such, I will defer to Parliament to consider this issue.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

GOING DARK

ISSUE: Is 'Going Dark' an issue/concern for the Service? What are the implications for 'Going Dark' for the Service? Why does CSIS require access to the personal and private details of Canadians?

- **The last 20 years have seen a rapid increase in the number of communications platforms, enabling near universal access to digital technology.**
- **At the same time, the diversity and complexity of communications technology has grown enormously.**
- **Communications services are moving away from traditional cable-and-wire infrastructure to virtual services, many of which originate from outside Canada. In other cases, a company may be headquartered off-shore or store data outside of Canada. Canadian laws governing communications service providers were not drafted for the borderless nature of telecommunications today.**
- **We are facing issues related to the maintenance of intercept capable networks, the widespread use of encryption and data retention requirements.**
- **This complex and rapidly evolving technological landscape presents significant challenges for CSIS in exercising our warranted authorities to collect information.**
- **Threat actors are also increasingly security aware and take advantage of digital tools to avoid detection.**
- **We refer to this issue as "going dark," meaning our warranted intercept coverage is lost or cannot be initiated. This can pose significant public safety risks.**

IF PRESSED ON IMPACT OF "GOING DARK"

- **This issue has a significant and detrimental impact on our ability to fulfill our mandate. It also creates significant pressure on resources.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **To protect Canadians, Canada's national security and law enforcement agencies need to be able to exercise their lawful authorities, including court-issued warrants, and to do so in a timely manner.**
- **For the Service, this capability is necessary to identify and investigate threats to Canadians and the security of Canada.**
- **This technological landscape presents obstacles and poses complex challenges for CSIS in our work to investigate threats to Canadians and the security of Canada.**

IF PRESSED ON RELATIONSHIP WITH COMMUNICATIONS SERVICE PROVIDERS AND PRIVACY

- **CSIS strives to maintain productive and cooperative relationships with communications service providers.**
- **Certainly, we are all navigating a difficult and changing landscape.**
- **Privacy and the ability to investigate criminal and national security threats are both important, and not mutually exclusive, objectives.**
- **Nor is there a requirement for communications service providers in Canada to ensure that their networks are capable of responding to court-authorized warrants to intercept communications.**

IF PRESSED ON DATA RETENTION

- **Canada does not have standardized data retention requirements. The volume of electronic communications today creates pressure on providers to delete data in shorter timeframes.**
- **There is also no general requirement for providers to retain telecommunications data, such as the telephone numbers an individual has dialed, which may be needed as part of a lawful investigation.**
- **Once destroyed, vital communications information required to undertake lawful investigations may not be available.**

IF PRESSED ON ENCRYPTION

- **Encryption is an important tool for safeguarding the privacy of Canadians and the security of personal, financial and trade data.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **However, the widespread availability of encryption technology also enables threat actors to conceal their communications and activities that threaten national security.**
- **The use of encryption creates delays and obstacles in the lawful investigation of threats to national security.**
- **Thus, while encryption is an important tool for security and privacy online, its increasing use also poses challenge for both CSIS and law enforcement agencies in exercising our warranted authorities.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L' INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Committee Note

CYBER SECURITY

ISSUE: Can you explain what CSIS is doing to protect Canadians against cyber threats?

- **Cyber operations have become a tool of choice for actors targeting Canada because they are efficient, cost-effective, and most importantly, deniable.**
- **The gravity of this threat continues to be highlighted in headlines. As you know, only two weeks ago, Yahoo announced that user account information for at least 500 million of its users had been stolen. In 2014, the compromise of the National Research Council was both damaging and costly for Canada.**
- **Digital technology plays a central role in the lives of Canadians and as this technology continues to evolve, so too will the range and scale of cyber threats to Canada, Canadians, and Canadian interests.**
- **Hostile cyber actors can include states, criminals, politically or ideologically motivated groups or individuals, and extremist groups.**
- **Hostile state-sponsored actors use cyber tools and capabilities to advance their economic, military, and political agendas.**
- **Hostile cyber actors employ tools to infiltrate networks for the theft of information, or to monitor the systems of Canadian public and private sector entities.**
- **Once compromised, Canadian digital infrastructure may be used to launch attacks against public and private sector entities abroad, damaging Canada's international reputation.**

IF PRESSED ON NATIONAL SECURITY FRAMEWORK - CYBER

- **CSIS is mandated to investigate activities which are suspected of constituting a threat to the security of Canada, including those emanating from cyberspace.**
- **CSIS investigates and assesses national security cyber threats and provides advice to Government partners, contributing to efforts to**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

protect Canada from cyber threats.

- **CSIS has been a key contributor to *Canada's 2010-2015 Cyber Security Strategy,* which is focussed on:**

  1) assisting efforts to secure Government systems,

  2) partnering to secure vital cyber systems outside the federal Government, and

  3) helping Canadians to be secure online.

- **CSIS works closely with other Government partners – such as the RCMP, the Communications Security Establishment Canada and the Canadian Cyber Incident Response Centre to respond to cyber threats to Canada.**

- **Overall, the Service provides unique dividends in the cyber area to both the public and private sectors.**

IF PRESSED ON CYBER REVIEW

- **As you know, the Government of Canada is reviewing its measures to protect critical infrastructure and Canadians from cyber threats. Along with Public Safety's partner departments and agencies, CSIS is engaged in this review, and supports efforts to evaluate Canada's cyber security.**

IF PRESSED ON CSIS' USE OF TRA AND OFFENSIVE CYBER OPERATION:

- **The internet represents a unique theatre of operations with its own dynamics and challenges.**

- **The internet itself is value-neutral and remains a tool and method of communication, used for both legitimate and nefarious purposes. CSIS is only interested in activity of the latter sort that represents a threat to national security as defined in the *CSIS Act*.**

- **While I cannot speak to tradecraft, I can state that any potential disruptive cyber activities undertaken by the Service would operate under the same stringent authorization requirements as other threat reduction measures, and would be conducted in consultation with CSE, as appropriate.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

PROLIFERATION

ISSUE: How is CSIS contributing to GoC efforts to counter the threat of proliferation?

- **Canada remains a target for illicit procurement efforts by state and non-state actors pursuing weapons of mass destruction or missile programs.**
- **Canada's advanced research and development in industrial, bio-chemical, medical, space, mining and nuclear technologies are attractive to states seeking to advance their military and WMD programmes, and others seeking to acquire WMD capacity.**
- **Individuals may also seek to enter Canada to engage in programmes of study on advanced materials and technologies that may have applicability to weapons of mass destruction.**
- **CSIS investigates attempts to procure WMD-applicable technology within and through Canada, and in turn advises the Government of Canada as to the nature of these efforts.**
- **CSIS also provides security screening advice on individuals of proliferation concern.**
- **CSIS intelligence on proliferation threats with a nexus to Canada is used by partners to inform a range of law enforcement, border and export control decisions.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L' INFORMATION

Committee Note

CSIS COOPERATION WITH FOREIGN AGENCIES

ISSUE: How is CSIS working with partners to keep Canada safe? How are such foreign arrangements established and assessed? How does CSIS assess human rights issues with respect to its relationships with foreign agencies?

- **CSIS maintains a well-established network of relationships with foreign agencies abroad.**

- **CSIS has more than 300 foreign relationships in some 150 countries, each authorized by the Minister of Public Safety and supported by the Minister of Foreign Affairs, in accordance with s.17 of the CSIS Act.**

- **In response to the evolving threat environment, and particularly following the events of 9/11, CSIS needed to expand its international presence and access to foreign agency intelligence to address increased threats to Canadians and Canada's national interests.**

- **CSIS also has officers stationed in various cities around the world whose role is to collect and, when required, share security intelligence information related to threats to Canada, its interests and its allies with host agencies.**

- **CSIS remains committed to collecting security intelligence information — within Canada and abroad — on threats to Canada, its interests and those of our allied international partners.**

IF PRESSED ON PROCESS FOR ESTABLISHING ARRANGEMENTS

- **As per s.17(1)(b) of the CSIS Act, the Service must obtain approval from the Minister of Public Safety to implement an arrangement with a foreign organization before it can begin exchanging classified information.**

- **As per s.17(1)(b) of the CSIS Act, the Minister of Public Safety must also consult with the Minister of Foreign Affairs before rendering a decision on such requests.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **The process to establish such an arrangement is stringent and takes into consideration a wide range of issues prior to the Service seeking Ministerial approval, including, for example: Canadian security requirements; the internal political situation and respect for human rights and the reliability of the agency.**

- **Additionally, prior to seeking the Public Safety Minister's approval for new arrangements, CSIS proactively consults with Global Affairs Canada.**

- **As per s.6(4) of the CSIS Act, I also provide an annual update to the Minister of Public Safety on the status of the Service's foreign arrangements inventory including the number of existing arrangements, as well as those implemented or altered during the fiscal year.**

IF PRESSED ON FOREIGN COOPERATION

- **The increased 'globalization' of terrorism cannot be countered in isolation. Cooperation with foreign agencies provides CSIS access to timely information linked potential or specific threats, and allows the Service (and, in turn, the Government of Canada) to obtain information which might otherwise not be available.**

- **The threat posed by 'Foreign Fighters' is international in scope. As such, a global reach is an absolute necessity in our efforts to track — and attempt to thwart — threats posed by such individuals to Canada and its allies.**

- **CSIS actively cooperates with its foreign partners on this issue, including in relation to specific investigations, lessons learned, and assessments of the phenomenon.**

- **Through such relationships, CSIS advances its own investigations into threats to the security of Canada and its interests, and gains a greater understanding of the scope and nature of the foreign fighter phenomenon itself.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L' INFORMATION

IF PRESSED ON HUMAN RIGHTS AND INFORMATION SHARING

- **CSIS opposes in the strongest possible terms the mistreatment of any individual by a foreign agency, and in all situations, we must and do comply with Canada's laws and legal obligations in sharing information with foreign entities.**

- **The human rights reputations of the agencies with which CSIS engages is not something which the Service takes lightly. CSIS must assess and mitigate potential risks of sharing information with foreign entities, always cognizant of the fact that our first responsibility is to the Canadian people and their safety.**

- **CSIS continuously assesses all of its foreign arrangements, including human rights reputations of the country, and more specifically, of the agency with which it has established such arrangements.**

- **As part of this assessment process, CSIS regularly reviews various government and non-government human rights reports and assessments for all countries with which the Service has implemented Ministerially-approved arrangements. We also liaise with allied foreign counterparts in support of such assessments.**

- **In addition to specific protocols for information sharing, the way in which we establish and manage foreign arrangements is designed to mitigate risk.**

IF PRESSED ON ALMALKI, ELMAATI AND NUREDDIN (AEN)

- **The actions of Canadian officials in relation to AEN's detention and mistreatment overseas were the subject of a Commission of Inquiry.**

- **In 2008, the Commissioner concluded that certain actions by the Service and other departments had indirectly contributed to AEN's detention and mistreatment overseas. Good-faith efforts in exceptionally difficult circumstances were, in some instances, found to be deficient.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **I can assure you that CSIS has taken the recommendations from this Commission of Inquiry and modified its governance surrounding information sharing with foreign partners accordingly. SIRC has commented positively on what we have put in place, and on our decision-making in relation to foreign information sharing.**

- **The civil cases between AEN and the Government are a matter before the Courts. To maintain the integrity of the judicial process, I will refrain from commenting any further on this issue.**

IF PRESSED ON MINISTERIAL DIRECTION

- **Ministerial Direction clearly states that in sharing information, CSIS must act in a manner that complies with Canada's laws and legal obligations and avoid any complicity in mistreatment by foreign entities.**

- **To do so, CSIS must assess and mitigate potential risks of sharing with foreign entities, as well as the accuracy and reliability of information received.**

- **We have very specific direction in place to do so, supported by a detailed decision-making process, supported by a senior-level committee that is convened as required. In this year's report, SIRC found the range of participants around the table fostered substantive discussion and provided for a rigorous decision-making process.**

- **There are also clear requirements to refer such decisions for more senior approval, as required, including to the Director and the Minister.**

- **Exchanges with foreign agencies are also incremental in nature, in order to gauge the reliability of the agency and the usefulness of such an arrangement. Exchanges are also commensurate with the degree of trust established over a period of time and reflective of the political and human rights climate within the country in question.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **That said, if CSIS received information indicating Canadian lives may be at risk, we would be negligent not to assess and attempt to corroborate it in order to prevent a direct and timely security threat, such as terrorist attack, against Canada or its interests regardless of the information's origins.**

IF PRESSED ON IDENTIFYING SPECIFIC ARRANGEMENTS

- **CSIS' relationships with its foreign partners are classified and not publicly identified.**

- **The majority of intelligence services worldwide do not wish to publicly divulge the list of foreign agency partners with which they liaise on security intelligence matters. Publicly divulging the existence of such arrangements could seriously hamper the Service's ability to liaise with such agencies in order to obtain security intelligence information relevant to the national security of Canada and Canadian interests.**

- **That said, our relationships with our close, traditional Five-Eyes partners – the United States, United Kingdom, Australia, and New Zealand – are widely known. The Five-Eyes is an invaluable network for the Canadian intelligence community. Without the benefits of this cooperation, Canada would suffer from significant intelligence gaps.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L' INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

INTELLIGENCE AND EVIDENCE

ISSUE: Why is intelligence appearing in judicial proceedings? What are issues associated with the reliance on intelligence as evidence? Are there not existing authorities that protect the release of sensitive information?

- **As the Service's mandate is to investigate threats to the security of Canada and provide related advice to the Government of Canada, CSIS frequently shares threat-related information with other government departments.**
- **CSIS intelligence may therefore inform decisions made by our domestic partners, as they administer or enforce laws for which they are responsible.**
- **The result, however, is that CSIS intelligence is often drawn into public proceedings – civil, criminal or administrative.**
- **If released publicly, this information could compromise: intelligence operations, the safety of CSIS sources, CSIS capabilities and techniques and Canada's relationships with foreign partners.**
- **It is therefore essential for the Service to protect sensitive national security information against public release using available legal tools, as appropriate.**

IF PRESSED ON EXISTING AUTHORITIES TO PROTECT SENSITIVE INFORMATION

- **A number of regimes allow the Government to protect sensitive information from public release.**
- **For instance, Section 38 of the *Canada Evidence Act* provides for the protection of sensitive information when national security is at risk. The *CSIS Act* was also amended to provide greater certainty in relation to the protection of the identity of CSIS human sources.**
- **That said, when the Service's sensitive information must be publically released, CSIS must make a decision as to whether or not that information should be disclosed.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **In such instances, CSIS must weigh the operational cost of publically releasing such information against the benefit of a potential prosecution or successful review of Government action.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

SIRC Annual Report

ISSUE: SIRC's annual report says that in one instance, you failed to notify the Minister. It also suggests you do not consult with GAC and are assessing the applicability of the Criminal Code. What is that about?

- **The SIRC Annual Report plays an important role in providing Parliament – and the Canadian public – with an understanding of our operations.**

- **SIRC's findings and recommendations provide valuable feedback for members of our Executive and, as a result, often directly influence policies and practices.**

- **I am particularly pleased to report that SIRC found that all threat reduction measures approved to date complied with the CSIS Act, Ministerial Direction and operational policies.**

- **In relation to information sharing with foreign entities, SIRC also found that, in response to Ministerial Direction, CSIS acted quickly in implementing a sound information-sharing framework and in establishing an executive level committee charged with evaluating the use of information where there may be a risk of mistreatment.**

- **In relation to a review of a CSIS foreign station, SIRC found that CSIS's presence in that part of the world was seen as both welcome and necessary to fulfilling our mandate on behalf of the Government.**

- **Where SIRC has indicated improvements are required, CSIS has accepted and acted on the vast majority of SIRC's recommendations this year. For example, strengthening certain decision-making processes, as well as accountability for our overseas operations. A policy framework recommended by SIRC in relation to the collection of datasets has also already been completed and is being implemented.**

- **Recommendations may be rejected for a variety of reasons, including where CSIS respectfully concludes a recommendation is based on an problematic finding, where it may be impossible to apply, or where the underlying issue may be addressed by other means.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **For example, this year CSIS did not agree with SIRC's recommendation to use specific suggested language in certain reviews. CSIS concluded that the required language is defined in legislation, and that CSIS will continue to ensure the required language is applied in a consistent manner.**

IF PRESSED ON CERTIFICATION OF ANNUAL REPORT/COMPLIANCE

- **SIRC found that the activities it reviewed this year did not constitute an unreasonable or unnecessary exercise of CSIS' powers**
- **SIRC also found that, with few exceptions, our operations complied with the CSIS Act and Ministerial Direction.**
- **Three instances of non-compliance were identified in SIRC's review. The first involved non-compliance with respect to a warranted collection activity. In the second instance, CSIS did not comply with Ministerial Direction to notify the Minister in certain circumstances. Finally, SIRC made reference to a previously reported incident of the collection of taxpayer information without a warrant.**
- **The Canada Revenue Agency matter referenced was previously reported in last year's SIRC Annual Report. There is no new information contained in this year's report; it was only mentioned again because their most recent report includes certifying my report to the Minister last year, which cited the CRA case.**
- **SIRC was satisfied that the instances identified were reported by CSIS in the Director's Report to the Minister.**

IF PRESSED ON REVIEW OF THREAT REDUCTION MANDATE

- **SIRC reviewed CSIS' performance in giving effect to its new mandate to reduce threats to the security of Canada.**
- **SIRC found that CSIS has developed a robust internal governance framework for TRA including compulsory training for CSIS employees.**
- **SIRC recommended that CSIS prioritize the development of formal mechanisms for consultation with other Government of Canada partners.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **Indeed, CSIS has negotiated and is implementing consultation mechanisms with three key partners and work on a fourth is underway.**

- **From the outset, CSIS has consulted closely with the RCMP on threat reduction measures. Similarly, early consultation with GAC and CSE has been prioritized, as appropriate considering the proposed measure.**

- **SIRC also recommended the CSIS develop a mechanism for tracking best practices and lessons learned for threat reduction measures.**

- **In developing the internal policy and procedures for this new mandate, CSIS recognizes the importance of tracking outcomes to assess best practices and identify issues for further consideration going forward and is implementing initial efforts in this area.**

IF PRESSED ON REVIEW OF CANADA REVENUE AGENCY DISCLOSURE

- **The Canada Revenue Agency matter referenced was previously reported in last year's SIRC Annual Report. There is no new information contained in this year's report; it was only mentioned again because their most recent report includes certifying my report to the Minister last year, which cited the CRA case.**

- **On learning of this issue, I referred the matter to SIRC for review and advised our colleagues at CRA, as well as the Privacy Commissioner. We of course conducted our own internal review. A limited number of disclosures were made to one of CSIS' regional offices; this was due to human error.**

- **It should be noted that none of the information received from the CRA was shared beyond CSIS. This information has been deleted from CSIS operational databases. The Service is satisfied this issue has been thoroughly investigated, that the information has been completely deleted, and that the necessary steps were taken to prevent recurrence.**

- **A number of corrective steps have since been taken and we are working with CRA to review our arrangements.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

IF PRESSED ON REVIEW OF DATASET ACQUISITION

- **Timely and reliable access to information is critical to the success of the Service's lawful investigations and also serves to enhance advice provided to Government.**

- **The exploitation of data is invaluable in relation to the exercise of CSIS' mandate, but it must be undertaken responsibly and in accordance with our authorities.**

- **CSIS agreed with SIRC's recommendation to finalize a governance framework for dataset acquisition, and in recognition of the significance of this issue, stopped ingesting datasets into a usable format pending the development of a governance framework.**

- **This framework sets out clear requirements for the collection of datasets, to ensure that our collection respects CSIS Act requirements and the Charter, including privacy considerations.**

- **A clear decision-making process has been established for <u>non-referential datasets</u>, to ensure they meet all collection requirements, including the strictly necessary threshold. We have also established a centre of expertise to support the implementation of this governance framework.**

- **<u>Referential datasets</u>, on the other hand, provide contextual information. They are publicly available and do not contain sensitive information related to individuals. This may include information such as maps, airport codes or the phone book.**

- **We are responsible for diligently managing and protecting any information we collect. We have stringent requirements in place, supported by robust operational policies and regular training, as well as rigorous internal auditing and review.**

- **The framework has since been implemented, and ingestion has resumed in line with the requirements it sets out.**

IF PRESSED ON REVIEW OF FOREIGN FIGHTER INVESTIGATION

- **CSIS' overseas collection activities related to the ongoing investigation of Canadian foreign fighters was the subject of SIRC review in 2015.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **The conflict in Syria has been a major draw for radicalized Canadians travelling abroad. After the declaration of a "caliphate" by Daesh in June 2014, there was an uptick in the numbers of Canadians travelling to the region.**

- **The scale of this extremist travel, and the unique investigative challenges associated with the Syrian conflict zone, has created unprecedented challenges for CSIS.**

- **Yet, the Service has an operational imperative to prevent extremist travel and to ensure individuals engaged in extremist activities abroad do not become a threat to Canada upon their return.**

- **The Service takes very seriously the findings and recommendations that came from SIRC's review of this investigative activity, and the shortcomings it identified.**

IF PRESSED ON LEGAL CERTAINTY

- **CSIS is seeking clarification on the legal issues identified by SIRC and will report to the Minister.**

- **CSIS is operationalizing the related Ministerial Direction, including working closely with GAC to formalize mechanisms for enhanced consultation on foreign policy risk.**

- **Our operational policy is being updated in parallel, to set out clear processes and lines of responsibility for identifying and assessing risks, including in consultation with partners as appropriate.**

IF PRESSED ON FAILURE TO NOTIFY THE MINISTER

- **I am committed to ensuring that our Minister is being appropriately engaged in relation to high risk activities.**

- **Clarifications to our operational policies and risk assessment process provide greater certainty in this regard.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Committee Note
TERRORISM

ISSUE: How is CSIS countering the terrorism and extremist threat? What actions are being taken to prevent terrorist travel or deal with returnees? How many Canadians abroad are engaged in terrorist activity? How many returnees?

- **The Service has never before faced a terrorist threat of the scope, scale and complexity of Sunni Islamist-inspired terrorism. In particular, DAESH has proven adept at directing attacks and influencing adherents abroad, whilst attracting others to their self-proclaimed "Caliphate".**
- **The number of Canadians abroad for terrorism-related purposes has, after a surge, levelled off.**
- **But the terrorist threat at home has not diminished. Indeed, preventing individuals from travelling abroad for extremist purposes may in fact increase the threat at home.**
- **Members, the principal terrorist threat to Canada remains that posed by violent extremists who are inspired to carry out an attack in Canada.**
- **As the terrorist incident in Strathroy, Ontario on August 10th reminded us, we are not immune to attempted attacks. Constant ongoing communication and collaboration between domestic and international partners is necessary.**
- **Canadians engaged in terrorist activity abroad are a significant concern for the Service. These activities are destabilizing and harmful to the countries in which they operate.**
- **While overseas, these individuals can expand their networks, develop new skills, and in some cases become further radicalized or influence others in Canada to follow their path.**
- **The activities of these extremist travellers vary widely, ranging from paramilitary activity, training, and logistical support, to terrorist fundraising and studying at extremist-influenced schools. Canadians have been valued by extremist groups for their English-language abilities, technical and social media skills.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **As you know, CSIS is not an enforcement organization, but the Service provides advice to other Canadian partners who may be in a position to take action against such travelers.**
- **Members understand that every extremist prevented or deterred from traveling abroad may become an individual at home that requires ongoing investigation.**

IF PRESSED ON NUMBERS

- **There are approximately 180 individuals abroad for terrorism-related purposes.**
- **Of the approximately 180 travelers, around half were last identified in Turkey, Syria or Iraq. Many extremists groups operating in the region freely traverse between Syria and Iraq; an individual known to be in Syria one day might be in Iraq the next.**
- **I must state that this number also includes individuals who are believed, or suspected, to have died while abroad.**
- **Members, as previously stated, there is not a lot to be gained by reporting frequently on incremental changes in these numbers, which fluctuate constantly.**
- **Nor do numbers of 'travelers' or 'returnees' adequately capture the scale of this threat: individuals who have never travelled – whether they aspire to, have been prevented from travelling or, for a variety of reasons, choose to remain in Canada – and are engaged in threat-related activities at home are not included.**
- **I will remind you, members, that Aaron Driver was a thwarted traveller who was prevented from going abroad.**
- **I should point out that that we remain concerned about the number of individuals that we are not aware of, or about whom we have incomplete information, due to the significant operational challenges associated with such investigations.**

IF PRESSED ON RETURNEES

- **The Service is currently aware of approximately 60 returnees to Canada who have travelled abroad for extremist purposes.**
- **CSIS is seized with this issue, as extremists returning to Canada have the potential to pose a significant threat to our national security.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **However, I would like to be very clear with the committee that I use the word "potential" because individuals' experiences vary widely.**
- **Returnees may respond in a number of different ways – from returning to regular life, radicalizing others, or financing and facilitating the travel of others, to attack planning.**
- **While travellers' experiences abroad will vary, we must be aware of all returnees to the extent possible in order to maintain situational awareness and to assess which returnees are engaging in activities that could constitute a threat to national security. CSIS operates in an environment where there is no margin for error.**
- **Some individuals never achieve their intent and simply return to Canada, while others return due to injury, lack of resources, or personal reasons.**
- **Some individuals do return home with significant operational experience and training. Of these, many have the credibility to encourage and recruit other individuals to go abroad or to conduct terrorist related activities in Canada.**
- **It is worth noting that the percentage of individuals returning from the Syrian conflict zone, particularly those associated with DAESH, is quite low. This is in part because of the control DAESH exerts over recruits.**

IF PRESSED ON THE PUBLIC THREAT REPORT

- **The Service welcomes the Public Report on the Terrorist Threat to Canada.**
- **Such reports are important in that they inform the general public about threats to the security of Canada and in this case, build understanding about global terrorism.**

IF PRESSED ON THE CURRENT THREAT LEVEL

- **As the Minister has stated, the current threat level for Canada is set at MEDIUM – intelligence indicates that a violent act of terrorism could occur in Canada.**
- **The principal terrorist threat to Canada remains that posed by violent extremists who could be inspired to carry out an attack in Canada.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **For the first time, the Public Report on the Terrorist Threat to Canada releases information on the methodology of setting the National Terrorism Threat Level.**
- **The Integrated Terrorism Assessment Centre (ITAC) is responsible for analyzing and terrorism threats and setting threat levels for Canadian interests at home and abroad.**
- **The threat level serves as a tool for government officials to identify risks and vulnerabilities from threats and, in turn, determine appropriate responses to prevent or mitigate an act of terrorism.**

IF PRESSED ON THE AUGUST 10TH AARON DRIVER INCIDENT

- **The Service closely engages with Canadian and international partners in relation to urgent matters of national security.**
- **The incident in Strathroy, Ontario, demonstrates the importance of close collaboration between international and domestic partners.**
- **Ongoing communication and deconfliction between the Service, RCMP and FBI throughout the incident prevented lives being lost.**
- **The Aaron Driver case also highlights the threat of frustrated travellers who turn their attention to conducting attacks domestically.**

IF PRESSED ON TAMIM CHOWDHURY'S REPORTED DEATH IN BANGLADESH

- **The Service cannot comment on ongoing investigations.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

ESPIONAGE, FOREIGN INTERFERENCE, FOREIGN INVESTMENT & INSIDER THREAT

ISSUE: Is Canada a target for espionage by foreign states? Why are investigations on foreign intelligence activities a priority for the Service? Is CSIS involved in the review of foreign investments? What measures is CSIS taking to prevent an insider threat, like Delisle?

- **States and other entities abroad have interests – political, economic and territorial – and will pursue those interests by a variety of means. Some countries will do so through espionage and interference, targeting the Canadian economy, strategic interests and assets, societal institutions and members of the diaspora.**

- **Canada remains a target for the traditional espionage activities of a number of foreign states, with Russia and China often cited in the press as examples. These foreign states continue to gather political, economic, and military information in Canada through clandestine means.**

- **Advanced technology is an attractive target for some states, which use both traditional espionage and foreign investments to transfer sensitive technology abroad.**

- **Cyber operations provide another means of espionage, as the theft of information and compromise of systems belonging to Canadian private and public sector entities can be done clandestinely, including from outside Canada.**

IF PRESSED ON FOREIGN INTERFERENCE

- **Foreign interference is the clandestine influence and direction of political or other Government actors to the detriment of Canadian interests and may involve a threat to persons in Canada, including members of a foreign state's diaspora community.**

- **While such investigations are highly sensitive, what I can say is that foreign interference is most certainly a threat to Canadians and to Canada's democratic form of Government, which is why when CSIS was created 30 years ago, we were authorized to investigate this threat.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

IF PRESSED ON FOREIGN INVESTMENT

- **While foreign investment is a key driver of Canada's economic prosperity, investments sometimes pose national security concerns.**
- **The Service assesses that corporate investments by some foreign entities can pose risks to Canada's national security, with loss of Canadian control over critical infrastructure and strategic sectors, and transfer of sensitive technology abroad.**
- **In 2009, the *National Security Review of Investments Regulations* provisions within the *Investment Canada Act* were introduced. These provisions enabled the Government to review foreign investments on national security grounds.**
- **CSIS works with partners to support this process whereby the Governor in Council may stop or impose mitigation conditions on proposed investments that could or would be injurious to Canada's national security.**
- **CSIS assesses that these concerns will continue, particularly given the prominent role that state owned enterprises play in the economic strategy of some foreign governments.**

IF PRESSED ON INSIDER THREAT

- **The unauthorized disclosure of classified information by individuals working in the intelligence community – whatever their motivation – is what we commonly refer to as the "insider threat."**
- **As we have seen with the Delisle case here in Canada and the Manning and Snowden cases in the United States, the threat is real, and in the digital age, poses a significant challenge to all intelligence agencies, including CSIS.**
- **In order for us to do our job, we need to protect information about how we do it – whether it be in relation to operations, methods, sources, or targets. We must also guard the product of our operations: the intelligence and advice we provide to Government.**
- **The unauthorized disclosure of sensitive information has the potential to undermine our ability to carry out the mandate given to**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

us by Parliament and jeopardizes the security of Canada and Canadians.

IF PRESSED ON FOREIGN INFLUENCE ON CANADIAN DIASPORA GROUPS:

- Every member of Canadian society has a right to freely associate and maintain connections with family, friends and organizations, whether in Canada or abroad.
- But when diaspora groups in Canada are subject to clandestine and deceptive manipulation by a foreign power for the purpose of advancing that country's strategic or economic objectives, this constitutes a threat to the security of Canada.
- CSIS actively investigates such threats, which are expected to continue in the coming years.

IF PRESSED ON WHAT CSIS IS DOING TO PREVENT UNAUTHORIZED DISCLOSURES

- To address such concerns, CSIS, alongside our Government of Canada partners, continues to develop and implement preventive measures as well as internal procedures and tools designed to enhance the safeguarding of classified information.
- CSIS maintains robust internal security procedures that address the unique world we operate in, including extensive background checks of employees, regular polygraph testing, extensive physical security measures at CSIS facilities, and strict rules and procedures for handling classified information and systems.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

CSIS MANDATE

ISSUE: How does CSIS's Security Screening program operate? What is CSIS's role in security screening for immigration? Why are investigations on foreign intelligence activities a priority for the Service?

- **CSIS' mandate is clearly defined in the *CSIS Act*. We are authorized to to collect information, to the extent strictly necessary, on activities suspected of constituting a threat to the security of Canada. We investigate threats and analyze information to provide advice to the government, including investigations related to the provision of security screening assessments and advice. We may also act directly to reduce threats to the security of Canada.**

- **I must be clear. CSIS is not an enforcement agency. We have no authority to arrest or detain individuals, nor do we make decisions related to security screening assessments and advice. These authorities rest with the responsible departments and agencies.**

IF PRESSED ON THREAT REDUCTION ACTIVITIES

- **CSIS' threat reduction mandate leverages CSIS' expertise, capabilities and early awareness of threats, bolstering its capacity to actively protect Canada and its citizens from harm.**

- **CSIS is authorized to take measures to diminish threats to the security of Canada identified in the conduct of its investigations.**

- **The measures must be reasonable and proportional and must meet a higher threshold for reasonable grounds to believe. CSIS has developed a robust internal governance framework for the approval conduct of threat reduction activities to ensure these legal requirements are met.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L' INFORMATION

IF PRESSED ON DEFINITION OF THREATS TO THE SECURITY OF CANADA:

- **Our Act clearly defines the threats we are authorized to investigate and, in this regard, has remained unchanged since 1984. We investigate espionage, sabotage, foreign interference and, of course, terrorism and extremism.**

- **Of note, the *CSIS Act* explicitly excludes the investigation of advocacy, protest and dissent, unless it is carried out in conjunction with the previously mentioned threat related activities.**

- **We will continue to investigate these threats as we have done for the past 30 years.**

- **In its reports, SIRC has, with rare exceptions, found that the Service carries out its duties in accordance with the CSIS Act and Ministerial Directions and that the exercise of its activities is reasonable and necessary.**

- **The Service will continue to honor and comply with its statutory authorities.**

IF PRESSED ON SECURITY SCREENING:

- **CSIS' Security Screening mandate supports the integrity of the immigration program, identifies non-Canadians who pose a threat to national security seeking to enter or gain status in Canada, and helps safeguard sensitive government information, assets, sites, or major events.**

- **The Security Screening program is perhaps the most visible across government, providing threat-related security assessments or advice to over 100 Government of Canada clients.**

- **It is important to note that CSIS has no enforcement mandate, nor do we make decisions on refugee claims or immigration applications or government security clearances, other than its own.**

- **CSIS' role in the screening process – be it in relation to Canada's immigration system or government security clearances, is to advise our partners of threat-related information, to assist them in making a decision.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

- **The Service has access to unique information that can assist our partners in making fully informed decisions.**

IF PRESSED ON FOREIGN INTELLIGENCE, SECTION 16:

- **At the written request of the Minister of National Defence or Minister of Foreign Affairs, Section 16 of the *CSIS Act* authorizes the Service to collect foreign intelligence. This collection is limited in that it only occurs in Canada, and the subjects of investigations are neither Canadian citizens, nor Permanent Residents.**

- **The Service's foreign intelligence mandate has not changed since CSIS was created.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L' INFORMATION

Date: October 6, 2016
Classification: Unclassified
Agency: CSIS

Committee Note

CSIS TODAY

ISSUE: Who are the people that CSIS employs? Where does CSIS operate?

- **The people of CSIS are committed to maintaining an organization that is flexible and innovative in the delivery of its mandate.**
- **The diversity of our workplace helps support the achievement of our objectives. It allows us to better understand the Canadian communities we protect.**
- **CSIS is an integral member of the security and intelligence community and an active participant in broader Government of Canada initiatives. Interestingly, we are shaped by the evolving threat environment and the Government of Canada's response.**

IF PRESSED ON DEMOGRAPHICS:

- **The Service has approximately 3,000 employees, with an almost even gender distribution.**
- **Almost 70% of our employees speak both official languages and 20% have a good or excellent knowledge of another language.**
- **The Service has been named *one of Canada's Top 100 Employers for 2016* This marks the 8th year in a row (2009 to 2016) that the Service has been awarded this honour, which is a record no other Federal Government Department/Agency has accomplished during that time period.**
- **CSIS has also been named one of the *National Capital Region's Top 25 Employers for 2016*, for the 9th year in a row.**

IF PRESSED ON REGIONAL PRESENCE:

- **The Service has 6 Regional Offices across Canada, as well as our National Headquarters in Ottawa.**
- **CSIS also has an international footprint with a publicly acknowledged presence in Washington, London, and Paris.**

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L' INFORMATION

News Summaries of Key Service Media Mentions

July 1, 2016 to Oct. 4, 2016

Table of Contents

Overview....1
Notable News articles....2
C-51....2
Torture....7
Kevin Garratt....9
Others....10

Overview

While the Service was most frequently mentioned in coverage on the death of terror suspect **Aaron Driver**, the most substantive mentions were in relation to **Bill C-51**. In the majority of **Aaron Driver** reports, the Service mentions were secondary. Whereas in C-51 coverage, the Service was front-and-centre—in addition to Public Safety Minister Ralph Goodale.

C-51 coverage was strongest in early September as Minister Goodale announced that the Liberal government will launch the public phase of its long-awaited national security review with the release of a discussion paper. The *Canadian Press* stated: **The government has promised to repeal** what it calls the problematic elements of omnibus security legislation, known as Bill C-51, ushered in by the previous Conservative government. The Liberals also plan to introduce new measures they say will do a better job of balancing collective security with rights and freedoms. Among other things, the government has pledged to ensure all Canadian Security Intelligence Service warrants respect the Charter of Rights and Freedoms.

Earlier in September, the Service figured prominently in the CBC's the **"Terror Files"** series. However coverage on this file was primarily limited to CBC/Radio-Canada platforms.

The Service/Director also figured prominently in a handful of reports—mainly from the Globe and Mail—on the **release of Kevin Garratt**.

(Mentions of Director are in bold)

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L' INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Notable News articles

C-51

Spies use C-51 to gather intelligence from Canadians detained overseas
Canadian Press, Jim Bronskill, 2016 10 03
Ottawa - Canada's spy agency is using controversial powers under the C-51 anti-terrorism legislation to gather intelligence from Canadians held in foreign prisons, a newly released memo reveals. Amnesty International Canada and the NDP are expressing concerns about the potential pitfalls of the previously unknown information-sharing arrangement between the Canadian Security Intelligence Service and Global Affairs Canada. In the House of Commons, Public Safety Minister Ralph Goodale stopped short of defending the arrangement Monday, saying a federal national security review would ensure the government's approach is consistent with ``what Canadians want." The spy service and Global Affairs made the sharing deal this year through the Security of Canada Information Sharing Act _ part of the omnibus security legislation known as C-51, says a secret memo to Public Safety Minister Ralph Goodale from CSIS director **Michel Coulombe**. The provisions, ushered in by the previous Conservative government, expanded the exchange of federally held information about activity that "undermines the security of Canada." "Information collected by (Global Affairs Canada) through the provision of consular services can be directly relevant to investigations of threats to the security of Canada," says the heavily censored CSIS memo, obtained by The Canadian Press under the Access to Information Act. However, it is often difficult for consular officials to determine when a detained Canadian has been tortured and what impact that has on the information they may be sharing, said Alex Neve, secretary general of Amnesty International Canada. That became glaringly evident in the case of Maher Arar, an Ottawa communications engineer who made false confessions of terrorist involvement while being tortured by his captors in a Syrian prison, Neve noted. In general, the new arrangement seems based on an understanding that information obtained by consular officers while working with or interviewing Canadians detained abroad "can and will be shared with CSIS when relevant to national security," Neve said. The sharing arrangement between CSIS and Global Affairs underscores the concerns raised by the privacy commissioner and reaffirms the NDP's desire to see C-51 repealed, said Matthew Dube, the party's public safety critic. "The appropriate safeguards aren't in place." Neither Global Affairs Canada nor CSIS would provide details about the sort of information the spy service hoped to obtain through the new sharing arrangement. Both agencies say they carry out their duties in accordance with relevant legal and privacy obligations.

CSIS has 'complied' with Bill C-51's anti-terror powers, watchdog committee says
Toronto Star Online, Tonda MacCharles, 2016 09 30
Ottawa - The civilian watchdog committee that oversees Canada's spy agency is giving a cautious thumbs-up to CSIS for its exercise of newly acquired anti-terror powers under Bill C-51, the controversial law passed last year that the Liberal government says it will amend. Pierre Blais, chair of the Security Intelligence Review Committee (SIRC), said in an interview that CSIS appears to have used in a responsible manner its warranted and unwarranted powers of threat disruption and information- sharing. Under Bill C-51, passed by the previous Conservative government in 2015, the Canadian Security Intelligence Service (CSIS) was given wide- ranging ability to disrupt or reduce threats to Canada's national security, inside or outside Canada. The only limits on the new power are that CSIS must not cause death or bodily harm, obstruct justice, or violate an individual's sexual integrity. If any steps that CSIS proposes to take might violate Canadians' charter rights, the spy agency is required to go to court to seek a judicial warrant for the activity. In its 2015-16 annual report (www.sirc-csars.gc.ca) , tabled Thursday in Parliament, SIRC said CSIS has put in place appropriate policies, procedures, and mandatory training to guide its agents on intervening to disrupt threats - "however this is still a work in progress."

The report recommended that CSIS formalize consultation with other affected departments, such as Global Affairs, when threat reduction activity could overlap their areas or raise concerns for their operations. The watchdog examined all 24 instances to date where CSIS acted to disrupt perceived security threats, and said "all complied with the CSIS Act, ministerial direction and operational policies." It reported no judicial warrants were issued, and no applications for such warrants were refused. SIRC said CSIS itself had documented a risk of over-collecting. The report said "a governance framework was drafted two years ago, but that it had not yet been finalized." SIRC's recommendations are non-binding. Yet CSIS director **Michel Coulombe** issued a written statement saying CSIS is acting to strengthen its rules around such information gathering. SIRC said CSIS uses bulk data sets in many ways, cross-checking it with "information already connected to a potential threat - such as an address, phone number or citizen identification number - and using it to search for 'hits' in the data."

Canada's CIA Had No Policy for Collecting and Using Massive Amounts of Data
Motherboard Blog, Jordan Pearson, 2016 10 01
Ottawa- The Canadian Security Intelligence Service (CSIS), the country's CIA equivalent, used large datasets to track and identify persons of interest without a policy to guide their collection, retention, or use, according to a new report from Canada's intelligence watchdog. CSIS is tasked with tracking terror suspects within and outside of Canada, and the investigation was undertaken in the context of new, and incredibly broad, powers bestowed upon the spy agency by the controversial Bill C-51. Canada has recently ramped up its efforts to identify people connected to pro- terror ideologies. In August, the Royal Canadian Mounted Police (RCMP) arrested 24-year-old Ottawa man Tevis Gonyou-McLean who was later released on a peace bond that restricts his movement, communication, and online activities. The RCMP's national security unit frequently receives intelligence from CSIS. A report published on Thursday by the civilian Security Intelligence Review Committee (SIRC) notes that CSIS uses large databases to find out more information about suspects, develop leads, and even to "identify previously unknown individuals of interest by linking together types of information which have mirrored threat behaviour."

C-51: de l'information échangée sans garde-fou
Le Devoir, Hélène Buzzetti, 2016 09 28
Ottawa - L'appareil gouvernemental a utilisé la loi à 58 reprises Sitôt adoptée, sitôt utilisée. L'appareil gouvernemental a eu recours à la Loi antiterroriste (C-51) dès les premiers mois de son entrée en vigueur, mais les ministères fédéraux n'ont pas pris les précautions qui s'imposaient, déplore le commissaire à la protection de la vie privée du Canada, Daniel Therrien. Le projet de loi C-51, adopté dans la controverse en 2015, n'a pas seulement accordé de nouveaux pouvoirs aux forces policières et au Service canadien du renseignement de sécurité (SCRS). Il a aussi autorisé les 128 institutions fédérales (ministères, agences, Gendarmerie royale du Canada, etc.) à s'échanger des informations qu'elles détiennent sur des citoyens canadiens. Dans son rapport annuel déposé mardi, Daniel Therrien révèle que, au cours des six premiers mois d'application de la loi, de l'information a été communiquée à 58 reprises. Cinq institutions se sont adonnées à ces échanges : la GRC, le SCRS, l'Agence des services frontaliers, le ministère Affaires mondiales et celui de l'Immigration, des Réfugiés et de la Citoyenneté.

Watchdog warns terror bill threatens privacy
Toronto Star, Alex Boutilier, 2016 09 28
Ottawa - Law-abiding Canadians are at risk of having their personal information scooped up by broad new powers granted to Canada's security agencies, according to a new report. Privacy commissioner Daniel Therrien said Tuesday that the federal government failed to assess the privacy implications of the new information-sharing powers granted to 17 departments and agencies under Bill C-51. Therrien's office found that only two of those departments commissioned "privacy impact assessments," standard reports used by Ottawa to ensure new policies and powers don't trample on Canadians' rights. "The issue is that if you allow greater information- sharing, the legal standards authorizing this activity should be

such that law-abiding Canadians, ordinary Canadians who should have nothing to fear from surveillance activities of the state, are not caught by the information-sharing regime," Therrien told reporters. Under Bill C-51, the controversial terrorism laws brought in by the previous Conservative government, several security and law enforcement agencies can share information on "activities that undermine the security of Canada." The broad powers were granted to security agencies such as CSIS and the RCMP, but also to departments handling immigration, health, foreign affairs and transportation. Therrien's office found the powers had been used a total of 110 times over six months.

Why the former CSIS director says the Liberals shouldn't touch Bill C-51
Global News, Monique Muise, 2016 09 12
The former director of Canada's Security Intelligence Service says Bill C-51 should remain untouched. He does, however, support the government's plan to re-examine the controversial piece of anti-terror legislation. "I would leave it as it is, but as a Canadian, I'm glad the government's carrying through on its promise to review things," Richard Fadden told the West Block's Tom Clark this weekend. "(Bill C-51) has been in effect for a while now, so Parliamentarians and others will be able to see the good, the bad and the ugly." Last week, the Liberals formally announced a review of the law as part of an overall consultation on national security. Fadden said he is aware that many Canadians have concerns about parts of the law that allow agencies and government bodies to share information. Privacy is an important consideration, he acknowledged, but it must be balanced with security. "When I was director of CSIS, the thing that worried me more than anything was if something went wrong and there was a terrorist act that was successful, and we subsequently found out that another department (had) the information and didn't share it. That's not an artificial concern, it's real." Clark also asked Fadden specifically about the parts of Bill C-51 that give CSIS more power to 'disrupt' potential terror threats. Fadden said that allowing the agency to take a more active role, rather than just monitoring and gathering intelligence, will help Canada confront security threats and possibly prevent them from ever occurring.

Goodale to launch C-51 consultations on Thursday
iPolitics.ca, Amanda Connolly, 2016 09 08
Ottawa - Opponents of the Harper government's controversial national security legislation, C-51, will have the chance to officially voice their concerns to government starting Thursday, when Public Safety Minister Ralph Goodale kicks off another round of consultations focused on Canada's national security. Goodale will make the announcement flanked by Justice Minister Jody Wilson-Raybould in Edmonton Thursday afternoon and it will make up the second part of a two-pronged review of Canada's national security, the first of which launched last month with a focus on cyber security. Prime Minister Justin Trudeau promised to fix "problematic elements" of C-51 during the 2015 election campaign, pledging to "guarantee that all Canadian Security Intelligence Service warrants respect the Charter of Rights and Freedoms; establish an all-party national security oversight committee; ensure that Canadians are not limited from lawful protests and advocacy; require that government review all appeals by Canadians on the no- fly list; narrow overly broad definitions, such as defining "terrorist propaganda" more clearly; limit Communications Security Establishment's powers by requiring a warrant to engage in the surveillance of Canadians; require a statutory review of the full Anti-Terrorism Act after three years; and prioritize community outreach and counter-radicalization, by creating the Office of the Community Outreach and Counter-radicalization Coordinator."

Liberals to release discussion paper to begin national security review
Canadian Press, Jim Bronskill, 2016 09 08
Ottawa - The Liberal government will launch the public phase of its long-awaited national security review Thursday with the release of a discussion paper. The government has promised to repeal what it calls the problematic elements of omnibus security legislation, known as Bill C-51, ushered in by the previous Conservative government. The Liberals also plan to introduce new measures they say will do a better job of balancing collective security with rights and freedoms. Among other things, the government has

pledged to ensure all Canadian Security Intelligence Service warrants respect the Charter of Rights and Freedoms. This could roll back new provisions allowing CSIS to disrupt terror plots through tactics that breach the charter as long as a judge approves. Public Safety Minister Ralph Goodale has said the government is open to an expansive revamp of national security legislation and policy, not just the handful of promised changes. Goodale and Justice Minister Jody Wilson-Raybould are slated to discuss the consultation at a news conference Thursday in Edmonton. They will release a discussion paper as well as a lengthy background document outlining national security issues.

PM says civil liberties must be balanced with security in battling terrorism
Canadian Press, Staff report, 2016 08 16
Halifax - An alleged terrorist plot in Ontario that created anxieties over police monitoring of suspects hasn't shaken Prime Minister Justin Trudeau's emphasis on balancing civil liberties with public safety. In his first reaction to an alleged plot that led to the death of Aaron Driver in Strathroy, Ont., Trudeau said Tuesday that balancing individual rights with keeping Canadians secure from bombing threats has to be handled with care. ``Canada is a country that values its freedom (and) its basic charter rights," he said during a stop in Bridgetown, N.S., for an infrastructure funding announcement. ``All Canadians expect their government to do two things: to keep Canadians safe and to defend and uphold the values and rights that all Canadians hold dear." ``Getting that balance right isn't always easy in the challenging situation we now live in but it's extremely important." During the last federal election, the Liberals pledged to guarantee that all Canadian Security Intelligence Service warrants respect the charter, that the right to lawful protests and advocacy aren't violated, and they pledged to ``narrow overly broad definitions (in Bill C-51), such as defining 'terrorist propaganda' more clearly." They also said a Liberal government would limit the Communications Security Establishment's powers by requiring a warrant to engage in the surveillance of Canadians and emphasize community outreach to battle radicalization of youths. Asked if the reforms are being revisited in light of cases like Driver's, Trudeau said the Liberals plan to create an all-party committee of parliamentarians to oversee national security agencies.

CSIS replies
Globe and Mail, **Michel Coulombe**, 2016 08 04
Letters to the Editor: Re Bill C-51: Why The Liberals Aren't Moving On Changes (Aug. 2): You state that Bill C-51 gave the Canadian Security Intelligence Service powers to make arrests on suspicion that someone might carry out a terrorist act. This is incorrect. CSIS does not have powers of arrest and C-51 did not change that. Instead, C-51 provided CSIS with a new threat-reduction mandate in order to respond more effectively to the current threat environment. This new mandate authorizes CSIS to take measures to diminish threats to the security of Canada as defined in the CSIS Act. These defined threats have never included lawful advocacy, protest or dissent. Moreover, the measures must be reasonable and proportional and must meet the threshold for reasonable grounds to believe and not "suspect," as noted in the article. Today's threats are fast, complex and dynamic, and CSIS's threat-reduction mandate bolsters the government's capacity to actively respond to these threats. Canadians can be assured that everything that CSIS does is consistent with Canadian law and Canadian values. Frankly, we would have it no other way. - Michel Coulombe, director, Canadian Security Intelligence Service.

Bill C-51: Why the Liberals aren't moving on changes
Globe and Mail, Lawrence Martin, 2016 08 02
Column: New Democrat MP Randall Garrison is putting together a bill aimed at repealing anti-terrorism measures brought in by the Conservative government a year ago. Mr. Garrison says the Liberal government is moving too slowly on its election promise to soften the security legislation, commonly known as Bill C-51, that gave the spooks all kinds of new powers. Our New Democrats have been considerably muted as a result of the October election. So it's good to hear them - they should be getting some inspiration from the likes of Bernie Sanders - holding up the values of the left. Any move by them to salvage civil liberties, however, won't get far. In due time there will probably be a few amendments to

C-51. But they are likely to be minor in nature, like the timid change the Liberals have introduced thus far - the appointment of a parliamentary oversight committee to monitor and scrutinize spy activities. It has the claws of a kitten. Justin Trudeau did not want to be seen as being soft on terror when the Harper government brought in C-51, which was in response to consecutive terror incidents on domestic soil. The Liberals backed the bill and sought cover with the promise of amendments. But given the climate of the times, given the recent spate of terrorist atrocities, they now feel a new need to be cautious. Politically speaking, the Liberals, because of all the global terror, are under little public pressure to move quickly. When C-51 was first introduced, there was a civil liberties outcry. Rather than just gathering intelligence, C-51 gave our spy agency (the Canadian Security Intelligence Service) powers to make arrests on suspicion that someone might carry out a terrorist act. "Suspicion" is a word of considerable latitude. The spooks were given powers to apprehend anyone engaging in an act that is deemed to promote terrorism. "Promote" is a rather flexible term as well. CSIS was given powers to disrupt gatherings whereas previously it had only a monitoring function.

Loi antiterroriste C-51 - Ottawa garde le cap, malgré le contexte européen
Le Devoir, Marie Vastel, 2016 07 28
Ottawa - L'Europe a beau resserrer sa sécurité dans la foulée des récents attentats qu'elle a subis, le gouvernement Trudeau n'a pas l'intention de son côté de retarder ses modifications promises à la loi antiterroriste adoptée par les conservateurs. Un expert estime cependant que le contexte des derniers mois devrait convaincre les libéraux de reculer. Car si leurs amendements manquent à prévenir un incident, ce sera à eux d'en porter le blâme. Le projet de loi C-51 a permis plus d'échange d'informations entre les ministères et le Service canadien du renseignement de sécurité (SCRS) ; a facilité les arrestations préventives ; a élargi l'interdiction de vol aux personnes soupçonnées de voyager pour s'adonner à des activités de terrorisme ; a et accordé au SCRS un nouveau pouvoir de " perturbation " et même celui de poser des gestes illégaux si un juge y consent. Le patron du SCRS, **Michel Coulombe**, révélait en mars que l'agence avait utilisé ses nouveaux pouvoirs près de deux douzaines de fois. Le SCRS n'avait pas obtenu de mandat d'un juge, avait-il indiqué, suggérant que l'agence n'avait donc pas estimé contrevenir aux droits des individus impliqués.

What Aaron Driver means for the debate on amending Bill C-51
CBC.CA, Aaron Wherry, 2016 08 12
Ottawa - The case of Aaron Driver, the ISIS sympathizer who was killed in Strathroy, Ont., on Wednesday, comes to the fore amid the outstanding question of federal anti-terror laws and the fate of Bill C-51, the former Conservative government's controversial legislation of last year. And on Thursday, the Conservatives spoke of both in nearly the same breath. "I salute and thank the law enforcement and intelligence officers who put their own lives on the line to stop this potential attack on innocent Canadians," interim Conservative Leader Rona Ambrose said in a statement distributed on Thursday morning. "Unfortunately, the Liberal government campaigned on a promise to strip these officers of some of the essential investigative and enforcement tools to do this work, which the previous Conservative government provided through Bill C-51, and which have already been wisely used to disrupt terrorist activities nearly two dozen times since last fall. I call on the Liberal government to ensure all of Canada's security and intelligence services keep the tools they need to do their jobs." On a very basic level, Driver's fate might well factor into the general debate: a case of suspected terrorism informing a debate about how the law should be used to respond to the threat of terrorism. "This disturbing event serves to remind us that Canada is not immune to the threat of terrorism," Public Safety Minister Ralph Goodale said on Thursday. The Liberals subsequently promised in their campaign platform last year to "repeal the problematic elements of Bill C-51, and introduce new legislation that better balances our collective security with our rights and freedoms." Specifically, the Liberals said new legislation would "guarantee that all Canadian Security Intelligence Service warrants respect the Charter of Rights and Freedoms; ensure that Canadians are not limited from lawful protests and advocacy; narrow overly broad definitions, such as defining 'terrorist propaganda' more clearly;" and "limit Communications Security Establishment's

powers by requiring a warrant to engage in the surveillance of Canadians." Ambrose referred to the fact that CSIS Director **Michel Coulombe** had told a Senate committee that new powers to disrupt extremist plots had been used close to a dozen times since the bill became law last year. But while Ambrose raises C-51 in her response to the Driver case, her statement does not directly link the bill's provisions with the particulars of Driver's case. Rob Nicholson, a former minister in the Conservative government, similarly sidestepped making any connection when asked by a reporter in Ottawa on Thursday afternoon about the relevance of C-51.

Torture

New Democrats want Trudeau government to rescind torture directive
Canadian Press, Jim Bronskill, 2016 09 29
Ottawa - The NDP is calling on the Liberal government to immediately rescind a directive that allows security agencies to use information that may have been obtained through torture. The Liberals _ who opposed the ministerial directive while in opposition _ say it will be reviewed as part of a sweeping examination of national security policy. "The input of all Canadians, including all members of Parliament, is most welcome," said Scott Bardsley, a spokesman for Public Safety Minister Ralph Goodale. The New Democrats want the directive repealed now. Information obtained under torture is not reliable _ and therefore the practice does not ensure the safety of Canadians, NDP public safety critic Matthew Dube said Wednesday. Added Helene Laverdiere, the NDP foreign affairs critic: "Torture is immoral and goes against all of our international commitments on human rights. "This practice tarnishes Canada's reputation. The Liberal government must put an end to this directive." Goodale said earlier this year the Liberals would review the "troubling set of issues" raised by the foreign- sharing policy, enacted by the previous Conservative government. The policy applies to the Canadian Security Intelligence Service, the RCMP, the Canada Border Services Agency, the Communications Security Establishment and National Defence. Human rights advocates have roundly criticized it as effectively condoning the torture of people in overseas prisons, contrary to international law and Canada's United Nations commitments.

'Shady, secretive system': Public Safety green-lit RCMP, CSIS spying devices, documents reveal
CBC News, Laura Wright, 2016 09 22
Canadians have been kept largely in the dark about police and intelligence agencies' surveillance capabilities. But recent revelations in a Montreal court case that police are using electronic tools to scoop up mobile phone signals have prompted some experts to call for greater transparency in the approval and use of technologies that potentially violate privacy. The new documents reveal Public Safety Canada approved requests from the RCMP, Canadian Security Intelligence Service and the Defence Department granting 13 licences to an unnamed company (or companies) for the purpose of possessing, manufacturing or selling devices "used primarily for the interception of communications." The documents, which are heavily redacted and don't identify the manufacturers or the devices and their capabilities, were shared with CBC News by Ottawa-based investigative researcher Ken Rubin. "It's a part of the puzzle," Rubin said. "There are too many questions there. All I've uncovered is a link to how this rather shady, secretive system works, and there's no public understanding of it." Government won't identify devices The one- and two-year licences were issued beginning in 2015, and in some cases, they extend until 2018. One was granted to CSIS retroactively. They were granted under Section 191 of the Criminal Code, which says technology for the surreptitious interception of private communications is illegal, unless permission to use such technology is granted by the public safety minister. The RCMP wouldn't disclose what the licences are for. "We generally do not comment on specific investigative methods, tools and techniques outside of court," said spokeswoman Cpl. Annie Delisle. CSIS didn't reply to CBC's request for comment. Delisle said the RCMP has been appointed to review all licence applications made under Section 191, including doing background checks on the individuals or

companies that apply. If they pass the RCMP's vetting process, Public Safety officials are then asked to sign off on the licences. Some, called "special licences," last for two years. The RCMP said this type allows a company to possess the equipment, which is otherwise illegal to own. The licensee can then demonstrate the equipment to law enforcement and government agencies.

Ministerial directive on use of evidence obtained from torture still on books

CBC News, Nazim Baksh and Terence McKenna, 2016 09 20

Even as Ottawa remains locked in a decade-long legal battle with three Canadians who were tortured in Syria in a post-Sept. 11 crackdown on terror suspects, Canada's intelligence service is still allowed to act on information obtained through torture. Public Safety Minister Ralph Goodale could rescind the ministerial directive that one of his predecessors, Conservative Vic Toews, issued in 2009. But in a statement to CBC's the fifth estate, Goodale said he "continues to assess ministerial directives to ensure that they both protect our rights and freedoms, and keep Canadians safe." The original directive was updated in 2010 to specify that CSIS is only allowed to use information derived from torture in "exceptional circumstances where CSIS may receive urgent, perishable information from a foreign agency linked to a specific and imminent security threat to Canada or Canadians." When the directive made headlines in 2012, interim Liberal Leader Bob Rae called it "unprecedented in our history." "It, I think, reflects a complete breach of our international obligations with respect to torture," he said. "And I think it shows a government which has simply lost its way in terms of Canadian values. "This is not how we do business in Canada." Abdullah Almalki, Ahmad Elmaati and Muayyed Nureddin were never arrested in Canada for suspected terror offences, but all three were targeted by CSIS and the RCMP and eventually detained and tortured in Syria. Documents obtained by the fifth estate and The National show CSIS and the RCMP not only knew the men would be tortured, but co-operated with Syrian officials in their interrogations. When asked why the RCMP sent questions knowing that torture was a possibility, Richard Fadden, a security adviser to former prime minister Jean Chretien and later CSIS director from 2009- 2013, defended the move on grounds government officials were "acting in good faith" in order to "advance our national security."

The Torture Files: Documents show CSIS and RCMP's role in post- 9/11 torture of 3 Canadians in Syria

CBC News, Nazim Baksh and Terence McKenna, 2016 09 19

Thousands of pages of secret files obtained by CBC reveal how Canada's police and intelligence service not only knew three Canadians were being tortured in Syrian jails in a post-Sept. 11 crackdown, but co-operated with Syrian officials in their interrogations. The files also show a Canadian ambassador helped deliver questions the RCMP and CSIS wanted put to the Canadians imprisoned in Syria, a country with a dismal human rights record. The revelations are featured in "The Torture Files," a joint investigation by The National and the fifth estate that airs this week. Abdullah Almalki, Ahmad Elmaati and Muayyed Nureddin were never arrested in Canada for suspected terror offences, but to this day there is a cloud of suspicion hanging over them. Ten years ago, they each filed $100-million lawsuits against the government. Maher Arar, another Canadian arrested and tortured in Syria in the wake of al-Qaeda's deadly attacks on New York and Washington, received an apology and a $10.5-million settlement from the federal government in 2007. Lawyers representing Almalki, Elmaati and Nureddin fought and eventually won a lengthy court battle with the RCMP and CSIS to gain access to thousands of heavily redacted files, amounting to hundreds of thousands of pages. They consist of internal memos, briefing notes from field agents to their superiors, inter-agency communications, emails, reports and even a memo that shows at least one senior RCMP case officer might have had serious doubts about the evidence Almalki was engaged in anything nefarious. CBC News obtained exclusive access to some 18,000 pages, which the trio's lawyers plan to use when the long-anticipated civil trials begin early next year.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Chinese agents enter Canada on tourist visas to coerce return of fugitive expats
Globe and Mail, Nathan Vanderklippe and Robert Fife, 2016 09 21
Ottawa and Beijing - China's security services have been sending undercover agents into Canada on tourist visas to strong-arm expatriates to return home, including some suspected of corruption and other criminal activities. The secret Chinese visits have raised concern among lawyers and prompted investigations by the Canadian Security Intelligence Service and the RCMP, even as the Trudeau government begins negotiations for an extradition treaty with China. According to an insider briefed on China's secret-agent operation, the Chinese moved to tactics that include threats and intimidation because they were were "ticked off" at Canada for "not being willing to send people back the instant they asked" and for dragging its feet on an extradition treaty. "Nobody has been caught and nobody has been taken to court," the insider said. The revelation comes as Chinese Premier Li Keqiang arrives in Ottawa on Wednesday for talks with Prime Minister Justin Trudeau. The two leaders are expected to discuss the extradition treaty between China and Canada. Formal talks on the extradition treaty were approved in Beijing on Sept. 12 between a top Communist Party official and Daniel Jean, national security adviser to Mr. Trudeau. A day later, a Chinese court ordered the deportation to Canada of jailed Canadian missionary Kevin Garratt. Toronto refugee and immigration lawyer Lorne Waldman told The Globe and Mail some of his Chinese clients in Canada have received cellphone messages from Chinese security officials threatening them and their families if they do not return home. One client suspected that people watching him "might be from the Chinese government," he said. Mr. Waldman said he has worked with at least six people sought by China as fugitives. In the past year, two of them and the family of a third have been approached by CSIS agents who "asked them whether or not they had suffered harassment at the hands of those Chinese officials in Canada ... in relation to their return to China, or made any threats directed toward them." The most recent such meeting took place this summer when "the officers told my clients that CSIS was investigating whether or not this type of harassment is occurring," he said.

PM urged China to free Garratt: source
Globe and Mail, Nathan Vanderklippe, 2016 09 17
Ottawa - Prime Minister Justin Trudeau insisted in several meetings with China's top leaders that a new relationship would be difficult to forge between the two countries without the release of a Canadian man held for two years on suspicion of being a spy, a senior government source says. By the time Mr. Trudeau's first official visit to China was over, the release of Kevin Garratt seemed all but guaranteed, according to the official who had knowledge of the Prime Minister's discussions with Chinese President Xi Jinping and Premier Li Keqiang. But the assurances Mr. Trudeau received in return cast his visit to China in a new light. Instead of leaving Beijing with only relatively small gains, his doggedness allowed him to achieve one of his central ambitions - even if critics say the deportation of Mr. Garratt is a minor achievement next to more serious concerns about China's treatment of foreign investors and its own people. Mr. Trudeau's insistence was reflected in a visit from **Michel Coloumbe**, director of the Canadian Security Intelligence Service, who in an unusual step was dispatched to meet his Chinese counterpart four months ago to personally attest that Mr. Garratt was not a spy for Canada. Co-ordinated efforts from Foreign Minister Stephane Dion and Canada's ambassador to China, Guy SaintJacques, on top of previous attempts by Stephen Harper in 2014, helped to secure the release of a man whose lengthy detention in China on questionable charges had raised questions among Canadians, and anger in Ottawa.

Canada goes extra mile to secure Kevin Garratt's release from China
Globe and Mail, Nathan Vanderklippe & Laura Stone, 2016 09 16
Ottawa - The sudden release of a Canadian held for two years in China on suspicion of spying comes after a high-stakes campaign to secure his freedom, including an unusual and unannounced visit four months ago by the director of the Canadian Security Intelligence Service, who met with Chinese officials to try to persuade them that Kevin Garratt wasn't a spy. On Thursday, a bearded Mr. Garratt landed in Vancouver

and embraced his family, a free man. He had been accused by Chinese authorities of stealing military and defence research secrets and charged with espionage. His release puts a sudden end to a major irritant between Canada and China less than a week before Premier Li Keqiang arrives in Ottawa for an official visit, and caps an extraordinary effort by the government of Canada, its embassy in Beijing and two prime ministers to push for Mr. Garratt's release. The visit to China by CSIS director **Michel Coulombe**, Canada's top spy, was one element of that effort, according to multiple sources with knowledge of the meeting. When Mr. Garratt was indicted in January, China's state media said investigators had found evidence he had accepted tasks to gather intelligence for Canada. Mr. Coulombe met with Geng Huichang, the minister in charge of China's powerful state security apparatus, to deliver the message in person that Mr. Garratt, a Pentecostal pastor, did not work for CSIS. The Canadian had first come to China in 1984 and had taught English, operated a kindergarten, sold coffee and conducted humanitarian work in North Korea. He was a missionary, not a spy.

Others

CSIS suspends some bulk data mining programs pending new guidelines
Globe and Mail, Colin Freeze, 2016 09 30
Ottawa - Canada's domestic spy service has halted its "bulk collection" of data after criticisms were raised within government about the lawfulness of such technique. A watchdog agency's new report about the Canadian Security Intelligence Service speaks of littleknown CSIS data- mining programs, and of how some have recently been suspended because of a lack of clear rules and guidelines surrounding them. CSIS is said to have wanted to leverage big pools of data "to identify previously unknown individuals of interest by linking together types of information that have mirrored threat behaviour," according to the report. But after concerns raised in the report, "CSIS agreed to halt ingesting bulk data sets pending" new rules. These findings are from the Security Intelligence Review Committee (SIRC), the watchdog agency that tabled its annual report in Parliament on Thursday. The cryptic discussion of CSIS's "data management and exploitation activities" is intriguing on several levels. Talk of spies "ingesting" data in "bulk" has had connotations of intelligence officials indiscriminately amassing citizens' telecommunications records. Yet CSIS officers, who work to track terrorists within Canada, are generally understood to handle cases one wiretapping warrant at a time. This makes them more like conventional police detectives than the foreignfocused signals-intelligence - or "sigint" - spies who deal in volume. This week, the federal Privacy Commissioner called for Parliament to pass new laws after finding Canada's other intelligence agency had been careless with records about the logged telecommunications of Canadians. Communications Security Establishment (CSE), a foreignfocused "sigint" agency, says that whenever it collects Canadians' telecommunications trails, it does so only "incidentally." That's because it is pursuing foreign records in enormous volumes. While CSIS and CSE have vastly different mandates, they also have adjacent headquarters. They can team up if a Federal Court judge endorses a joint operation. In 2013, the former U.S. intelligence contractor Edward Snowden leaked documents to the media about the bulk collection of American citizens' telecommunications trails.

Maryam Monsef, Canada's first Afghan cabinet minister, says she was born in Iran
Canadian Press, Bruce Cheadle, 2016 09 23
Ottawa - A longtime refugee advocate says stories such as that of Liberal MP Maryam Monsef are not uncommon as families fleeing war and violence reconstruct their past in a new land. Monsef, widely touted as Canada's first Afghan-born cabinet minister, caused a stir in the capital Thursday when she issued a statement saying she only recently learned from her mother that she was in fact born in Iran. The 31-year-old minister of democratic institutions says she and her two sisters never held Iranian citizenship and were always considered Afghan citizens, but she was not born in Herat, Afghanistan, "as I was led to believe for my whole life." "It's fair to say I have experienced a range of emotions over the past few days

as I have tried to understand this with my family," said the statement. Monsef said she's learned she was actually born 200 kilometres from the Afghan border in Mashhad, Iran, in 1984. The revelation -- initially disclosed Thursday by the Globe and Mail newspaper -- prompted NDP immigration critic Jenny Kwan to question what she called the "troubling" Liberal cabinet vetting process. But Janet Dench, the executive director of the Canadian Council for Refugees, told The Canadian Press that after years of refugee work, "I really don't understand the significance." "To me it's like, 'Oh, she was born in a different month than she thought she was.' Why is this so exciting for us all?" And the Privy Council Office, the bureaucracy supporting cabinet, said potential ministers face "a rigorous vetting process" using information from the RCMP, the Canadian Security Intelligence Service, the Canada Revenue Agency and a bankruptcy and solvency check. "The same process is in place for all members of cabinet in this government and has been in place for a number of years," said PCO spokesman Raymond Rivet. As Liberal minister MaryAnn Mihychuk described the process Thursday, "for me they went through even my sock drawer, so it was pretty comprehensive from my point of view." U.S. President Barack Obama, in an address to Parliament earlier this year, made a point of noting Monsef's Afghan heritage as a sign of Canada's inclusiveness.

Discipline cases in Canada spy agency hit peak in 2015 -govt data
Reuters, Staff reporter, 2016 09 22
Toronto - The number of disciplinary cases in Canada's main spy agency nearly quadrupled over six years to reach 26 in fiscal 2015, before dropping to 13 the following year, government data showed. Just fewer than half of the incidents in the year ended on March 31, 2015, appeared to involve security issues, according to Canadian Security Intelligence Service data that Reuters obtained under access-to-information laws. The data showed just seven disciplinary cases in fiscal 2009. Canada's ruling Liberals ran on an election platform last year to increase oversight of the country's spy agencies and have said they plan to set up a parliamentary committee to do this. Reuters obtained summaries of the 63 CSIS disciplinary cases in the last three of the government's fiscal years. The files were redacted to the extent that some details were unclear or unavailable. For fiscal 2015, at least 12 cases clearly involved security matters. For the three years as a whole, there were 20. They include removing classified material from premises, bringing home "protected and secret" documents and sending classified information through "unsecure email." The CSIS invoked laws that allow withholding of information if releasing it would be "injurious" to international affairs, national defense or prevention of "hostile activities." A CSIS spokeswoman declined to provide more details on the cases, citing "national security and privacy," and said only that the agency had "strict policies" and "strict disciplinary measures." "I can assure you that these breaches of policy did not have an operational impact," she said. The CSIS did not address follow-up questions on the matter.

Terror suspects getting younger
National Post, Stewart Bell, 2016 09 14
Toronto - A 15-year-old who robbed a Montreal dépanneur to finance his plan to join the Islamic State of Iraq and the Levant. A Toronto girl of the same age caught at a Middle East airport on her way to Syria. In Winnipeg, a terrorist offence committed by a 16-year-old. Over the past two to three years, Canadian counterterrorism police have found themselves investigating minors as young as 13 - members of the online generation engrossed in extremism, some of them turned in by their families. "This is something that we've been seeing for a number of years now," RCMP Deputy Commissioner Mike Cabana said in an interview Tuesday. "And not just in Canada actually. It's in other countries as well. The same reality is there." The latest case emerged Monday, when the Public Prosecution Service of Canada announced a youth had pleaded guilty in Manitoba youth court for counselling the commission of an offence for the benefit of, or at the direction of, a terrorist group. In a few cases, police have dealt with adolescent extremists through terrorism peace bonds, including one for a young offender in Thunder Bay, Ont. In Toronto, police arrested an 18-year- old last September on a terrorism peace bond. Intelligence analyst Phil Gurski wrote in a September, 2015, blog post that while those involved in extremist violence were once in the 18-to-28 range, "we are seeing a worrisome development of late: a lowering of the

radicalization age." "But I think there is a silver lining. The younger the radical the greater the chance of diversion," wrote Gurski, who worked on radicalization at the Canadian Security Intelligence Service and Public Safety Canada. "As the radicals get older, the opportunities for success are smaller." Teenaged extremists may also be more likely to be detected. Assuming they live at home, their families will know if they have disappeared, and may notice changes in their behaviour or that they have been viewing terrorist propaganda on the Internet.

Fonctionnaires fédéraux en voyage : attention aux espions
Radio-Canada - Nouvelles (site web), Catherine Lanthier, 2016 09 12
Ottawa - « La menace qui pèse sur vous en tant que fonctionnaire canadien en voyage officiel est bien réelle. » Le Service canadien du renseignement de sécurité (SCRS) vient tout juste de mettre à jour ses directives sur les voyages à l'intention des fonctionnaires fédéraux. Obtenu par Radio-Canada Ottawa-Gatineau, ce document interne d'une quarantaine de pages insiste sur l'importance pour les employés du gouvernement d'être extrêmement prudents à l'étranger. Le SCRS soutient que « la menace terroriste qui pèse sur les Canadiens a changé » depuis les attaques survenues à Saint-Jean-sur-Richelieu et au Parlement canadien en octobre 2014.

CSIS to brief other agencies on operations
Globe and Mail, Colin Freeze, 2016 09 09
Ottawa - A controversial law that allows Canada's spies to engage in terrorism-disruption campaigns may pose problems for federal police and diplomats. For this reason, they are being given a peek at some CSIS operations - and even allowed to challenge them. Newly released records suggest that Bill C-51, the controversial 2015 omnibus bill that overhauled the Canadian Security Intelligence Service, has sent ripples throughout the federal-security bureaucracy. CSIS's so-called "threat-reduction activities" (or TRAs) have prompted fears of unintended fallout. To mollify concerns, the spy agency has committed to giving potentially affected agencies a heads up about what it is doing, according to records recently released to The Globe and Mail via access to information laws. For example, an "enhanced consultation memo" was recently signed between CSIS and Global Affairs Canada. While much is redacted in the undated document, CSIS promises to loop in foreign-affairs functionaries about things it is doing. "The Service will provide intelligence assessments ... of TRA measures which have a foreign policy component." On Nov. 24, 2015, CSIS Director **Michel Coulombe** and RCMP Commissioner Bob Paulson cosigned a memo where they agreed to have their lieutenants brief each other on counterterrorism probes. CSIS's "new mandate to reduce threats" could potentially increase the likelihood of the agencies "adversely affecting each other." Mr. Coulombe, the spy chief, told Parliament in March that such powers have been exercised only a couple of dozen times since the bill passed. Prior to that, he once testified that C- 51 could allow CSIS to "go into disrupting a financial transaction," or "disabling a mobile device" or "tampering with equipment." Yet these are among the more innocuous kinds of questionable tactics that global spy agencies engage in. The law says that CSIS officers cannot physically harm a suspect, but it can consider violating his or her Charter rights - so long as the minister and a Federal Court judge first approve.

How to stop a terrorist
Maclean's Magazine, Michael Friscolanti, 2016 08 29
The phone rang at 8:30 a.m.-and from that moment, the clock started ticking. "A race against time," to borrow the words of RCMP Deputy Commissioner Mike Cabana. On the other end of the line that Wednesday morning, Aug. 10, was an agent with the Federal Bureau of Investigation, calling to warn the Mounties about a chilling discovery: in a dark corner of the Internet (exactly where has yet to be disclosed) the FBI found an ISIS- inspired martyrdom video, starring a mystery man wearing a black balaclava. The would-be terrorist was planning an "imminent" attack, the agent said, location unknown. "Oh Canada, you received many warnings," said the masked man, his camera rolling. "You were told many times what will become of those who fight against the Islamic State?.?.?.?There is a fire burning in

the chest of every Muslim, and this fire can be cooled only by the spilling of your blood." Reciting a prepared script, the man wrapped up his two-minute rant by pledging allegiance to ISIS leader Abu Bakr al-Baghdadi, who "has called for jihad in the lands of the crusaders." "I'm responding to this call," he said. Over the next two hours, the RCMP and CSIS, Canada's spy agency, frantically pored over hundreds of photos in their investigative files, scrambling to figure out the man's identity-and where he might be. By 11:00 a.m., authorities were fairly certain they'd found their match: Aaron Driver, 24, a Saskatchewan-born Muslim convert who was anything but a stranger to Canada's national security apparatus. Of course, it also would have ended a lot differently if Driver hadn't been so arrogant and careless, posting his videotaped manifesto in advance of his planned attack. Or if the FBI had never noticed the clip in the first place. What's clear is that no Canadian official had any idea that Driver-an Islamist extremist well-known to police, arrested last year on suspicion of terrorism, and living under a court-ordered peace bond, which prohibited him (theoretically) from possessing explosives or using the Internet-was on the brink of targeting innocent civilians. "Let's look at this from the positive side and the not- so-positive side," says Phil Gurski, a former intelligence analyst at CSIS, and the author of The Threat from Within: Recognizing Al Qaeda-Inspired Radicalization and Terrorism in the West. "The positive side is that the FBI is an amazing partner of the RCMP and CSIS; it is an excellent relationship and there are constant exchanges of intelligence. But I can only imagine that in the highest echelons of CSIS and the RCMP, there is a lot of soul searching: 'OK, we've done good. But what did we miss-and how can we ensure we don't miss it next time?' "

Canada a 'target of direct threats' from ISIL and other extremists, government says in overdue report

National Post, Stewart Bell, 2016 08 26

Toronto - Canada's "principal terrorist threat" comes from those inspired by extremist ideologies to conduct attacks, the government said Thursday in its latest update on the security challenges facing the country. Released by Pubic Safety Minister Ralph Goodale just over two weeks after a failed ISIL-inspired suicide bombing in Ontario, the report said ISIL and its sibling al-Qaida "continue to appeal to certain individuals in Canada." Some promote violence online, radicalize their peers, recruit and fundraise, it said. "Others may consider travelling abroad to join a terrorist group or conducting terrorist attacks themselves," said the 2016 Public Report on the Terrorist Threat to Canada. As of the end of 2015, about 180 "individuals with a nexus to Canada" were suspected of participating in terrorist activities overseas, up from 130 the previous year, it said. The Canadian government has been struggling to deal with ex-foreign fighters since the conflict in Afghanistan in the 1980s and '90s, said Larry Brooks, a former Canadian Security Intelligence Service counter-terrorism official. The central problem is proving to the satisfaction of a Canadian judge that someone had engaged in terrorism in a foreign country, particularly the lawless ones where terrorist groups like al-Qaida and ISIL are based, he said. "It's tremendously difficult to collect credible evidence that would satisfy a Canadian court for prosecution," said Brooks, who was the operational manager of the CSIS investigation of the Toronto 18. "The challenges are significant."

One in five Canadian extremist travellers is a woman, federal report says

Canadian Press, Jim Bronskill, 2016 08 26

Ottawa - Women account for about one-fifth of extremists from Canada who head overseas, says the government's latest public report on terrorism. In some cases women have taken their children to conflict zones, says the annual assessment of the terrorist threat. The report issued Thursday says the participation of women in terrorist organizations is not new. However, there has been an increase in the number of women who have travelled or attempted to travel abroad to join the Islamic State of Iraq and the Levant. The report says it is often unclear what roles are performed by women who travel to join extremist groups. It notes the most common assumption is women travel abroad to marry terrorists, but some may occupy secondary roles within extremist groups, and in other cases appear to be training and taking part in combat. Groups such as Boko Haram in North Africa are using female suicide bombers to cause mass

casualties, the report adds. "Some of these women and girls were likely kidnapped and forced into the attacks, while others may be willing relatives of male fighters who have been killed." As of the end of 2015, the federal government was aware of approximately 180 people abroad with a nexus to Canada who were suspected of engaging in terrorism-related activities, the report says. More than half were believed to be in Turkey, Iraq or Syria. The figures are consistent with ones made public in February by CSIS director **Michel Coulombe**.

Fired CSIS agent with mental health issues suing the federal government
Ottawa Citizen, Andrew Duffy, 2016 08 23
Ottawa - A former spy agency employee with ties to the Paul Bernardo murder case is suing the federal government after being fired in the wake of a mental health crisis that resulted in criminal charges. A judge stayed those criminal harassment charges in October 2013, but by that time Martin McSweeney had already lost his top-secret security clearance and his job as a technologist with the Canadian Security Intelligence Service (CSIS). McSweeney had spent a decade with the national spy agency. He's now suing CSIS and the federal government for damages related to what he contends was his wrongful dismissal. Federal lawyers, however, want the lawsuit dismissed as an abuse of process.

Our wolves will come to you': ISIL ramps up anti-Canada propaganda after Ontario terror incident
National Post, Stewart Bell, 2016 08 18
Toronto - An image circulated by an ISIL propaganda outfit on Wednesday showed Toronto burning while a terrorist watched from nearby mountains, a wolf at his side. "Our wolves will come to you," it read. As expected, ISIL has ramped up its propaganda campaign against Canada following last week's police killing of Aaron Driver, an ISIL supporter in Strathroy, Ont. who was allegedly in the final stages of planning a bomb attack. Attempting to capitalize on the incident, the pro-ISIL al-Wa'd Foundation released two posters on its Telegram channel on Wednesday, including the one showing an apocalyptic Toronto, according to the SITE Intelligence Group. "O worshippers of the cross in Canada, now now fighting came, our wolves will come to you from where you will not know so you won't enjoy life," it read. The second poster showed a terrorist walking through a destroyed Toronto street. "Soon very soon," it read. ISIL makes heavy use of propaganda, much of it distributed on social media. A retired senior Canadian Security Intelligence Service official, Andy Ellis, said in April that Canadians were part of the ISIL propaganda wing, which valued their English-language skills.

Goodale seeks new anti-terror measures; Peace bonds have failed to stop extremists
Ottawa Citizen, Ian Macleod, 2016 08 18
Ottawa - Stronger anti-terror measures are needed after a court- ordered peace bond failed to stop jihadist Aaron Driver from making bombs and plotting an attack, Public Safety Minister Ralph Goodale said Wednesday. "What the incident shows is that peace bonds are tools and instruments with limited capacity, it's not a perfect solution to every situation," Goodale told reporters Wednesday after a speech to the Canadian Association of Chiefs of Police. One option would be to amend the Criminal Code to require professional de-radicalization counselling for individuals suspected as terrorist sympathizers "to change (their) behaviour," he said. Leading terrorism experts say the problem goes beyond court orders to keep the peace, especially when dealing with individuals willing to sacrifice their lives for the jihadist cause. Peace bonds are based on threat assessments by the RCMP, possibly with input from the Canadian Security Intelligence Service (CSIS).

Aaron Driver: Troubled childhood, ISIS supporter, terror threat suspect
CBC.CA, 2016 08 12
Ottawa - In a calm and collected tone, Aaron Driver told CBC News last year that he didn't think Muslims belonged in the West and that their ways of life weren't compatible with Canada's. In a nearly 90-minute phone conversation in June 2015 the then-23-year-old ISIS supporter, who was living in Winnipeg at the

time, spoke about his beliefs. "If a country goes to war with another country or another people or another community, I think that they have to be prepared for things like [the Parliament Hill shooting] to happen," Driver said. "And when it does happen they shouldn't, they shouldn't act surprised. They had it coming for them; they deserved it." On Wednesday, RCMP descended on the southwestern Ontario town of Strathroy after it said credible information of a potential terrorist threat was received earlier in the day. A memo circulated among National Defence personnel warning of a terrorist threat. CBC News later learned that Driver's family was told by the RCMP that police shot Driver after he detonated a device in the back of a cab, injuring himself and the taxi driver. The family was also told Driver had another device that he was going to detonate. At a news conference on Thursday, RCMP said Driver died in an altercation with police but it was unclear whether his death was a result of the explosive or from police fire.Before Driver caught the attention of the Canadian Security Intelligence Service, Canada's spy agency, in October 2014, he went through a difficult childhood and found Islam online in his teens. Driver was born to a Christian family in Regina.

Liberals still plan to repeal parts of counterterrorism powers brought in by Harper government
Ottawa Citizen, Jason Fekete and Marie-Danielle Smith, 2016 08 12
Ottawa - The Liberal government, following a thwarted terrorism plot, says it still plans to repeal parts of sweeping new counterterrorism powers adopted by the Conservatives and insists Canada must focus much more on counter-radicalization. Prime Minister Justin Trudeau's government came under fire Thursday from the opposition Conservatives over its plans to revoke some of the national security measures contained in the contentious Bill C-51, as well as for the Liberals' overall approach to fighting terror. Trudeau, who has been holidaying in British Columbia, didn't comment Thursday - leaving it to Public Safety Minister Ralph Goodale and the RCMP - prompting more criticism from interim Conservative Leader Rona Ambrose. Goodale told reporters the "disturbing event" serves to remind Canadians that the country is not immune to terrorism, insisting "unwavering vigilance is always required." "There is no greater responsibility for any government than to ensure public safety," Goodale said at a news conference in Regina. Nevertheless, Goodale said the Liberals still plan to live up to their election promise to repeal "problematic elements" of C-51. The Liberals want to guarantee that all Canadian Security Intelligence Service warrants respect the Charter of Rights and Freedoms; require that government review all appeals by Canadians on the no-fly list; and narrow overly broad definitions such as defining "terrorist propaganda" more clearly, among other measures.

Aaron Driver, ISIS sympathizer under peace bond, killed by police responding to terror threat
CBC News, Staff reporter, 2016 08 11
Aaron Driver, an ISIS sympathizer under a peace bond, was killed Wednesday night by police responding to what they call "a potential terrorist threat" in the small southern Ontario town of Strathroy. RCMP told Driver's family that police shot the 24-year-old after he detonated a device that injured himself and one other person, CBC News has learned. It's not clear who the injured person is. Police told the family they had to shoot Driver because he had another device and planned to detonate it. A senior police official told Canadian Press Wednesday the suspect allegedly planned to use a bomb to carry out a suicide mission in a public area. The deadly confrontation occurred while RCMP were conducting an operation in a residential southwestern Ontario neighbourhood of Strathroy on Wednesday evening after it said credible information of a potential terrorist act was received earlier in the day. "Earlier today, the RCMP received credible information of a potential terrorist threat. A suspect was identified and the proper course of action has been taken to ensure that there is no danger to the public's safety," according to an RCMP statement. "As this is still an unfolding matter and that the investigation is still underway, we are not able to provide further comment at this time." Driver, a known ISIS supporter, agreed to the conditions of a peace bond in a Winnipeg court earlier this year after being arrested in June 2015. By agreeing to the peace bond, Driver was "consenting or acknowledging that there are reasonable grounds to fear that he may participate, contribute -- directly or indirectly -- in the activity of a terrorist group." He first caught the attention of CSIS, Canada's spy agency, in October 2014 when he was tweeting support for the

militant group ISIS under the alias Harun Abdurahman. He has also said the Parliament Hill attack in October of that year by Michael Zehaf-Bibeau was justified. Ralph Goodale, minister of public safety and emergency preparedness, said in a statement Wednesday evening he had made Prime Minister Justin Trudeau aware of the situation.

Survol près du quartier général Les drones inquiètent le SCRS
La Presse+, Hugo De Grandpré; William Leclerc, 2016 07 27
Ottawa - Avis aux amateurs de drones : faire voler votre avion téléguidé près du quartier général des espions canadiens ne passe pas inaperçu à l'intérieur de l'immeuble sous haute surveillance. Des documents obtenus par La Presse en vertu de la Loi sur l'accès à l'information montrent que ces survols dans les environs du quartier général du Service canadien du renseignement de sécurité (SCRS), dans l'est d'Ottawa, causent une réelle agitation derrière les murs de l'immeuble triangulaire. Un agent a suivi cette recommandation à la lettre et a même avisé un autre service de renseignement, le Centre de sécurité des télécommunications(CST), de la présence d'un drone près du QGN.

Peace bond for man held on terror fears
National Post (Online), Stewart Bell, 2016 07 18
Toronto - A Toronto man arrested over police concerns he would travel abroad to engage in terrorism agreed Friday to the terms of a one- year peace bond that requires him not to communicate or associate with ISIL. At a court appearance in Brampton, Kadir Abdul, 27, signed a peace bond the RCMP had sought against him after he was arrested at Pearson airport on April 15 following his return from Turkey, where he had allegedly been detained. The peace bond restricts him from leaving Ontario. He cannot possess a passport or weapons. According to leaked ISIL documents, Abdul Malik, a Bangladeshi-Canadian, entered ISIL territory in July 2014. The contact number listed on his ISIL form matches a land line in Abdul's building. A man who answered the phone declined to comment. "You do your thing," he said. On his ISIL form, Malik said he was a "student" and wanted to be a fighter, rather than a suicide bomber. He named his reference as Abu Turab, believed to be ISIL member Mohamed Ali, from Mississauga, Ont. Aviles lives on the same Whitby, Ont., street as Kevin Omar Mohamed, who was arrested March 25 and charged with terrorism. The RCMP alleged Mohamed travelled to Turkey in 2014 to join Jabhat al-Nusrah, the al-Qaida faction in Syria. The **director of the Canadian Security Intelligence** Service has said the conflict in Syria and Iraq has attracted about 100 extremists with "a nexus to Canada." Another 90 to 100 have not left Canada but aspire to, he said.

New spy law protects old CSIS sources, court rules
Ottawa Citizen, Andrew Duffy, 2016 07 18
Ottawa - A new law designed to protect spy agency sources applies to old court cases, including the $100-million torture lawsuit launched by Ottawa's Abdullah Almalki, the Federal Court of Appeal has ruled. At issue in the case was a law that came into effect in April 2015 known as the Protection of Canada from Terrorists Act. It gave people who supplied information to the Canadian Security Intelligence Service (CSIS) the same kind of legal protections afforded police sources. The law made it illegal to disclose any information that could reveal the identity of a confidential CSIS source, even in a court proceeding. Last November, Federal Court Judge Richard Mosley ruled that the law could not be applied retroactively in a lawsuit filed by Almalki and two other Arab-Canadians tortured overseas in the aftermath of 9/11. The three men are suing federal officials for breaching their human rights and contributing to their detention and torture in Syria and Egypt.

CSIS tries to show it can be more 'accessible' with new Twitter account: 'Now it's your turn to follow us'
National Post, Stewart Bell, 2016 07 13
Ottawa - Canada's intelligence service posted its first Tweet on Wednesday, joining the Central Intelligence Agency and other secretive government organizations that have ventured into social media.

"Now it's your turn to follow us," the Canadian Security Intelligence Service wrote on its new @CSISCanada account. The handle @CSIS was already taken by the Centre for Strategic and International Studies. Among the first to follow CSIS was the CIA, which joined Twitter in 2014 with the post, "We can neither confirm nor deny that this is our first tweet." The @CIA account is heavy on history rather than actual intelligence. While CSIS already had a Twitter account for job openings, the new one appears to be an attempt to demystify the agency to Canadians who are sometimes wary of what it does in the name of national security. "Speaking publicly on the nature of our work isn't always easy, but we want CSIS to be more accessible, and want to help the public understand more about our work," Director **Michel Coulombe** said in a statement. Canada's signal's intelligence agency, the Communications Security Establishment, which has been Tweeting since April, welcomed CSIS to Twitter with what it called "some neighborly advice: 'password' is never a good password."

Watchdog condemns lack of diversity among CSIS senior staff

Globe and Mail, Laurent Bastien, 2016 07 02

Ottawa - The federal government's human-rights watchdog has repeatedly admonished the Canadian Security Intelligence Service over a lack of diversity in its upper echelons, according to newly disclosed reports. Records obtained by The Globe and Mail show that the Canadian Human Rights Commission has conducted two employment equity audits of CSIS over the past decade and, on both occasions, the spy agency was criticized because it had not hired a sufficient number of visible minorities, people with disabilities and indigenous Canadians. The 2014 and 2011 audits found that none of CSIS's senior managers were indigenous or visible minorities, and only 17 per cent are women, a decrease of 13 per cent since 2009. "Your organization has a lower overall EE [employment equity] result when compared to separate agencies and is therefore considered to be a less successful employer with respect to EE," the commission wrote, urging the agency to close gaps in its hiring practices. One of its main challenges, the commission noted, was to increase the diversity of its managerial staff. Formed three decades ago from a former RCMP intelligence division, CSIS is a $500-million-a-year organization with 3,000 employees.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L' INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS A L' INFORMATION

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

Comité permanent de la sécurité publique et nationale

EVIDENCE NUMBER 04,
TÉMOIGNAGES DU COMITÉ NUMÉRO 04

UNEDITED COPY - COPIE NON ÉDITÉE

Tuesday, February 23, 2016 - Le mardi 23 février 2016

* * *

(1105)

[*English*]

The Chair (Mr. Robert Oliphant (Don Valley West, Lib)): Good morning. I'm going to call to order this is the fourth meeting of the Standing Committee on Public Safety and National Security.

Thank you very much to our witnesses for joining us.

As the committee members will know we've received a notice of motion from Mr. O'Toole and I have checked with him and want to let the committee know that we'll be meeting within this meeting for the last 15 minutes to deal with his motion. He's agreed to that which does mean that each of these rounds will be 50 minutes as opposed to 60 minutes.

So we're going to welcome our guests, Mr. Paulson and Mr. Coulombe.

Mr. Paulson, will go first for 10 minutes. Welcome and thank you and we'll have both our witnesses at the first give their presentations and then the questioning will be opening and you can direct your questions to either of our officials.

Thank you.

Commr Bob Paulson (Commissioner, Royal Canadian Mounted Police): Thank you very much, Mr. Chair, and good morning members of the committee.

Thank you for the invitation and the opportunity to come to introduce the RCMP to you.

I don't have any prepared remarks. What I do have is a presentation that is in for translation. It is available in one language and will be distributed subsequently, along with the French version. I might just go off this presentation if that's all right with the committee. Thank you.

The idea is that I'll give you just a high-level overview of the organization, the RCMP: what it does, where its authority comes from, and some of the challenges we're facing in our present operating environment.

Of course the RCMP Actoutlines the mandate for the RCMP and it is essentially threefold: it provides for the apprehension of offenders, criminals; it provides for prevention; and it provides for the protection of specific individuals, so a threefold mandate in the RCMP Act.

We operate as one force but we have very many contexts, we have very many business lines. For example, federal policing is our core mandate; however, contract policing, where we provide front line police services to provinces, municipalities, and territories, is the largest part of our business. We also are engaged in specialized police services which support police activities across the country.

I've included in the presentation that you'll get the list of my senior executive committee and their functions.

The RCMP is about a $4.5 billion operation. Often when the estimates are provided they refer to the federal appropriations and they don't take into account the revenue that we receive from the contracting jurisdictions, making it a $4.5 billion operation.

In February of this year we had over 30,000 employees; 30,101 as of February 1. That occupies a variety of positions including what we would refer to as police officers, or what we refer to as regular members; civilian members, so civilian people hired to discharge our responsibilities under the act; public servants; and in many cases, municipal employees.

We have three operational business lines. I mentioned federal policing, and that includes organized crime, it includes terrorism, counterterrorism, investigations in partnership with my colleague, and enforcement of many other statutes in the federal context.

The specialized police services provide critical front line police services such as laboratory services, DNA services, information management services along the lines of CPIC. You may have heard of the Canadian Police Information Centre, so managing the existence of warrants, criminal records, fingerprints, and so on, and also child sexual offenders and cybercrime are in our specialized police services.

Contract and aboriginal policing services is what we refer to as our contract policing function. In all of the provinces, except for Ontario and Quebec, we are the provincial police force. We are the territorial police force in the three territories. We police over 600 aboriginal communities, 150 municipalities, and it is a big source of day-to-day complexity in terms of delivering police services to Canadians.

We, in the last several years, have undertaken efforts at our transformation. You will have heard much discussion around the cultural transformation of the RCMP. Efforts have been ongoing for years and have increased certainly in the last four years that I have been commissioner. We have worked towards restoring the traditional ethos of the RCMP. We have worked along the lines of developing a gender and respect action plan which came on the heels of a gender-based assessment of our policies and practices, stemming from the very public presentation of internal harassment issues and sexual harassment allegations within the organization.

(1110)

We've also succeeded in securing a new RCMP act called the Enhancing the RCMP Accountability Act, which has been very instrumental at bringing to bear a more repairing approach to discipline and human resource management.

We have developed a mental health strategy and deployed a mental health action plan, which is in place. And we've changed the mission profile of the organization to one that is called results and respect. While at the same time, trying to develop and maintain and promote a respectful workplace. Also, keep in mind that we are in the business of providing policing services to Canadians.

There remain challenges of course, some of which have been public just recently. There continues to be efforts at transforming the culture of the organization into one that is more tolerant and inclusive of all dimensions of our communities. We also have challenges in the area of labour relations as we move into a new world where RCMP members will have the opportunity to seek certification as a bargaining agent once the government completes its work on the new enabling legislation.

We have struggled with some RCMP funding shortfalls and challenges in respect to balancing our various responsibilities. We are engaging now in a complete program review, which will seek to put data around the demands that are being made on the organization. There is a continuing need for the ongoing maintenance of legal and investigative support tools as society evolves and threats evolve and present themselves.

Our strategic priorities continue to be along the lines of serious organized crime, national security, youth, aboriginal communities, and economic integrity. In the last few years we focused on some additional priorities which include national security investigations, cyber criminality, child sexual exploitation, and the workplace health of the RCMP.

The organization is very broad, it has 16 divisions. All of the commanding officers of those divisions report to me, along with the senior executive. The divisions are, for the most part, aligned with the provinces and territories. How you get to 16 is by adding Depot, our national headquarters, and an area called our National Division.

There is lots of work going on in lots of dimensions. It is a tremendous organizations comprising devoted and committed men and women who love the work they do. I'm very pleased to come here and help you understand the organization.

Thank you, Mr. Chair.

The Chair: Thank you very much, Commissioner.

Mr. Coulombe.

Mr. Michel Coulombe (Director, Canadian Security Intelligence Service): Good morning. I do have opening remarks.

[*Français*]

Bonjour, monsieur le président, mesdames et messieurs les membres du comité. J'ai le plaisir de comparaître devant vous aujourd'hui pour vous donner un aperçu du Service canadien du renseignement de sécurité, auquel je vais référer comme le SCRS pour le reste de la présentation, et vous entretenir brièvement sur les principaux facteurs et les grandes tendances qui influent sur la sécurité nationale du Canada et de ce qu'ils signifient pour le service et le Canada.

Mon objectif, aujourd'hui, est de vous donner une bonne idée de ce que nous faisons, des méthodes que nous utilisons et de nos priorités actuelles. Toutes les activités du SCRS s'appuient sur la Loi sur le Service canadien du renseignement de sécurité qui énonce clairement le mandat et les pouvoirs de l'organisme. Malgré les modifications qui ont été apportées à la loi, la plupart des principes fondamentaux qui régissent le service demeurent les mêmes.

(1115)

[*English*]

There are three main pillars to our mandate.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. REVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

First and foremost, we collect, analyze, and respond to activities suspected of constituting a threat to the security of Canada. Our act clearly defines the threats that we are authorized to investigate and in this regard have remained unchanged since 1984. We investigate espionage, sabotage, foreign interference, and of course, terrorism and extremism.

Of note, the CSIS Act explicitly excludes the investigation of advocacy, protest, and dissent unless it is carried out in conjunction with the previously mentioned threat related activities. It is important to note that the power to arrest, detain, and enforce the law remains the purview of our law enforcement partners. The service is not a police service.

We provide advice to government in a number of ways, including through the production of intelligence assessments and reports, which are disseminated to clients across the Government of Canada.

CSIS may also take measures to reduce threats to the security of Canada. These authorities are similar to those exercised by many of our foreign partners.

To fulfill the second pillar of our mandate, security screening, we provide advice and assessments to government partners. We share advice with our immigration partners to help them make decisions about an applicant's admissibility to Canada. We also provide security assessment to government partners to support the screening of employees and contractors who require access to sensitive government assets, sites, or information.

Lastly, section 16 of the act authorizes service to collect foreign intelligence in relation to the defence of Canada or the conduct of international affairs, but we may only do so at the written request of the Minister of National Defence or the Minister of Foreign affairs.

It is also important to note that this collection of foreign intelligence may only be undertaken within Canada and may not target Canadians or permanent residents. There have been no changes to this mandate.

In order to fulfill our mandate, CSIS maintains strong cooperative relationships with many federal partners and with provincial territorial authorities. These partnerships facilitate both lawful sharing of information and provision of advice as well as operational de-confliction. These relationships are essential to active CSIS investigations.

[*Français*]

La relation entre le SCRS et la GRC est essentielle pour contrer la menace terroriste. Les deux organismes comprennent bien leurs rôles respectifs et collaborent efficacement afin d'assurer la sécurité du public. Les poursuites contre des terroristes intentées avec succès depuis 2002, témoignes de l'engagement du service et de la GRC à l'égard de la lutte contre cette et de la priorité qu'on lui accorde.

Maintenant que j'ai décris sommairement le mandat du service, j'aimerais ajouter Monsieur le Président, que la surveillance et la réédition de compte étaient des facteurs importants au moment de la création du service en 1984, et qu'il continue de jouer un rôle de premier plan dans la façon dont le service mène ses activités aujourd'hui. Le service respecte de divers façons ses obligations de rendre compte d'abord, en donnant suite aux instructions que le ministre peut lui envoyer par écrit et qui peuvent porter sur toutes les questions qui touchent le SCRS, dont ses priorités en matière d'enquêtes et d'analyses et la conduites des opérations, ainsi que sur le moment et la façon dont le service informe le ministre de ses activités.

Le SCRS dois aussi soumettre à la probation du ministre les ententes de coopérations avec des partenaires canadiens et étrangers, ainsi que les demandes de mandats à la Cours fédérale. La loi sur le SCRS établie des exigences claires en matière de rapports, un autre élément clé de la réédition de compte.

Chaque année, le service rédige à l'intention du ministre, un rapport classifié sur ses activités opérationnelles, dont un exemplaire est remis à son organisme de surveillance, le Comité de surveillance des activités de renseignements dite de sécurité, le CSAR à des fins d'attestations.

Le CSAR peut alors vérifier que le SCRS mène ses activités de façon adéquate et efficace, en respectant le principe

de la primauté du droit. Le SCRS rédige aussi un rapport public, que le ministre dépose au Parlement et qui présente un aperçu de haut niveau des priorités opérationnelles du service et des faits saillants. Ils s'agit d'un moyen important de sensibiliser le public et d'éclairer le débat public.

(1120)

[*English*]

Of course, independent review is a significant element of the service's accountability regime. SIRC investigates and reviews CSIS activities and complaints—and it has access to all CSIS documents—excluding Cabinet confidences, and produces an annual report which is a summary of its review and complaint findings.

While the report is tabled annually, the dialogue between CSIS and SIRC is ongoing throughout the year as reviews and investigations into complaints evolve. SIRC's recommendations are given serious consideration and routinely inform service policies and practices. This fosters within CSIS a culture of continued learning and improvement.

Further, in terms of accountability, we appear regularly before Senate and parliamentary committees such as SECD and SECU, and are subject to review by the Privacy and Information Commissioners, as well as the Auditor General. These frequent interactions between the service and external review bodies help CSIS to become a more effective and professional organization.

This accountability is essential for public confidence and support, which is required for the service to be effective.

Mr. Chair, CSIS is a diverse and dynamic institution. It currently employs approximately 3,400 employees in six regional offices, overseas, and in our national headquarters here in Ottawa. Sixty-eight percent of our employees are bilingual and around 20% have a good or excellent knowledge of a language other than French or English. Collectively, our employees speak over 100 languages. The diversity of our employees ensures an engaged workforce, innovative thinking and ultimately helps us achieve our objectives.

CSIS is recognized as an employer of choice, and I am happy to report again this year for the eighth year in a row, CSIS has been named one of Canada's Top 100 Employers.

[*Français*]

Permettez-moi maintenant de vous donner un aperçu du contexte de la menace. Comme vous le savez, le terrorisme, notamment la radicalisation de Canadiens, demeure la menace la plus importante, la plus grave et la plus immédiate qui pèse sur les Canadiens et les intérêts canadiens aux pays et à l'étranger. Monsieur le président, il m'appartient de vous présenter la meilleure évaluation possible de la nature et de l'ampleur de la menace. Sans vouloir exagérer la menace terroriste, je crois fermement qu'il ne faut pas relâcher la vigilance dans un contexte complexe et en évolution constante et qu'il est risqué pour la sécurité des Canadiens de tenter de minimiser cette menace.

[*English*]

The Chair: Oh, one minute. Excuse me.

Mr. Michel Coulombe: It is important to understand that some people look at what happened in Ottawa in 2014 and will say that as tragic as the events were, in fact, it's only two events. But that to me is a wrong logic that forgets important factors.

[*Français*]

Le nombre de personnes présentement emprisonnées pour des activités terroristes, l'impact économique que des activités terroristes auraient sur notre pays, les victimes canadiennes d'attaques terroristes à l'étranger et ne pas oublier

les Canadiens qui ont participé à des activités terroristes à l'étranger comme en Algérie en 2013, donc il est important de garder la menace terroriste dans un contexte global et non pas seulement sur les incidents qui sont arrivés dans les dernières années. Sur ce, il me fera plaisir de répondre à vos questions.

[*English*]

The Chair: Thank you very much to both of you.

We begin our questions with Mr. Erskine-Smith. Seven minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thanks very much. Thanks to you both for the presentations.

I'd like to begin with the allegations against the two former RCMP instructors and the long and documented history of workplace harassment in the RCMP.

Mr. Paulson, can you update this committee with the status of the investigation, and when can we expect to receive a report?

(1125)

Commr Bob Paulson: Thank you for that question.

I think it would be helpful just to throw a little context around the allegations.

In April 2014, a complainant at the Police College in the explosives training unit came forward to make allegations relating to conduct in 2012-13 of two individuals. The director general of the Police College at the time ordered what we call a code of conduct investigation, and that went forward as it would have in the old system, ultimately resulting in four and five days' pay docked against the individuals whose behaviour was impugned.

In November of 2014, at about the time we switched to BillC-42, which is the new accountability act for the RCMP, another employee came forward and made another allegation of one of those two individuals. Let me just say that those two individuals had been suspended while the investigation took place in the first instance, and they went back to the Police College, but not directly to the work site. Managers there were somewhat challenged as they themselves started to complain about entitlement to their old employment and so on.

In any case, a new allegation came forward and that was handled pursuant to the new act, ultimately resulting in 15 days of discipline against that individual.

I want to point out just for a moment that the new act features an ability of the organization to review and, as it were, appeal instances of discipline where the view is perhaps it was not commensurate with the behaviours, which wasn't a feature of the old system. That process was underway up until the point where I got an email on February 9 from an individual who broadened again the allegations. That led to the almost-immediate transfer of those individuals. I wasn't acquainted with any of these facts, got acquainted with the facts, moved those individuals out of the workplace. A couple of days later a new code of conduct investigation was ordered, and they were suspended.

In terms of an update, we have an experienced team of investigators going in to investigate these new broader allegations which hadn't until then been known. We formed a multi-disciplinary team of individuals to do a couple of things while this investigation is ongoing to include making sure that the victims and the complainants are properly attended to and supported. Looking at the decision-making all along that spectrum of time I just described—

Mr. Nathaniel Erskine-Smith: Mr. Paulson, I don't want to cut you off, but I only have seven minutes, and I do have other questions. Is there a timeline that we can expect a report?

Commr Bob Paulson: Well, the code of conduct investigation is underway. The review of all those things is

underway and they are proceeding with all deliberate haste. I would say within, and I'm guessing so it would be a disservice to the men and women who are going in to do that work, so very quickly.

Mr. Nathaniel Erskine-Smith: Okay. In February 2012, the RCMP public complaints commission found rampant bullying in the police force. I note that in 2013 there was an action plan on gender and respect issued from your office that proposed 37 steps. How many of those 37 steps have been implemented by the force?

Commr Bob Paulson: Thirty-seven.

Mr. Nathaniel Erskine-Smith: All 37, great.

When individuals do complain, is there an opportunity for them to complain to an external party, or is it all done internally?

Commr Bob Paulson: There's an opportunity. People are free to complain to whomever. The process is one that includes internal paths, but we have created a number of different sort of points of access for lodging complaints.

Mr. Nathaniel Erskine-Smith: So at the moment there's no independent individual a complainant could go to, to avoid the process—

Commr Bob Paulson: Sure there is, sure. No, no, there is, a number of individuals. They could go to you.

Mr. Nathaniel Erskine-Smith: I see, but there's no designated individual by the RCMP?

Commr Bob Paulson: No.

Mr. Nathaniel Erskine-Smith: Thanks very much.

Moving to Mr. Coulombe, have preventative detention powers been used since Bill C-51 was adopted?

Mr. Michel Coulombe: That would be a Criminal Code enforcement and that wouldn't be the service. That would be the police forces that would (inaud).

Mr. Nathaniel Erskine-Smith: So let's move to something that is directly under CSIS, then. The new disruption powers, have they been used since Bill C-51 was adopted?

(1130)

Mr. Michel Coulombe: Yes, they have.

Mr. Nathaniel Erskine-Smith: With respect to information sharing, has information sharing increased since Bill C-51 was adopted?

Mr. Michel Coulombe: We'd have to go back and check. We have daily information-sharing. I wouldn't be able to say if it has actually increased since the Security of Canada Information Sharing Act came into force, but I can get to the committee with that.

Mr. Nathaniel Erskine-Smith: Thanks very much.

Now assume for the sake of argument that Bill C-51 has not been adopted. Other jurisdictions explicitly state the powers of intelligence agencies. If we were to do the same, what specific powers would CSIS require that were unavailable pre-C-51?

Mr. Michel Coulombe: We've talked about—and it's certainly timely with the debate in the U.S.—the issue of what is labelled as "going dark" or inability despite the fact that we have Federal Court warrants or the inability to intercept or obtain the information that we've been authorized to do by the court. There's a number of reasons, encryption, the

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. REVISE PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

data sitting outside Canada, etc., why that would certainly be a top priority for the service.

Mr. Nathaniel Erskine-Smith: I'm running out of time, but there was one concern with respect to seeking judicial authorization of Charter violations. Has that occurred since the adoption of Bill C-51?

Mr. Michel Coulombe: No.

Mr. Nathaniel Erskine-Smith: Thanks very much.

Just a final note, if you could report back to the committee with respect to information-sharing, it'd be most appreciated.

Mr. Michel Coulombe: Yes, I will.

Mr. Nathaniel Erskine-Smith: Thanks to you both.

The Chair: Thank you very much.

Mr. O'Toole.

Hon. Erin O'Toole (Durham, CPC): Thank you very much, Mr. Chair.

I'd like to thank you both very much, and through you to your organizations, the men and women that are at the forefront of public safety and security for Canada. Their work is appreciated. Certainly on this committee we also have to make sure that the organizations conform with the law and with the expectations. So please pass along that thanks and understand that's what we try and get at through the committee.

My first question would be for you, Commissioner Paulson. You spoke in your presentation in response on Bill. C-42 In particular, the Enhancing of the RCMP Accountability Act, which was passed by the past government, had a section on investigation of serious incidents of harassment, some of the very disturbing things we've heard. Has that act helped you internally get at the root issues and the culture change you spoke about in your remarks.

Commr Bob Paulson: Yes, it has.

Hon. Erin O'Toole: The one thing from the Explosives Training Unit that really concerned me was the allegation that in at least one of the cases the investigator of the complaint had previously been the subject of a harassment complaint. Can you give confidence to this committee that investigations will be undertaken by people that are basically blemish-free so that we can ensure that people making allegations don't fear that the investigator is someone that's had an issue?

Commr Bob Paulson: Certainly the people that I will be investigating harassment and associated kinds of behaviour would be free of allegations or harassment and that nature of allegation. Who among us is blemish-free? We are trying to get the organization to be inwardly accountable and outwardly accountable, and in doing so we hold our members and employees to very high standards of behaviour, so that what we would refer to as infractions against the code of conduct would not generally attract criminal liability or any other sort of liability.

Hon. Erin O'Toole: Commissioner, if I may, I think it would be quite easy to find a vast majority of RCMP members that are blemish-free when it comes to sexual harassment. As you said in your own—

Commr Bob Paulson: Well, you didn't frame that in your question. If they're free from—

Hon. Erin O'Toole: You described it as "bad apples", I think, in one of your speeches. How can we be sure that the people you draw to investigate these complaints are not bad apples, at least to make sure that they have not had previously a sexual harassment claim against them?

Commr Bob Paulson: Well, because we screen them.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. REVISE PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Hon. Erin O'Toole: Okay. You said the first incidence with the ETU situation came pre-C-42, the second came post-C-42. You've said Bill C-42 is helpful at getting at the root of these. Has the accountability act in that bill been widely communicated within the force and is it well-known the expectations throughout the human resources organization?

Commr Bob Paulson: Yes.

Hon. Erin O'Toole: Thank you.

Mr. Coulombe, thank you very much for your presentation.

I'm following up on Mr. Erskine-Smith's line of questioning. He's expressed concern about Bill C-51 before, although I notice his private member's bill is on shark fin soup, not on Bill C-51, or issues related to that. But some of his questions talked about disruption. Specifically he asked about how many people had been detained, so it doesn't appear that he understands that CSIS has no arrest powers. The disruption powers don't extend to CSIS as a police force, and you mention that in your remarks. Could you break out the difference between investigations, disruption, and how you engage law enforcement to arrest?

(1135)

Mr. Michel Coulombe: Like I mentioned, our first mandate is to investigate threat to the security of Canada, analyze that information and then advise government. One form of advice to government is informing or calling the RCMP. So if they meet their threshold, they can launch a criminal investigation. Like I mentioned, the Service doesn't have arrest power. We don't detain people and we're not in the business of collecting evidence to bring people to court. We collect intelligence to advise the government on that threat.

The same applies to the threat reduction. The threat reduction doesn't change that first pillar of our mandate. All it does it gives us the authority to use that intelligence to reduce the threat not again to detain people or charge them criminally. So we are not an enforcement agency.

The same with our screening program. We don't have the final word in terms of is somebody admissible or not. We provide advice to CBSA and Immigration and it's their decision.

Hon. Erin O'Toole: This committee has tried to look at radicalization and counter-radicalization but so far we've been blocked from a study on that. We'll be talking about that again at the end of today.

Working with Five Eyes Allies, this radicalization phenomenon through social media, we saw the 12 Canadian women travel to start families. We were all concerned about that last week.

Do you coordinate with other security agencies on the disruption piece to make sure that if someone returns to Canada with plans to cause harm, those are stopped?

Mr. Michel Coulombe: Yes, we coordinate, collaborate, exchange daily with foreign partners but also very important with domestic partners including on the threat reduction mandate. Before we will do a threat reduction measure, we will coordinate, consult with either the RCMP or other domestic partners.

Hon. Erin O'Toole: How much time left, Mr. Chair.

The Chair: A minute.

Hon. Erin O'Toole: One final question for you, Commissioner Paulson. You talked about CPIC. One part of CPIC is the identification data bank that municipal police forces, the RCMP, CBSA draw from to check criminal background, that sort of thing. The Minister of Public Safety has talked a lot about biometric screening and these sorts of things for the Syrian refugees. How many unknown persons in Syria would ever appear on the CPIC database when their fingerprints were run against it? Do you have an idea? It's essentially criminal activity in Canada by Canadians or

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. REVISED AS PER SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

landed immigrants, that sort of thing.

Commr Bob Paulson: I don't know. I don't know how many.

Hon. Erin O'Toole: CPIC is a great tool for law enforcement here but because it's a Canadian data base coordinated with the U.S. with very little impact on a fingerprint run from someone in Syria or Lebanon.

Commr Bob Paulson: I didn't answer your question.

The Chair: Very quickly.

Commr Bob Paulson: It keeps track of criminal records in Canada but it also is an option to diffuse information to frontline police officers on things that happen abroad.

[*Français*]

Le président: Monsieur Dubé, vous avez la parole.

M. Matthew Dubé: Merci, monsieur le président.

Merci, messieurs, d'être là aujourd'hui. Il est très important de dire, surtout quand ce sont des débats très émotifs avec le projet de loi C-51 que, malgré nos différences politiques, c'est certain qu'on appuie les hommes et les femmes qui travaillent au sein de vos agences. Là-dessus, je vais faire écho des commentaires de M. O'Toole.

Monsieur Paulson, vous avez parlé de l'impact qu'ont eu les budgets et les coupures. On a vu dans les rapports déposés par le président du Conseil du Trésor que l'ancien gouvernement avait coupé 687,9 millions de dollars par année au ministère de la Sécurité publique, dont 195 millions de dollars par année chez vous et 24,4 millions de dollars chez vous, monsieur Coulombe. J'ai deux questions à ce sujet: premièrement, pouvez-vous me parler de l'impact que cela a eu, brièvement élaborer sur votre commentaire? Et deuxièmement, qu'est-ce que le gouvernement actuel devrait faire dans son prochain budget pour combler les besoins que vous avez dans vos ministères?

(1140)

Comm. Bob Paulson: C'est assez clair et simple que si on n'a pas d'argent, on ne peut faire ce qu'on doit faire, il faut de l'argent pour faire le travail de policier, pour des enquêtes, pour faire tout ce qu'on fait au service des Canadiens. Cela dit, on ne peut jamais avoir assez d'argent, parce qu'il y aura toujours une menace quelque part, le moyen de comprendre une menace. C'est très difficile de dire ce dont on a besoin en ce qui concerne les montants d'argent. On est présentement engagé à faire une étude de nos activités, démontrer ce qu'on doit avoir pour faire le travail des enquêtes fédérales, des enquêtes au contrat et des services spécialisés. Je suis très confiant que si on peut démontrer au gouvernement ce que cela prend, on aura l'occasion de demander de l'argent.

M. Matthew Dubé: Merci.

Monsieur Coulombe, de votre bord, avez-vous senti les impacts de ces compressions? Si oui, que peut-on faire pour améliorer la situation?

M. Michel Coulombe: Les compressions de 24 millions de dollars étaient dans le cadre du Plan de réduction du déficit qui date de 2012. Le service s'était donné deux objectifs: le premier était que cela n'allait pas avoir d'impact sur nos activités opérationnelles et le deuxième était de garder nos ressources. On ne voulait pas de mises en pied d'employé et on a atteint ces deux objectifs. Il s'agissait vraiment d'essayer de trouver de l'efficience et de réduction de voyage de voyage, par exemple, en utilisant les téléconférences sécurisées. Le Budget principal des dépenses a été déposé ce matin et pour le service, on retrouve, dans le budget, une augmentation d'environ 6 %. Donc, les compressions de 2012 n'ont pas vraiment eu d'impact sur nous.

M. Matthew Dubé: Parfait.

Merci.

[*English*]

On another topic, the fight against radicalization here at home, that's something that we felt wasn't included in Bill C-51 and should have been. It's something we haven't talked about enough as far as we're concerned and under the current government either.

Are you folks being asked to be involved with some of the work that's being done? We had department officials here last Thursday saying a plan was being worked on. What can you tell us about that and are you being asked to work with faith communities and local authorities like Montreal, for example, that have been doing a lot of the heavy lifting on this file?

[*Français*]

M. Michel Coulombe: Je peux répondre.

[*English*]

—for the service we are actively engaged with Public Safety on that program within our mandate. We have a lot of experience. We've done a lot of analysis on factors that lead to radicalization, so we share that.

We exchange with foreign partners to get more knowledge. So we are actively working within our mandate with Public Safety on the program.

Commr Bob Paulson: In respect of, say, the foreign traveller phenomenon we work with the service and other government agencies to coordinate an operation centre. In there we look for opportunities to bring to bear counter-raicalizing resources from communities where these individuals are coming from, including families, including mental health, including additions, including counselling and we do that now as a matter of practical necessity.

Public Safety Canada is, as you've heard I think, engaged in trying to broaden and deepen the resources and the coordination of that activity and we're supporting that along with our partners.

Mr. Matthew Dubé: Great. Fantastic.

[*Français*]

On a parlé de C-51, encore une fois, à la rencontre de jeudi passé, on a cru comprendre de la part des gens du département que des changements s'en venaient. De votre bord, vous a-t-on demandé de participer à la révision et aux changements que le gouvernement s'est engagés à apporter à la loi? Si oui, que pouvez-vous nous en dire?

M. Michel Coulombe: Il est certain que le service sera partie prenante dans le processus de consultation, mais vous comprendrez que je vais garder mes avis et mes conseils pour le ministre. Le service participera au processus, le mettra en oeuvre et utilisera les outils qui ressortiront de la révision.

Comm. Bob Paulson: C'est bien dit.

M. Michel Coulombe: Merci, Bob.

M. Matthew Dubé: Je terminerais, monsieur Paulson, sur la question des filles et des femmes autochtones assassinées et disparues. Mme Bennett a fait des commentaires très dures à l'égard de certains aspects de la GRC la semaine passée, si je ne me trompe pas. Sans critiquer votre travail, vous a-t-on demandé de participer dans tout ce processus et dans le travail qui sera fait dans une enquête publique?

(1145)

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND/OR ACCESS TO INFORMATION ACT. REVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Comm. Bob Paulson: Oui.

M. Matthew Dubé: Pouvez-vous parler du rôle que vous envisagez et du travail qu'il reste à faire, selon vous.

Comm. Bob Paulson: Comme toujours, on est prêt à améliorer nos pratiques. On est toujours prêt à recevoir des critiques de n'importe qui. Selon moi, la réponse à la question de pourquoi les femmes autochtones sont aussi nombreuses parmi les femmes assassinées ou disparues ne se retrouvait pas dans nos enquêtes. Je vais le dire en anglais pour que ce soit plus clair.

[*English*]

Mr. Matthew Dubé: Sure, go ahead.

Commr Bob Paulson: My point is that we're always ready to improve our practices and our investigative responses and our processes. I can speak to that at length when you want, but our study and our work has been designed to bring some data to the issue.

Frankly, the answer to the question—Why are indigenous women over-represented in the cohort of women and girls who are killed or gone missing in suspicious circumstances?— doesn't lie in how we respond to the investigations of those people in those circumstances.

So I think it's a golden opportunity to understand what can be done to help our indigenous people and to the extent that we can take criticism on how we can do better, we're happy to do it.

The Chair: Thank you, Commissioner.

Ms. Damoff. You'll be a bit shy of seven minutes, just to warn you.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Okay, that's fine.

Thank you both for being here.

My question has to do with similar questions that were asked earlier.

Many people say the best way to change a culture in the organization around sexual harassment is to have women in leadership positions. In fact, I would probably say it's "the" best way to change the culture.

I'm wondering if you could let us know what you're doing to promote women to join the RCMP and also to put women into positions of leadership that are not just communications roles. Often in policing you'll see women who are in leadership, but they tend to be communications positions as opposed to other ones. I'm just wondering if you can let us know how many women are in leadership and what you're doing to do that within the RCMP.

Commr Bob Paulson: I'll briefly add how we're recruiting.

A couple of years ago I set some very ambitious targets, against some advice that it probably was not a good idea. We're targeting for a 30% representation of females in the organization by 2020, I believe. It's very ambitious, because of the numbers and the amount of intake. Nevertheless, we have targeted recruiting, bringing women into the organization, and those numbers are improving.

With respect to leadership roles, I agree with you. Right now we have a number of senior women in leadership roles, a deputy commissioner in Alberta. We have an assistant commissioner who is the commanding officer of Saskatchewan. I have a deputy commissioner here at headquarters who looks after contract and aboriginal policing.

While keeping that representation at that level is a challenge, because of keeping people coming up, what we are doing there is employing a mentoring type of philosophy to look into the, forgive the term, "feeder group" of individuals. Women don't want to get promoted because they're women; they want to get promoted because they're

good. We're looking at the women who are good, and we're bringing them along and attaching them to senior leaders, both men and women, in the organization to feed them.

We have succeeded in increasing our numbers in the executive ranks substantially in the last little while. I agree with you, and we're doing it.

Ms. Pam Damoff: Are you changing anything in terms of the work environment, itself, so that women are joining the RCMP? Certainly it's a challenge when—

Commr Bob Paulson: Certainly what we need to do is avoid the kind of public display of behaviour of this last week or two. To the extent that we have done a number of things, which I'm happy to enumerate, I thought we were advancing on that. That's why I tried to put some context around your colleague's question earlier on, to isolate that behaviour at the Police College.

We have some very robust, respectful workplace initiatives across this country, with consultative groups that are formed by the people on the frontline to advise on that, and our stats are going down.

Let me just add one other stat, because the CPC was referenced some time ago. In 2012 we had 219 harassment complaints, five of them were sex harassment; in 2013, 189, of which five were sex harassment. The CPC noted this, as well, in their review. Yes, we had a bullying problem—there's no question about that—and we're working on it. Recent events notwithstanding, I'm here to tell you that we're doing better.

But it can be understood as a sexual harassment problem. Sexual harassment has no place in the organization, don't get me wrong, but it's the culture of bullying, intimidation, and general harassment that I think needs everybody's focus and attention.

(1150)

Ms. Pam Damoff: Changing the subject a little bit, at our last meeting we were told that child sexual exploitation over the Internet is going up exponentially as well as organized crime and their work on the Internet. I'm just wondering, with the additional demands that you were talking about and the fact that you never have enough money—

Commr Bob Paulson: Yes.

Ms. Pam Damoff: —how are you dealing with the increase in those two crimes in particular?

Commr Bob Paulson: Well, they are going up exponentially. They are being facilitated and accelerated by technology. What we are doing is partnering with non-government agencies that are very interested in seeing some results there. We have developed a coordinating centre here in Ottawa on child sexual exploitation. We find it very difficult to sustain the workforce there because it is soul-destroying work, but it's also very rewarding work. We are building that capacity in partnership with other police agencies, and trying to bring to bear some technological support to counter what's going on.

I have a presentation that nobody wants to see. If you want to see it, I'll bring it here, but you're going to start crying in the middle of it and you'll get up and leave. I say that because it's the same phenomenon that happens in juries when they hear about terrible murders. Nobody wants to see that.

I think we need to, and I've embarked with the centre for child exploitation in Winnipeg, to start a socializing project to bring Canadian consciousness to just exactly what's going on there. It's a very difficult topic to share with the average Canadian.

The Chair: Thank you, Commissioner. I suspect we will be back to you.

Sorry for cutting you off. Because we have a motion to deal with later, we have to end your time with us. I know you look forward to coming back. We will, I am sure, have several reasons to call upon you. Thank you very much for your

work today.

We'll have a quick turnaround. We'll suspend for just three or four minutes while we change witnesses and get back to work.

(1155)

The Chair: We're going to reconvene, and thank both Mr. Head and Mr. Cenaiko for joining us. I know you especially look forward to coming to public safety and security committee meetings. We're going to have 10 minutes from each of you, and then the members will be able to question you at their will. We have 50 minutes again in this round.

We're going to begin with Mr. Head. He is still my model of a warden, having been the head of the Whitehorse Correctional Centre when I used to do chaplaincy services there. Now I know how jails are run, and he's still doing it and I'm not. I'm glad you're here.

Mr. Don Head (Commissioner, Correctional Service of Canada): Thank you, Mr. Chair. Every time I see you now, I'm not sure whether I should be giving testimony or giving a prayer. It really is a pleasure to—

The Chair: I pray more now...[*Inaudible*]

Mr. Don Head: Mr. Chair, honourable members of the committee, thank you and good day for allowing me to be here today.

I am pleased to appear before the committee to provide an overview of the Correctional Service of Canada or CSC as we refer to it in the short.

First, I'd like to take a brief moment to formally introduce myself to this committee. In my38 year career, I've had the privilege to work with tens of thousands of dedicated and committed correctional service employees. I began my federal public service career as a correctional officer in 1978 and I've held various operational, managerial, and executive positions working in four federal penitentiaries, two regional headquarters, and national headquarters.

Between 1995 and 2002, I accepted various positions within the territorial and provincial correctional systems in both the Yukon and Saskatchewan. In 2002, I rejoined the Correctional Service of Canada as senior deputy commissioner and was appointed commissioner in 2008. As the commissioner of the Correctional Service of Canada, I've appeared many times before this and other parliamentary and senate committees over the past eight years.

It's been such a privilege to be given the opportunity to provide members of this house and the senate with information on a broad range of matters concerning CSC, as pieces of legislation make their way through parliament or when committees undertake specific studies. Most importantly as the head of one of the Canada's public safety agencies, I believe that appearing in this type of public forum provides an opportunity for me to highlight the achievements and great work that my staff does every single day in the institutions and in the community.

CSC is a federal agency within the Government of Canada's Public Safety portfolio, who's responsibilities are derived from the Corrections and Conditional Release Act as well as the Corrections and Conditional Release Regulations. In addition to the Charter of Rights and Freedoms, approximately 70 other acts and regulations impact CSC.

The CCRA, Corrections and Conditional Release Act and Regulations direct CSC to contribute to public safety by administering court imposed sentences of two years or more. This work involves managing institutions of various security levels, preparing inmates for safe and timely release, and supervising offenders under conditional release and

PROCESSED PRESIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

long-term supervision orders in the community.

The CCRA also requires CSC to develop, implement, and monitor correctional policies, programs, and practices that respect gender, ethnic, cultural, and linguistic differences and are responsive to the specific needs of women, men, and indigenous offenders. As well the guiding legislation requires that CSC provide essential health care services and reasonable access to non-essential mental health care that will contribute to offenders' rehabilitation and successful reintegration into the community.

The act also mandates CSC to provide services to victims of crime such as information sharing and awareness building to support victims.

As commissioner, I'm supported by an executive committee comprised of national and regional officials. I oversee the operation of 43 federal penitentiaries, 91 parole offices and sub-parole offices, and 15 community correctional centres. The CSC also manages 4 healing lodges and works in partnership with indigenous communities to support the reintegration of indigenous offenders back into the community. On a typical day, CSC is responsible for approximately 23,000 offenders, of which roughly 15,000 are incarcerated.

Since assuming the role of commissioner in 2008, I've witnessed significant changes in the offender population, which have put pressures on CSC and its operations.

For instance, the number of women in federal custody has increased substantially over the last 10 years. Offenders now have more extensive histories of violence, are more likely to have mental health needs. Offenders continue to exhibit a high prevalence of substance of abuse problems and infectious diseases.

Furthermore, as offender populations age, the prevalence of physical health problems increases. The admission of indigenous offenders to the deferral correctional system continues to impact the level of overrepresentation in the system.

These changes have required CSC to change how it operates, to better respond to the offenders by enhancing intelligence and the information systems, implementing population management and mental health strategies, and regularly reviewing and modernizing the delivery of penitentiary operations and rehabilitation programs.

(1200)

Mr. Chair, as indicated in the 2015-2016 supplementary estimates tabled in the House of Commons last December, CSC's budgetary authorities is about approximately $2.4 billion. As with other government departments, CSC has faced significant funding reduction and pressures over the past several years. Budget 2012 Economic Action Plan resulted in the reduction of $295 million. Further the operating budget freeze announced as part of Budget 2014 has generated an estimated $27 million financial pressure for 2015-2016 and is expected to grow to $31 million for next fiscal year and ongoing. This is in addition to the Budget 2010 operating budget freeze which resulted in $55 million of ongoing financial pressure. Overall since 2008-2009 the total ongoing impact of funding reductions and pressures amounted to $400 million. In order to meet these budgetary reduction levels CSC implemented a series of initiatives intended to achieve efficiencies and streamline operations. At this time when you consider the cumulative impacts are government-wide and legislative initiatives which have had an impact on CSC, we're no longer in a position to absorb any other incremental costs without potential impacts on public safety results.

The Correctional Service of Canada employs approximately 18,000 staff, 85% of which work in institutions or in the parole offices in the community, and 15% work at our national or regional headquarters. CSC's workforce reflects the wide variety of skills needed to operate institutions and community offices such as correctional officers, parole officers, program delivery officers, health professionals, plumbers, electricians, food service staff, and the list goes on. These are staff that provide essential services both in the community and in the institutions. As well staff provide corporate administrative functions at local, regional, and national levels.

Like many other federal organizations, CSC must manage the challenges associated with recruiting and retaining staff because of the government-wide ageing workforce. That being said, CSC is committed to creating and retaining a

diverse workforce that is representative of Canadian society. A strong focus on fostering diversity has resulted in significant increases in the representation of women and visible minorities at CSC in the last three years. Given the high proportion of indigenous offenders CSC has made targeted efforts to recruit and retain indigenous employees and as a result is the largest employer of indigenous peoples in the core public administration. Of note in 2014-2015 47% of CSC's staff were women, 9% were visible minority groups, 5% were persons with disability, and just over 9% were indigenous peoples.

Mr. Chair, every day across the country CSC employees ensure the safety of our communities in one of the most challenging environments of the federal public service. CSC's contributions to public safety would not be possible without the passion and dedication of our staff.

Thank you once again for the opportunity to appear today. I'd be more than happy to respond to any questions that you have shortly.

(1205)

The Chair: Thank you, Commissioner.

Sort of the before and the after, Mr. Cenaiko, welcome.

Mr. Harvey Cenaiko (Chairperson, Parole Board of Canada): Thank you very much, Mr. Chair, and members of the committee for inviting the Parole Board of Canada to appear before you today.

I welcome this opportunity to talk to you about the board's important public safety mandate and the work that we do.

The Parole Board of Canada is an independent, administrative tribunal within the Public Safety portfolio. The Chairperson of the board is its chief executive officer and reports to parliament through the Minister of Public Safety and Emergency Preparedness. The board carries out its work through its national office located in the National Capital and through offices in five regions, which include the Atlantic, Quebec, Ontario, Prairie and Pacific regions.

Conditional release decision making takes place in the board's regional offices while appeal decisions and record suspension decision processes and clemency recommendations are made at the national office. The board has a complement of 89 full time and part time board members which is set in legislation. They are supported by a public service staff of 437 full time employees. The board's budget for the current fiscal year is $45.9 million.

As a key component of the criminal justice system, the board makes independent, quality conditional release and record suspension decisions and clemency recommendations. The board contributes to the protection of society by facilitating, as appropriate, the timely reintegration of offenders as law-abiding citizens. The board has three key program areas: conditional release decisions; conditional release openness and accountability; and record suspension decisions and clemency recommendations. These are supported by a fourth program area, internal services.

The board's conditional release program accounts for fully 77% of our budget while its record suspension program is funded under a cost recovery model through a $631 applicant user fee. The board's conditional release mandate is prescribed by the Corrections and Conditional Release Act—CCRA. The CCRA provides the legal framework for the board's composition, policies, training and operations. The board's mandate, in relation to record suspensions, is prescribed under the Criminal Records Act—CRA. The board's authority, in relation to clemency, and the Royal Prerogative of Mercy, is prescribed under the CCRA as well as the Criminal Code of Canada and The Letters Patent.

Board members are appointed by the governor in council, that is, by the Governor General, on the advice of the federal cabinet. Board members come from all walks of life and their diverse backgrounds help to ensure that the board represents Canada's broad range of community values and views. On appointment, all board members are provided with extensive training in risk assessment and interviewing techniques, as well as the legislation that governs the board's activities. Board members also receive ongoing training in their regions as well as annual training at the national level.

As I mentioned, the board's main program area is conditional release. Under the CCRA, the board has exclusive

authority to determine whether, and under what conditions, federal offenders serving a sentence of two years or more, may be released on parole. The board also makes decisions on parole for provincial offenders serving sentences of less than two years in all provinces except Ontario and Quebec, which have their own parole boards. Last year, the board conducted 17,800 parole reviews.

The CCRA includes two key principles that guide the board in its conditional release decision making. One, that the protection of society, be the paramount consideration in the determination of any case, and that the conditions we impose be necessary and proportionate to the purpose of the conditional release and consistent with the protection of society. Putting these principles into practice, the board looks at whether the offender will not, by re-offending, present an undue risk to society before the expiration of the sentence and whether the release of the offender will contribute to the protection of society by facilitating their reintegration as a law abiding citizen. The paramount consideration, in every board decision, is the protection of society.

In order to maintain the highest quality decision making possible, the board has developed a risk assessment framework that grounds all of its decisions in a sound analysis of risk relevant information. When conducting reviews, board members assess risk by taking into account actuarial measures and by considering and weighing relevant components of the risk assessment framework. These components include the offenders criminal and parole history, institutional behaviours, offender change, and their release plan, as well as any factor specific to the situation.

(1210)

Board members also consider information provided by the victim including formal victim statements. Board members consider mitigating, neutral, and aggravating factors, for all components and will take into account the information from the hearing or review, in order to render a final decision. This includes factors specific to Indigenous offenders. For example, the Supreme Court of Canada's decision on the Gladue principles in relation to attendance at residential schools, societal upbringing, and their own victimization.

The board is acutely aware that indigenous people are over-represented in the male and female offender population. To address the needs of this group the board provides alternate models of parole hearings, specifically Elder-Assisted and Community-Assisted Hearings which are responsive to the cultural values and traditions of indigenous peoples. In addition to this, the board has policies and specialized training that recognize the unique societal and cultural factors related to indigenous offenders, victims, and communities. The board also has an advisory committee known as the 'Indigenous Circle' which provides strategic advice to the board on ways it can improve its efficiency and effectiveness in meeting the needs of this community.

The board also uses elders to assist in interviewing candidates for board member positions. The board also believes that victims have an important role in the conditional release process and works hard to balance the rights of victims with those of offenders. Victims can receive information related to an offender's parole, they can attend and present victim statements at hearings, and receive written decisions. There are over 8,000 victims registered with the board receiving information on over 4,200 offenders.

Last year, there were 231 victim statements presented at 128 hearings, and 27,191 contacts with victims. In terms of the board's parole outcomes we have seen these improve to their highest levels in more than a decade and a half over the past two years. Last fiscal year, nearly 99% of federal day parole and 96% of federal full parole supervision periods for offenders serving determinate sentences were completed without reoffending with a grant rate of 71% for day parole and 30% for full parole.

As well, last year all parole periods, both day and full, were successfully completed without a violent offence conviction. This reflects the board's work over the past few years in developing a more robust risk assessment framework. Given its important public safety mandate it is critical that the board be seen as open and accountable to the public it serves. The CCRA requires that the board's decisions be made available to the public upon request. Over the last five years the board has released over 31,700 decisions through its Decision Registry. In addition, members of the public may also request to observe a board hearing. Last fiscal year, there were 4,171 observers at board hearings across the country.

As I mentioned at the outset the board is also responsible for making record suspension decisions under the Criminal Records Act. A record suspension removes the stigma of a criminal record for people who, having been convicted of an offence, have satisfied all of their sentences and remained crime free for a specific period of time.

As per the CRA the board needs to consider specific factors in deciding whether or not to order a record suspension including whether it will provide a measurable benefit to the applicant, how it will help sustain their reintegration into society as a law-abiding citizen, and whether ordering a record suspension would bring the administration of justice into disrepute.

Since 1970, more than 490,000 individuals have received pardons and record suspensions. Ninety-five per cent of these remain in force, indicating that the vast majority of pardon and record suspension recipients remain crime-free in the community. The board has also taken significant steps to address its backlog of pardon applications under the former Criminal Records Act. The board has reduced its backlog from over 22,400 applications down to approximately 4,480.

Under the CCRA, the board is also authorized to make recommendations for the exercise of clemency through the Royal Prerogative of Mercy. Clemency is granted in exceptional cases and circumstances in deserving cases involving federal offences where no other remedy exists in law to reduce severe negative effects of criminal sanctions. The board reviews clemency applications, conducts investigations at the direction of the Minister of Public Safety and Emergency Preparedness, and makes recommendations to the minister regarding whether to grant the clemency request.

I would like to thank you for the time. I would be more than happy to answer any questions that you have.

Thank you.

(1215)

The Chair: Thank you very much.

Mr. Spengemann.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Commissioner Head and Chairperson Cenaiko, thanks very much to you and your colleagues, first of all for your service to the nation, and for appearing in front of us today to discuss some very important matters. I'm very glad that you both raised the plight of our first nations in your comments. This is an area that I would like to follow through this afternoon.

Last week, on February 18, *Maclean's* magazine published an article titled "Canada's prisons are the 'new residential schools'". The article is subtitled "A months-long investigation reveals that at every step, Canada's justice system is set against Indigenous people".

I just want to bring one particular paragraph, early on in the article, to your attention, to give colleagues some awareness of the numbers that we're talking about. The article reads:

> While admissions of white adults to Canadian prisons declined through the last decade...

And this article specifically looks at the last decade.

> ...Indigenous incarceration rates were surging: Up 112 per cent for women. Already, 36 per cent of the women and 25 per cent of men sentenced to provincial and territorial custody in Canada are Indigenous—a group that makes up just four per cent of the national population. Add in federal prisons, and Indigenous inmates account for 22.8 per cent of the total incarcerated population.

That's almost a quarter, almost one in four people in our system.

If I put to you, and to colleagues around the table that I think we all agree that, as a society, as Canadians, we are all measured and judged each and every day by how well we take care of our most vulnerable members, this article really disturbs and saddens many of us. The question around the table really is how do we fix this? What's the systemic

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. REVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

problem that's plaguing us, and what are the resources that we need to put in place to correct it?

What I wanted to lead with is to get your reactions to this article, in particular, and ask you the extent to which both of you were aware of this problem in your organizational context prior to the release of this article.

Mr. Don Head: Maybe I'll go first. Thank you very much.

We're very aware of those numbers. We see them play out in our facilities and community parole offices on a day-to-day basis.

There is no question in my mind that just narrowly focusing on trying to deal with the overrepresentation of indigenous people in correctional facilities is just a narrow view. If you really want to tackle this issue, we have to go back to some of the systemic societal issues. We need to look at issues in relation to education, employment, and housing. We need to talk about the engagement of my colleague, Bob Paulson, and his colleagues across the country. We need to talk about how the courts look at this situation differently before sentencing, and then we can talk about corrections, as well.

We, unfortunately, are at the back end of this system, and we're expected to resolve all of the problems as they relate to indigenous people. In our legislation, we have a very specific section that requires us to provide the spiritual and cultural type programs and activities to support aboriginal people who want to pursue those paths, and we offer everything from elder services to sweat lodge ceremonies to aboriginally specifically designed programs. We have, for example, aboriginal substance abuse programs and aboriginal violence prevention programs. We offer these kinds of activities.

One of the challenges for us is how do the gains that those offenders make while they're in our care get supported when they're released into the community? For individuals who go back to any of the aboriginal communities, some of those communities don't have the kinds of support services or networks that are needed to carry on the good work that offenders commit to do personally and to work on. We need to look at how we bolster aboriginal communities to provide the support that returning individuals need, as well.

(1220)

Mr. Sven Spengemann: Can you give the committee a thumbnail sketch of what the substance abuse and anti-violence programs look like inside your organization? What kind of steps do you take?

Mr. Don Head: These are programs that specifically target what are called the criminogenic needs of offenders. This is based on evidence and research that's been done over decades. They would be programs that run anywhere from 8 to 16 weeks that target issues in relation to substance abuse or violence prevention in the two instances that I gave; we have other programs as well. There is an aboriginal, spiritual, cultural component that's built in to that, so an elder is part of the program delivery, and ceremony is part of the program delivery.

One of the things that we hear from aboriginal offenders in the system is that they sometimes have to come to jail in order to get back in touch with their culture. This isn't right, and this is something that—

Mr. Sven Spengemann: Sorry to cut you off. Time is limited.

Have either of your organizations conducted or commissioned any studies on this problem? If so, would you be able to share that work with the committee?

Mr. Don Head: We have some research reports that talk about the kinds of things that effectively work with aboriginal offenders when they are incarcerated.

In terms of the broader systemic issues, criminal justice system issues, we haven't commissioned any reports like that.

Mr. Harvey Cenaiko: In relation to the Parole Board, having come to the board in 2009, the biggest issue we had

was the education.

I'm from western Canada. I grew up close to a first nations community so my background and my knowledge is there, but many Canadians have never been involved or lived close to those communities, and many of our board members that have been appointed or are appointed don't have that so education of our board members is critical.

We have indigenous cultural awareness training going on throughout the year two times actually, one in English and one in French. The French training is going on next week in Montreal.

Mr. Sven Spengemann: Maybe a final specific question directed at the Parole Board.

One of the issues of deep concern for us, of course, is the missing and murdered aboriginal women. It's not just looking back and making sure we have a national inquiry, but also that we stop what's going on, that there are no further future cases.

Specifically on the Parole Board side, are there any programs that are aimed at first nations with respect to the propensity to reoffend, the release process, and the protection of women and children in particular through that process?

Mr. Harvey Cenaiko: Domestic violence again is extremely important as we look at individual programs. The programs are not provided by the Parole Board. They are provided through CSC. However there are programs available.

When those are brought to the Board's attention at the hearing or through the parole officer, we want to ensure those conditions are in place that the offender will have those opportunities to learn and/or get the training they need in the community, not just in the institution, but hopefully in the community where he can reintegrate himself back.

The Chair: Thank you, Mr. Cenaiko.

Monsieur Rayes.

[*Français*]

M. Alain Rayes (Richmond—Arthabaska, PCC): Monsieur le président, je vais partager mon temps avec mes confrères.

Merci de votre présence parmi nous aujourd'hui. J'ai deux brèves questions à poser.

Auparavant, je salue la réponse que vous avez donné à mon collègue d'en face. J'ai beaucoup été questionné sur le dossier des autochtones en situation carcérale et leur pourcentage d'incarcération par rapport à la population en général. Je considère que les gens prennent trop souvent un raccourci. Vous l'avez très bien signifié, c'est plutôt à la base qu'il faut travailler.

Dans une autre vie, avant d'être politicien et maire, j'ai été enseignant et directeur d'école. C'est à la base qu'il faut travailler dans les communautés pour éviter que les gens se retrouvent dans la situation actuelle. Il n'y a pas deux classes de citoyens. Lorsqu'un geste est posé, il y a une conséquence et je crois qu'il faut la respecter. Bravo pour votre réponse.

J'en reviens à ma première question. J'aimerais savoir la confiance du public envers notre système carcéral. Les gens se posent beaucoup de questions sur les délinquants qui obtiennent une libération conditionnelle. J'aimerais connaître le pourcentage des personnes incarcérées qui se rendent au bout de leur peine sans libération conditionnelle. Pouvez-vous répondre à cette question?

(1225)

[*English*]

Mr. Don Head: Thank you very much.

The percentage is very small. Those are individuals that we refer to under the legislation as individuals that are detained.

It's less than 5% of the population that are detained. The process required to do that is we have to present information to the Parole Board. The Parole Board—I'll let Mr. Cenaiko describe it in a little more detail—will have to make a determination as to whether the individual meets some very specific criteria that's set out in the Corrections and Conditional Release Act in terms of going to commit a serious violent offence, commit a serious drug offence, or commit a very serious offence against children.

If they meet that criteria the Parole Board can detain them. They could be detained right up to what we call warrant expiry, the end of their sentence.

But the number of individuals that fall into that category is less than 5%.

[*Français*]

M. Alain Rayes: Merci.

[*English*]

Mr. Harvey Cenaiko: In relation to the indigenous file or indigenous offenders, we have found through the elder-assisted hearings that we have or the community-assisted hearings that are done as well on occasion that those appear to be very successful for both the offender and for the offender going back into the community.

As I mentioned in my remarks, our statistics are such that 97% that are released do not commit another offence or are not convicted of another offence during the rest of that period of time they are on parole, so from the day they are on parole right through to their warrant expiry date that they haven't committed another offence.

These are tremendous results we're seeing so it shows that the programs that are being provided for in the institution are being carried through, and the conditions are being met as we move forward in safe reintegration of offenders back into the community.

[*Français*]

M. Alain Rayes: Merci, je vais passer la parole.

[*English*]

Mr. Larry Miller (Bruce?—?Grey?—?Owen Sound, CPC): Thank you to both witnesses for being here.

Mr. Cenaiko, I just want to continue on where you were going there. I think most people would agree that some people in the prison system are curable, if I could use that term. Some simply aren't. And there are some that should never see the light of day. And that's not just my words, I think most in the public would say that. I'll use an example: Paul Bernardo.

It seems whether it's every five years—you can tell me the number—people like Paul Bernardo's name will come up, and of course my office phones ring off the wall about it; "What the heck is wrong with our system?" "Why should this guy even be considered?"

Is there anything that you could do to reduce or eliminate that kind of reaction in society? There are some heinous crimes that were committed by certain people, and Bernardo is certainly one of them, that guy should never see the light of day. What could we do to appease the public on that issue?

As briefly as possible before I pass it over to my colleague here.

Mr. Harvey Cenaiko: Again, I think it's part education and the fact that all lifers—and I won't speak about one particular individual—have their first opportunity for a parole hearing at 22 years; three years prior to their 25 years. They will always be on parole. Lifers will never be released back into the community without being on parole.

Serious offenders, that's a good question.

Again, the legislation says that all offenders are eligible for parole based on the time period that a judge sentences them to. That's part of the justice system in Canada, that all offenders are eligible for parole, and we follow the legislation.

(1230)

Hon. Erin O'Toole: Thank you both for your work and the work done by your teams.

My question, Mr. Cenaiko, relates to one of your comments. You said the overarching issue is public safety. In fact, your words were "it's paramount" in all decisions about parole or early release.

Public Safety Canada has about 14 characteristics that are considered when the rehabilitation of an offender is considered for early release parole. Those would include things like understanding the impact of their crime, denunciation of past conduct, remorse for the victims. Can you talk about how those elements of rehabilitation are considered, particularly in the cases of violent offenders?

Mr. Harvey Cenaiko: As board members assess risk of an offender they look at the charges that the offender was convicted of. They'll look at any prior criminal history that he may have as well. But again, they'll look at societal issues, being a victim themselves in their own childhood, victimization of a victim, those types of issues.

But as well, they're looking at the institutional behaviour, the programming that the institution provides, and whether they're successful and they're engaged in the programming in the institution.

Hon. Erin O'Toole: If there is no remorse shown, or a lack of comprehension of the impact of their conduct, does that prevent release or parole?

Mr. Harvey Cenaiko: That would be one area that a board member would take into account. However, they're going to look at all of the factors. It's not just that one factor that will decide whether this individual is going to be released on parole or not. There are a number of factors that are looked into.

The Chair: Thank you, Mr. Cenaiko.

We're a little over time.

Mr. Dubé.

[*Français*]

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

[*English*]

Thank you both for being here.

Mr. Head, I just want to talk a bit about the last Parliament. There were a few tragic incidents related to solitary confinement, and there was a bit of semantic debate, both when you appeared at the Senate committee and also the questions that were asked of the minister. I'm asking these questions because, now with the new government, part of the Justice Minister's mandate letter—and this is sort of an overlapping issue between our committee and theirs in the justice committee—the minister has been asked to see that our practices come more in line with the United Nations

Commission on Human Rights.

What are your thoughts on that given the debate and notably the tragedy around Mr. Snowshoe.

Mr. Don Head: Yes, I think...a couple of things to note there.

This is an area we've been looking at very closely for the last several years in terms of how administrative segregation is used. That's the term that's in the legislation. People call it "solitary confinement", or they use other terms. We use the term that's just defined in the law for separating offenders from the general population.

Having said that, we've looked at our practices, we examined the oversight processes in place, and we're continuing finding ways to try to ensure we live up to the spirit of the law and live to the letter of the law as it relates to anybody who is placed in segregation.

Some of the work we've done just in the last year.... We were running on average, for decades, between 700 and 800 individuals in segregation on any given day across the country, out of an incarcerated population of about 15,000. We now are running between 410 and 440, and the length of stay of people in segregation is much reduced.

Some of the things we put in place are more engagement with mental health professionals for individuals who are in segregation, and more direct oversight by the wardens of those institutions. The wardens are required now to go down there daily and to see every offender in every cell in segregation.

We also have a more significant national oversight body that looks at finding an alternative. If an individual cannot be released back into the general population in the institution they're currently residing in, can they be moved to a general population in another institution in one of our regions, or can they be moved to another general population across the country?

(1235)

Mr. Matthew Dubé: Okay. Fair enough, I appreciate all of that.

You did touch on the mental health issue and we can look at the John Howard Society, for example, that argues that it sometimes seems that—and we can argue over the term—solitary confinement tends to target people with mental health issues, or aboriginal people.

Is that an assessment you agree with? Do you see that problem? Is that something you're seeking to rectify?

Mr. Don Head: Yes, on both fronts. This is a challenge for us and this is something we're working to rectify.

The problem we encounter at times with some individuals with mental health problems is that when they act up, as a result of a mental health problem, their behaviour is such that we have to move them somewhere for their protection and for the protection of others, so they're not assaulting people or so that they aren't assaulted by other offenders.

In cases where offenders are willing to agree to be placed in one of our psychiatric facilities—i.e., have the ability to give consent to receive psychiatric treatment—we would move them to one of the psychiatric facilities. However, if an offender has the ability to deny treatment we're left with very few options in the interim until we can find some other viable solution.

The staff work very hard to try to find solutions where the individuals can be placed back in general population.

Mr. Matthew Dubé: Okay. Thank you.

Hearing all this it's definitely something worthy of further study, especially given the changes that would be coming under the justice minister's mandate. Is that fair to say?

Mr. Don Head: Yes, I think you'll see that as we go forward there are a lot of changes we've made, there are a lot of

things that we have in consideration right now, and things that are feeding into the review by the justice minister.

Mr. Matthew Dubé: All right, I appreciate that. Thanks.

[*Français*]

L'autre sujet, c'est la question qui va monopoliser beaucoup de notre temps dans le prochain mois, ce sont les budgets. On sait qu'il y a eu beaucoup de coupures, des prisons ont été fermées dans les quatre dernières années et la question qui s'ensuit est à savoir si les ressources que vous avez sont suffisantes, parce qu'on sait qu'il y a des problèmes comme l'occupation double, par exemple? Contrairement à ce que l'ancien gouvernement disait, ce n'est pas pour être *hug-a-thug* au NPD, mais c'est surtout quelque chose que le syndicat amène par exemple, parce que c'est une chose importante pour la sécurité des agents correctionnels, entre autres. Considérez-vous que vous avez les ressources adéquates ou pensez-vous qu'il faudrait peut-être revoir cela en vue des coupures des quatre dernières années?

[*English*]

Mr. Don Head: I'll never turn down an offer of money in my organization.

Mr. Matthew Dubé: I've heard that more than once today.

Mr. Don Head: There is no question. As I mentioned in my opening comments, we're at a level now that any further cuts in our organization will have impacts on public safety results that we're supposed to provide. There is no question. Funding for additional mental health capacity although I still would argue, I do not want to be the default mental health system in the country for individuals. That needs to be dealt with in the provinces, in homes, in schools. There are other places to deal with that, not in a penitentiary setting.

However, until that is resolved, funding for mental health, funding for dealing with the disproportionate number of aboriginal offenders that we have in the system right now. One of the areas that we continue to need funding around is in relation to services for women although the overall population for women is small, federally sentenced women, it is the fastest growing population, sub population that we have. The women offenders that come into our system have greater needs than the men. Getting funding to ensure that we've got the right supports is key.

But I would also argue, sorry and I just have to squeeze this in, I would also argue that we need to find a way as a Canadian society to put in place the funding in the community to support the offenders when they go out. I can do a lot of work with the money that I have and if you give me more money, I can do more work and provide better results. But the offenders need the support when they get released. They need support in terms of family, they need support in terms of jobs, they need support in terms of housing and health care.

Find the funding for that and you don't have to give me any more money. We'll do the best job we can and feed into a system that will help these people on the path of being law-abiding citizens.

(1240)

[*Français*]

M. Matthew Dubé: Merci, monsieur Head.

[*English*]

The Chair: Thank you, Mr. Head.

Mr. Mendicino.

Mr. Marco Mendicino (Eglinton—Lawrence, Lib.): Thank you very much, Mr. Chair. I first of all want to attribute myself to the thanks have been provided by both the Chair and members of the opposition. My intent is to share some of my time with Ms. Damoff. I have two questions. One first that focuses on openness and transparency which is one of

the central themes on which we ran and were elected on. Specifically as it relates to the accessibility of decisions rendered by the parole board.

In your presentation you say that the CCRA requires the board's decisions to be made available to the public on request. But to put a finer point on it, it's just not a matter of requesting. There is a legal threshold that has to be reached in order to get access. Correct?

Mr. Harvey Cenaiko: Written request.

Mr. Marco Mendicino: But there needs to be something more than just an open request. Don't you have to demonstrate an interest in the case?

Mr. Harvey Cenaiko: Yes.

Mr. Marco Mendicino: Is easily met is what you're saying. That would explain why it is that you've got 31,700 decisions which have been released.

I noticed on the website that there isn't anything resembling a docket of when cases come up to the fore to be heard. Is that true?

Mr. Harvey Cenaiko: Yes, sir.

Mr. Marco Mendicino: Is there something within the statute that prohibits the parole board from creating something of a docket that there is transparency about these cases as they come up?

Mr. Harvey Cenaiko: That's a good question. That's a good question.

Mr. Marco Mendicino: That's why I'm here.

So perhaps that's something that you can take away.

Mr. Harvey Cenaiko: It's a legislative change that is required to open up the decision registry.

Mr. Marco Mendicino: I'm not talking about that in my latter question. I'm just talking about whether or not there's something within the act that prohibits there being a docket so that if the public wishes to see cases as they come up, they know. There's a separate question there about the contents of the decision and so on and so forth.

The hearings themselves are not presumptively open. There also needs to be a request in order to attend.

Mr. Harvey Cenaiko: There has to be a request because there is a security clearance check that has to be done by individuals going into entering into an institution.

Mr. Marco Mendicino: Thank you very much.

Mr. Head, my question is for you regarding radicalization. As part of our campaign platform, we are going to be creating something called the Office of the Community Outreach and Counter-radicalization Coordinator. That is a mouthful that we are working on I understand. Is that right, Mr. Chair, who knows.

The Chair: We don't know.

Mr. Marco Mendicino: There you are.

In any event, it's a very poly syllabic word and it would be helpful to reduce it.

But my question is this, have you encountered within your inmate population this phenomenon of both individuals who have been convicted of terrorist activity and those who have not for whom there is evidence that they are

embarking on this path and very briefly, what are some of the beginnings of the strategy that you have used within your institutions.

Thank you.

Mr. Don Head: Yes, so very quickly, this is something that we've been examining in quite detail. We actually have a few research reports that we have been leading. We currently have 13 individuals that fall under the definition of individuals who have been convicted of terrorist acts. So, our population base at this moment is small. So, we do not have immediate issues with those individuals. We're more concerned about those that are susceptible to being radicalized by some of those types of individuals.

Mr. Marco Mendicino: So, very briefly—because I do want to share some of my time with Ms. Damoff—could you tell us what are the two or three points? I'm happy to have you report back at some point in the future but what have you started to do to try and countervail those...?

Mr. Don Head: It probably would be better to have me come back in order to go into it because once I get going I probably won't be able to stop. But we are in the early stages of formulating a strategy and I would really love to share the information that we've gathered.

Mr. Marco Mendicino: Thank you.

Ms. Pam Damoff: Mr. Head, I know you've done a lot of work on mental health in the workplace. I'm just wondering if you could comment a little bit on occupational stress injury in your facility and also whether you think we would benefit from a national strategy. We have a bit of piecemeal going on, Ontario, different provinces and there's always a focus on the recovery of the individual but not so much on prevention, intervention and education. I'm just wondering if you can comment on whether you think that would be helpful for you, in corrections, and in the broader sense as well.

(1245)

Mr. Don Head: I cannot stress enough how important that is. My staff, on any given day, face just unbelievable situations that have tremendous impact on their mental resilience. That's the way we talk about it now, is how do we build and sustain the mental resilience of our staff who have, as I would argue, one of the toughest jobs in the federal public service.

We've started to work with the Mental Health Commission of Canadadelivering what is called the Road to Mental Readinessto all our staff across the country. This is a first step in us building up that capacity. This is more than just the employment assistance program kind of things. This is something that's very specific to the issue of mental resilience. If this committee was to take anything on along those lines I would be glad to be.... I don't really like offering up to come back to committee but this is one I would love to come and talk to you and share with you personal experiences of my staff and even experiences myself and what needs to be done to support individuals who deal with some very traumatic incidents.

Ms. Pam Damoff: Okay. I have just one really quick question. When you were talking about budget freezes. I understand that there are clients who require programs while they're in correctional services but you won't or can't provide them because of cutbacks. So in order to get parole they have to have completed these programs. So, they're a little bit stuck between the organizations. I was told that the John Howard Societywould provide these if they had the funding to do it. Are either of you aware of issues with this and how we might be able to deal with getting people out of correctional services and back out into the community and rehabilitated?

Mr. Don Head: There's actually a couple of issues there. The research is very clear that for low risk offenders delivering programs to them will not do anything. As a matter of fact we actually run.... The research shows very clearly we run the risk of actually pushing them in the wrong direction. So, we have stopped providing those kinds of programs to low risk offenders. One of the discussions that the Chair and I have is how do we position the work that those offenders do while they're incarcerated, position it in front of the board so that they can make a decision for release knowing that the program really isn't needed or required. So, that's one of the issues or challenges....

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT, REVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Ms. Pam Damoff: But it sounds like right now they are sort of caught in limbo between the two because they haven't done these programs so, therefore, they don't qualify for release. Is that...?

The Chair: I'm afraid I have to cut this off.

I think what I'm hearing is a standing invitation to both of you because we have lots to talk about.

I want to thank you on behalf of the committee for both your expertise and your ongoing public service. So, thank you very much.

Committee, we'll just say goodbye to the witnesses and then we have to get very quickly into a discussion on the motion.

The Chair: Okay, let's get back and going because as I understand, Mr. Miller has a commitment right away.

Mr. O'Toole, I give you the mike.

Hon. Erin O'Toole: Thank you, Mr. Chair.

The Notice of Motion is in front of you in both languages. Because of urgency of time, you can read it yourself. Do I have to read it for the record?

The Chair: Yes.

Hon. Erin O'Toole:

> The Committee undertake a study of now few than six meetings on the phenomenon of the radicalization of refugees, permanent residents and Canadians within Canada; that the committee call witnesses that are community organization leaders, academics and official experts to speak on the threat of radicalization and counter-radicalization strategies; that the committee travel to visit one anti-radicalization centre; that the committee make recommendations; and that the committee reports its findings to the House.

As my colleagues know, this is something that we from the first instance have wanted to look at. Each week, there seems to be more urgent need and this is continuing to come into focus, whether it's the story of the twelve women who travelled overseas; whether it's the announcement of the polysyllabic organization that Mr. Mendicino spoke about; whether it was touring Ban Ki-moon through one of these centres, I think we should as the Public Safety committee do the same thing so that we can learn, see and recommend to Parliament, addressing this issue and countering it.

I'm hoping we can get this on the agenda quite quickly.

(1250)

The Chair: Opened up for discussion.

If you just signal to me who wants to get on, Mr. Dubé and then Mr. Mendicino, and then we'll continue.

Mr. Dubé.

[*Français*]

M. Matthew Dubé: Merci, monsieur le président.

Il y a une première pour tout, alors, je vais être d'accord avec mes collègues conservateurs.

Je n'aime pas particulièrement la formulation, je n'aime pas qu'on mette les réfugiés en premier, parce que les cas dont on a entendu parler c'était surtout des gens qui habitaient déjà au Canada. Cet argument de vocabulaire à part, le NPD a été assez clair depuis le début, une des grandes lacunes, nous croyons, est de s'attaquer à la radicalisation ici chez nous.

J'apprécie notamment l'aspect d'aller visiter le centre à Montréal. C'est le genre de travail que nous devons faire et c'est une belle façon de combattre l'État islamique chez nous, donc j'offre mon appui à la motion de mon collègue M. O'Toole.

[*English*]

The Chair: Mr. Mendicino.

Mr. Marco Mendicino: Thank you, Mr. Chair.

First of all, I just want to say that, to a certain extent, I agree that this is an issue that has come up. We've heard about counter-radicalization from some of the witnesses. Mr. O'Toole said that he wanted to have the matter discussed very quickly. What I'm going to suggest right now is that we adjourn debate on this until the next meeting at which time we can consider this motion along with some of the other priorities which have emerged within the context of the witnesses and the briefings that we've received from senior officials.

The Chair: Is that a motion you're making to adjourn?

Mr. Marco Mendicino: Yes, it is, please.

The Chair: I believe that's not debatable. Am I correct on that?

So we have a motion on the floor which does not adjourn the meeting. It adjourns the debate on the motion, and it puts it into the next meeting which we would call for Thursday to do committee business and discuss all options for work.

Mr. Marco Mendicino: That's correct.

Thank you, Mr. Chair.

The Chair: It's not debatable so I will immediately call the question.

Do we have agreement to adjourn the debate on the motion until the next meeting?

Mr. Marco Mendicino: Are you asking for the yaes or are you asking for—

The Chair: Yes, if this is unanimous.

(Motion agreed to: yeas 5, nays 4)

The Chair: We will revisit this motion on Thursday.

Mr. Mendicino, just before you leave, I wanted to check something. Normally, a subcommittee on agenda and procedure is meant to speed up the work of the committee. We would normally meet as a subcommittee during a study, for instance, to continue committee work to get things done. My thought is—and I want to check it with the committee, I could call either one—that we would meet as a whole committee on Thursday to do committee business because if we have a subcommittee meeting it could actually slow down this work. That is because the subcommittee would have to take time for the clerk to write a report and we would have to consider the report. I'm worried we would actually debate the same issues in the full committee as we do at the subcommittee.

PROCESSED PRESIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE BUREAU VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

I would like a nodding of agreement or a no that we have a full committee meeting on Thursday. Mr. O'Toole's motion will be considered first at that meeting where we will do that. Because we will be in a meeting of committee business we don't need the 48-hour notice. If people have studies or concerns or things that they think the committee should be doing in the next couple of weeks, or months, be prepared to offer your motions. I think we'll design a process whereby we look at several motions and then choose one as a committee to begin and maybe set two or three pieces of work to help the analysts begin to do their work plan about where we'll be going between now and June.

Is that's agreed—I'm getting a kind of nodding—that we'll have a business meeting then, on Thursday?

(Motion agreed to)

The Chair: Okay.

Meeting adjourned.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Standing Committee on Public Safety and National Security

Tuesday, February 23, 2016

Question 1

Mr. Nathaniel Erskine-Smith: With respect to information sharing, has information sharing increased since Bill C-51 was adopted?

Mr. Michel Coulombe: We'd have to go back and check. We have daily information sharing, and I wouldn't be able to say if it has actually increased since the Security of Canada Information Sharing Act came into force, but I can get back to the committee with that information.

Mr. Nathaniel Erskine-Smith: Thanks very much.

RESPONSE

Effective and responsible sharing of information between institutions is critical to the Government's ability to protect Canadians. The *Security of Canada Information Sharing Act* (SCISA) provides an explicit authority for Government departments to share information with designated recipients where relevant to activities that undermine the security of Canada. It should be noted that *SCISA* does not in any way alter CSIS' mandate or collection authorities, nor does it expand the range of threats CSIS is authorized to investigate.

Each federal government institution is responsible for its own use and implementation of SCISA. It is important to note that while *SCISA* provides a legislative authority to facilitate information sharing, it does not obligate departments to share information. The decision to share information rests with the disclosing institution. As related recordkeeping is the responsibility of disclosing institutions, it is difficult to assess the overall impact on information sharing. CSIS can, however, confirm that it has indeed received information on numerous occasions that has been shared in accordance with *SCISA*.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Comité permanent de la sécurité publique et nationale

Le mardi 23 février 2016

Question 1

M. Nathaniel Erskine-Smith: Et y a-t-il eu communication d'information depuis l'adoption du projet de loi C-51?

M. Michel Coulombe: Il faudrait vérifier. Nous communiquons quotidiennement de l'information, et je ne pourrais vous dire si cela a augmenté depuis l'entrée en vigueur de la Loi sur la communication d'information ayant trait à la sécurité du Canada, mais je pourrais vous transmettre la réponse plus tard.

M. Nathaniel Erskine-Smith: Merci beaucoup.

RÉPONSE

Le partage d'informations doit se faire de façon efficace et responsable. Ceci est indispensable pour permettre au gouvernement d'assurer la sécurité des canadiens. La *Loi sur la communication d'information ayant trait à la sécurité du Canada* (LCISC) prévoit une autorité explicite permettant aux départements gouvernementaux d'effectuer le partage d'informations avec des institutions gouvernementales désignée, lorsqu'une activité qui porte atteinte à la sécurité du Canada est en jeu. La LCISC ne modifie aucunement ni le mandat du SCRS ni l'autorité sous laquelle est recueillie l'information. Également, la LCISC n'agrandit pas l'étendue des menaces dont le Service est autorisée à enquêter.

Chaque institution gouvernementale est responsable d'assurer la mise en œuvre adéquate de la LCISC. Bien que cette dernière octroi une autorité législative pour faciliter le partage, la loi n'y crée pas pour autant une obligation. La décision de partager de l'information demeure entre les mains de l'institution qui la possède. Comme la tenue des registres est du ressort individuel de chaque institution, il est difficile d'évaluer l'impact global sur le partage d'informations. Le SCRS peut toutefois confirmer avoir reçu de l'information à plusieurs reprises sous la LCISC.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

SENATE SÉNAT

CANADA

First Session
Forty-second Parliament, 2015-16

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

Proceedings of the Standing Senate Committee on

NATIONAL SECURITY AND DEFENCE

Chair:
The Honourable DANIEL LANG

Monday, February 22, 2016
Monday, March 7, 2016
Monday, March 21, 2016

Issue No. 2

Second, third and fourth meetings:
Examine and report on Canada's national security and defence policies, practices, circumstances and capabilities

and

First and second meetings:
Study on security threats facing Canada

WITNESSES:
(*See back cover*)

Délibérations du Comité sénatorial permanent de la

SÉCURITÉ NATIONALE ET DE LA DÉFENSE

Président :
L'honorable DANIEL LANG

Le lundi 22 février 2016
Le lundi 7 mars 2016
Le lundi 21 mars 2016

Fascicule nº 2

Deuxième, troisième et quatrième réunions :
Examiner, afin d'en faire rapport, les politiques, les pratiques, les circonstances et les capacités du Canada en matière de sécurité nationale et de défense

et

Première et deuxième réunions :
Étude sur les menaces à la sécurité nationale

TÉMOINS :
(*Voir à l'endos*)

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

52388-52409-52441

STANDING SENATE COMMITTEE ON NATIONAL SECURITY AND DEFENCE

The Honourable Daniel Lang, *Chair*

The Honourable Joseph A. Day, *Deputy Chair*

and

The Honourable Senators:

Beyak	Ngo
* Carignan, P.C.	Smith (*Saurel*)
(or Martin)	White
Kenny	
Mitchell	

*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 Beyak replaced the Honourable Senator Wells (*March 21, 2016*).

The Honourable Senator Wells replaced the Honourable Senator Beyak (*March 21, 2016*).

The Honourable Senator Smith (Saurel) replaced the Honourable Senator Dagenais (*March 18, 2016*).

The Honourable Senator Ngo replaced the Honourable Senator Runciman (*February 24, 2016*).

The Honourable Senator White replaced the Honourable Senator Manning (*February 24, 2016*).

The Honourable Senator Runciman replaced the Honourable Senator Ngo (*February 23, 2016*).

The Honourable Senator Manning replaced the Honourable Senator White (*February 23, 2016*).

COMITÉ SÉNATORIAL PERMANENT DE LA SÉCURITÉ NATIONALE ET DE LA DÉFENSE

Président : L'honorable Daniel Lang

Vice-président : L'honorable Joseph A. Day

et

Les honorables sénateurs :

Beyak	Ngo
* Carignan, C.P.	Smith (*Saurel*)
(ou Martin)	White
Kenny	
Mitchell	

* 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 sénatrice Beyak a remplacé l'honorable sénateur Wells (*le 21 mars 2016*).

L'honorable sénateur Wells a remplacé l'honorable sénatrice Beyak (*le 21 mars 2016*).

L'honorable sénateur Smith (Saurel) a remplacé l'honorable sénateur Dagenais (*le 18 mars 2016*).

L'honorable sénateur Ngo a remplacé l'honorable sénateur Runciman (*le 24 février 2016*).

L'honorable sénateur White a remplacé l'honorable sénateur Manning (*le 24 février 2016*).

L'honorable sénateur Runciman a remplacé l'honorable sénateur Ngo (*le 23 février 2016*).

L'honorable sénateur Manning a remplacé l'honorable sénateur White (*le 23 février 2016*).

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

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

ORDER OF REFERENCE

Extract from the *Journals of the Senate,* Tuesday, February 2, 2016:

The Honourable Senator Lang moved, seconded by the Honourable Senator Neufeld:

That the Standing Senate Committee on National Security and Defence be authorized to examine and report on security threats facing Canada, including but not limited to:

(*a*) cyber espionage;

(*b*) threats to critical infrastructure;

(*c*) terrorist recruitment and financing; and

(*d*) terrorist operations and prosecutions.

That the papers and evidence received and taken and the work accomplished by the committee on this subject during the Second Session of the Forty-first Parliament be referred to the committee; and

That the committee report to the Senate no later than December 31, 2017, and that it retain all powers necessary to publicize its findings until 180 days after the tabling of the final report.

After debate,

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

Le greffier du Sénat,

Charles Robert

Clerk of the Senate

ORDRE DE RENVOI

Extrait des *Journaux du Sénat* du mardi 2 février 2016 :

L'honorable sénateur Lang propose, appuyé par l'honorable sénateur Neufeld,

Que le Comité sénatorial permanent de la sécurité nationale et de la défense soit autorisé à examiner, afin d'en faire rapport, les menaces à la sécurité nationale, notamment :

a) le cyberespionnage;

b) les menaces aux infrastructures essentielles;

c) le recrutement de terroristes et le financement d'actes terroristes;

d) les opérations antiterroristes et les poursuites contre les terroristes.

Que les documents reçus, les témoignages entendus et les travaux accomplis par le comité sur ce sujet au cours de la deuxième session de la quarante-et-unième législature soient renvoyés au comité;

Que le comité fasse rapport au Sénat au plus tard le 31 décembre 2017 et qu'il conserve tous les pouvoirs nécessaires pour diffuser ses conclusions pendant 180 jours après le dépôt de son rapport final.

Après débat,

La motion, mise aux voix, est adoptée.

MINUTES OF PROCEEDINGS

OTTAWA, Monday, February 22, 2016
(3)

[*English*]

The Standing Senate Committee on National Security and Defence met this day at 1 p.m., in room 2, Victoria Building, the deputy chair, the Honourable Joseph A. Day, presiding.

Members of the committee present: The Honourable Senators Beyak, Carignan, P.C., Dagenais, Day, Kenny, Mitchell, Ngo and White (8).

In attendance: Dominique Valiquet and Katherine Simonds, Analysts, Parliamentary Information and Research Services, Library of Parliament.

Also present: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Tuesday, January 26, 2016, the committee continued its study on 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:

Reserves 2000:

Lieutenant-Colonel (Retired) John Selkirk, Executive Director.

Security Intelligence Review Committee:

The Honourable Pierre Blais, Chair;

Michael Doucet, Executive Director.

Office of the Communications Security Establishment Commissioner:

The Honourable Jean-Pierre Plouffe, Commissioner;

J. William Galbraith, Executive Director.

Office of the Auditor General of Canada:

Nancy Cheng, Assistant Auditor General;

Gordon Stock, Principal;

Nicholas Swales, Principal.

The chair made a statement.

Lieutenant-Colonel (Retired) Selkirk made a statement and answered questions.

At 2:02 p.m., the committee suspended.

At 2:07 p.m., the committee resumed.

Mr. Blais and Mr. Plouffe each made a statement and, together with Mr. Doucet and Mr. Galbraith, answered questions.

PROCÈS-VERBAUX

OTTAWA, le lundi 22 février 2016
(3)

[*Traduction*]

Le Comité sénatorial permanent de la sécurité nationale et de la défense se réunit aujourd'hui, à 13 heures, dans la pièce 2 de l'édifice Victoria, sous la présidence de l'honorable Joseph A. Day (*vice-président*).

Membres du comité présents : Les honorables sénateurs Beyak, Carignan, C.P., Dagenais, Day, Kenny, Mitchell, Ngo et White (8).

Également présents : Dominique Valiquet et Katherine Simonds, analystes, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 26 janvier 2016, le comité poursuit son étude sur les politiques, les pratiques, les circonstances et les capacités du Canada en matière de sécurité nationale et de défense. (*Le texte intégral de l'ordre de renvoi figure au fascicule n° 1 des délibérations du comité.*)

TÉMOINS :

Réserves 2000 :

Lieutenant-colonel (à la retraite) John Selkirk, directeur exécutif.

Comité de surveillance des activités de renseignement de sécurité :

L'honorable Pierre Blais, président;

Michael Doucet, directeur exécutif.

Bureau du commissaire du Centre de la sécurité des télécommunications :

L'honorable Jean-Pierre Plouffe, commissaire;

J. William Galbraith, directeur exécutif.

Bureau du vérificateur général du Canada :

Nancy Cheng, vérificatrice générale adjointe;

Gordon Stock, directeur principal;

Nicholas Swales, directeur principal.

Le président fait une déclaration.

Le lieutenant-colonel (à la retraite) Selkirk fait une déclaration, puis répond aux questions.

À 14 h 2, la séance est suspendue.

À 14 h 7, la séance reprend.

MM. Blais et Plouffe font chacun une déclaration puis, avec MM. Doucet et Galbraith, répondent aux questions.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

At 3:16 p.m., the committee suspended.

At 3:19 p.m., the committee resumed.

Ms. Cheng made a statement and, together with Mr. Stock and Mr. Swales, answered questions.

At 4:18 p.m., the committee suspended.

At 4:20 p.m., the committee resumed in camera pursuant to rule 12-16(1)(d) for the consideration of a draft agenda (future business).

At 4:32 p.m., the committee adjourned to the call of the chair.

ATTEST:

À 15 h 16, la séance est suspendue.

À 15 h 19, la séance reprend.

Mme Cheng fait une déclaration puis, avec MM. Stock et Swales, répond aux questions.

À 16 h 18, la séance est suspendue.

À 16 h 20, la séance se poursuit à huis clos, conformément à l'article 12-16(1)d) du *Règlement du Sénat*, afin que le comité examine un projet d'ordre du jour (travaux futurs).

À 16 h 32, le comité s'ajourne jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

Le greffier du comité,

Adam Thompson

Clerk of the Committee

OTTAWA, Monday, March 7, 2016
(4)

[*English*]

The Standing Senate Committee on National Security and Defence met this day at 12:57 p.m., in room 2, Victoria Building, the chair, the Honourable Daniel Lang, presiding.

Members of the committee present: The Honourable Senators Beyak, Carignan, P.C., Dagenais, Day, Kenny, Lang, Mitchell, Ngo and White (9).

In attendance: Dominique Valiquet and Katherine Simonds, Analysts, Parliamentary Information and Research Services, Library of Parliament; Marcy Galipeau, Communications Officer, Senate Communications Directorate.

Also present: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Tuesday, January 26, 2016, the committee continued its study on 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:

Canadian Security Intelligence Service:

Michel Coulombe, Director.

National Defence and the Canadian Armed Forces:

General Jonathan Vance, Chief of the Defence Staff.

Canada Revenue Agency:

Cathy Hawara, Director General, Charities Directorate, Legislative Policy and Regulatory Affairs Branch;

OTTAWA, le lundi 7 mars 2016
(4)

[*Traduction*]

Le Comité sénatorial permanent de la sécurité nationale et de la défense se réunit aujourd'hui, à 12 h 57, dans la pièce 2 de l'édifice Victoria, sous la présidence de l'honorable Daniel Lang (*président*).

Membres du comité présents : Les honorables sénateurs Beyak, Carignan, C.P., Dagenais, Day, Kenny, Lang, Mitchell, Ngo et White (9).

Également présents : Dominique Valiquet et Katherine Simonds, analystes, Service d'information et de recherche parlementaires, Bibliothèque du Parlement; Marcy Galipeau, agente de communications, Direction des communications du Sénat.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 26 janvier 2016, le comité poursuit son étude sur les politiques, les pratiques, les circonstances et les capacités du Canada en matière de sécurité nationale et de défense. (*Le texte intégral de l'ordre de renvoi figure au fascicule n° 1 des délibérations du comité.*)

TÉMOINS :

Service canadien du renseignement de sécurité :

Michel Coulombe, directeur.

Défense nationale et les Forces armées canadiennes :

Général Jonathan Vance, chef d'état-major de la Défense.

Agence du revenu du Canada :

Cathy Hawara, directrice générale, Direction des organismes de bienfaisance, Direction générale de la politique législative et des affaires réglementaires;

Alastair Bland, Director, Review and Analysis Division, Charities Directorate, Legislative Policy and Regulatory Affairs Branch.

The chair made a statement.

Mr. Coulombe made a statement and answered questions.

At 2 p.m., the committee suspended.

At 2:05 p.m., the committee resumed.

General Vance made a statement and answered questions.

At 3:08 p.m., the committee suspended.

At 3:34 p.m., the committee resumed.

Ms. Hawara made a statement and, together with Mr. Bland, answered questions.

At 4:35 p.m., the committee suspended.

At 4:40 p.m., pursuant to the order of reference adopted by the Senate on Tuesday, February 2, 2016, the committee began its study on security threats facing Canada.

WITNESSES:

Public Safety Canada:

Monik Beauregard, Senior Assistant Deputy Minister, National and Cybersecurity Branch;

Patrick Boucher, Acting Director General, Critical Infrastructure and Strategic Coordination Directorate;

Suki Wong, Director General, National Security Operations Directorate;

Colleen Merchant, Director General, National Cyber Security Directorate.

The chair made a statement.

Ms. Beauregard made a statement and, together with Mr. Boucher, Ms. Wong and Ms. Merchant, answered questions.

At 5:20 p.m., the committee suspended.

At 5:22 p.m., pursuant to rule 12-16(1)(d), the committee resumed in camera for the consideration of a draft agenda (future business).

At 5:27 p.m., the committee suspended.

At 5:30 p.m., the committee resumed in public.

The Honourable Senator Mitchell moved:

That the following budget application (as it pertains to the order of reference dealing with security threats facing Canada) for $190,158 for the fiscal year ending March 31, 2017, be approved for submission to the Standing Committee on Internal Economy,

Alastair Bland, directeur, Division de l'examen et de l'analyse, Direction des organismes de bienfaisance, Direction générale de la politique législative et des affaires réglementaires.

Le président fait une déclaration.

M. Coulombe fait une déclaration, puis répond aux questions.

À 14 heures, la séance est suspendue.

À 14 h 5, la séance reprend.

Le général Vance fait une déclaration, puis répond aux questions.

À 15 h 8, la séance est suspendue.

À 15 h 34, la séance reprend.

Mme Hawara fait une déclaration puis, avec M. Bland, répond aux questions.

À 16 h 35, la séance est suspendue.

À 16 h 40, conformément à l'ordre de renvoi adopté par le Sénat le mardi 2 février 2016, le comité entreprend son étude sur les menaces à la sécurité nationale.

TÉMOINS :

Sécurité publique Canada :

Monik Beauregard, sous-ministre adjointe principale, Secteur de la sécurité et de la cybersécurité nationale;

Patrick Boucher, directeur général par intérim, Direction générale des infrastructures essentielles et de la coordination stratégique;

Suki Wong, directrice générale, Direction générale des opérations de sécurité nationale;

Colleen Marchant, directrice générale, Direction générale de la cybersécurité nationale.

Le président fait une déclaration.

Mme Beauregard fait une déclaration puis, avec M. Boucher ainsi que Mmes Young et Merchant, répond aux questions.

À 17 h 20, la séance est suspendue.

À 17 h 22, conformément à l'article 12-16(1)d) du *Règlement du Sénat*, la séance se poursuit afin que le comité examine un projet d'ordre du jour (travaux futurs).

À 17 h 27, la séance est suspendue.

À 17 h 30, la séance publique reprend.

L'honorable sénateur Mitchell propose :

Que la demande de budget suivante, découlant de l'ordre de renvoi relatif aux menaces à la sécurité nationale et s'élevant à 190 158 $ pour l'exercice se terminant le 31 mars 2017, soit approuvée aux fins de présentation au Comité permanent de la

Budgets and Administration following a final review by the Senate administration that will be overseen by the Subcommittee on Agenda and Procedure.

GENERAL EXPENSES	$ 0
Activity 1:	
Halifax & Washington	101,546
Activity 2:	
Montreal & Regina	88,612
TOTAL	$ 190,158

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

The Honourable Senator Mitchell moved:

That the following budget application (as it pertains to the order of reference dealing with Canada's national security and defence policies, practices, circumstances and capabilities) for $14,742 for the fiscal year ending March 31, 2017, be approved for submission to the Standing Committee on Internal Economy, Budgets and Administration following a final review by the Senate administration that will be overseen by the Subcommittee on Agenda and Procedure.

GENERAL EXPENSES	$ 14,742
TOTAL	$ 14,742

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

At 5:32 p.m., the committee adjourned to the call of the chair.

ATTEST:

La greffière intérimaire du comité,

Shaila Anwar

Acting Clerk of the Committee

Le greffier intérimaire du comité,

Kevin Pittman

Acting Clerk of the Committee

régie interne, des budgets et de l'administration après l'examen final réalisé par l'Administration du Sénat et supervisé par le Sous-comité du programme et de la procédure.

DÉPENSES GÉNÉRALES	0 $
Activité 1 :	
Halifax et Washington	101 546
Activité 2 :	
Montréal et Regina	88 612
TOTAL	190 158 $

La motion, mise aux voix, est adoptée.

L'honorable sénateur Mitchell propose :

Que la demande de budget suivante, découlant de l'ordre de renvoi relatif aux politiques, aux pratiques, aux circonstances et aux capacités du Canada en matière de sécurité nationale et de défense et s'élevant à 14 742 $ pour l'exercice se terminant le 31 mars 2017, soit approuvée aux fins de présentation au Comité permanent de la régie interne, des budgets et de l'administration après l'examen final réalisé par l'Administration du Sénat et supervisé par le Sous-comité du programme et de la procédure.

DÉPENSES GÉNÉRALES	14 742 $
TOTAL	14 742 $

La motion, mise aux voix, est adoptée.

À 17 h 32, le comité s'ajourne jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

OTTAWA, Monday, March 21, 2016
(5)

[*English*]

The Standing Senate Committee on National Security and Defence met this day at 1:01 p.m., in room 2, Victoria Building, the chair, the Honourable Daniel Lang, presiding.

Members of the committee present: The Honourable Senators Beyak, Carignan, P.C., Day, Lang, Mitchell, Ngo, Smith (*Saurel*), Wells and White (9).

In attendance: Dominique Valiquet, Analyst, Parliamentary Information and Research Services, Library of Parliament.

OTTAWA, le lundi 21 mars 2016
(5)

[*Traduction*]

Le Comité sénatorial permanent de la sécurité nationale et de la défense se réunit aujourd'hui, à 13 h 1, dans la pièce 2 de l'édifice Victoria, sous la présidence de l'honorable Daniel Lang (*président*).

Membres du comité présents : Les honorables sénateurs Beyak, Carignan, C.P., Day, Lang, Mitchell, Ngo, Smith (*Saurel*), Wells et White (9).

Également présent : Dominique Valiquet, analyste, Service d'information et de recherche parlementaires, Bibliothèque du Parlement.

Also present: The official reporters of the Senate.

Pursuant to the order of reference adopted by the Senate on Tuesday, January 26, 2016, the committee continued its study on 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:

Canada Border Services Agency:

Martin Bolduc, Vice President, Programs Branch;

Caroline Xavier, Vice President, Operations Branch.

Communications Security Establishment:

Greta Bossenmaier, Chief.

The chair made a statement.

Mr. Bolduc made a statement and, together with Ms. Xavier, answered questions.

At 2:05 p.m., the committee suspended.

At 2:08 p.m., the committee resumed.

Mr. Bossenmaier made a statement and answered questions.

At 3:08 p.m., the committee suspended.

At 3:31 p.m., pursuant to the order of reference adopted by the Senate on Tuesday, February 2, 2016, the committee continued its study on security threats facing Canada.

WITNESSES:

As individuals:

Stephanie Carvin, Assistant Professor, International Relations, Norman Paterson School of International Affairs;

Adam Chapnick, Professor and Deputy Director, Education, Canadian Forces College, Department of National Defence;

Kevin Quigley, Associate Professor and Director, MacEachen Institute for Public Policy and Governance;

Andrew Graham, Adjunct Professor, School of Policy Studies, Queen's University.

The chair made a statement.

Ms. Carvin and Mr. Chapnick made statements and answered questions.

At 4:30 p.m., the committee suspended.

At 4:34 p.m., the committee resumed.

Mr. Quigley and Mr. Graham made statements and answered questions.

Aussi présents : Les sténographes officiels du Sénat.

Conformément à l'ordre de renvoi adopté par le Sénat le mardi 26 janvier 2016, le comité poursuit son étude sur les politiques, les pratiques, les circonstances et les capacités du Canada en matière de sécurité nationale et de défense. (*Le texte intégral de l'ordre de renvoi figure au fascicule n° 1 des délibérations du comité.*)

TÉMOINS :

Agence des services frontaliers du Canada :

Martin Bolduc, vice-président, Direction générale des programmes;

Caroline Xavier, vice-présidente, Direction générale des opérations.

Centre de la sécurité des télécommunications Canada :

Greta Bossenmaier, chef.

Le président fait une déclaration.

M. Bolduc fait une déclaration puis, avec Mme Xavier, répond aux questions.

À 14 h 5, la séance est suspendue.

À 14 h 8, la séance reprend.

M. Bossenmaier fait une déclaration, puis répond aux questions.

À 15 h 8, la séance est suspendue.

À 15 h 31, conformément à l'ordre de renvoi adopté par le Sénat le mardi 2 février 2016, le comité poursuit son étude sur les menaces à la sécurité nationale.

TÉMOINS :

À titre personnel :

Stephanie Carvin, professeure adjointe, Relations internationales, Norman Paterson School of International Affairs;

Adam Chapnick, professeur et directeur adjoint, Éducation, Collège des Forces canadiennes, ministère de la Défense nationale;

Kevin Quigley, professeur agrégé et directeur, MacEachen Institute for Public Policy and Governance;

Andrew Graham, professeur auxiliaire, École des études sur les politiques publiques, Université Queen's.

Le président fait une déclaration.

Mme Carvin et M. Chapnick font chacun une déclaration, puis répondent aux questions.

À 16 h 30, la séance est suspendue.

À 16 h 34, la séance reprend.

MM. Quigley et Graham font chacun une déclaration, puis répondent aux questions.

At 5:30 p.m., the committee adjourned to the call of the chair.

ATTEST:

Le greffier intérimaire du comité,

Mark Palmer

Acting Clerk of the Committee

Le greffier intérimaire du comité,

Kevin Pittman

Acting Clerk of the Committee

À 17 h 30, le comité s'ajourne jusqu'à nouvelle convocation de la présidence.

ATTESTÉ :

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

EVIDENCE

OTTAWA, Monday, February 22, 2016

The Standing Senate Committee on National Security and Defence met this day at 1 p.m. to examine and report on Canada's national security and defence policies, practices, circumstances and capabilities.

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

[*English*]

The Deputy Chair: I call to order this meeting of the Standing Senate Committee on National Security and Defence. Honourable colleagues, we will hear from three panels over a period of three and a half hours today.

We will begin with an appearance by retired Lieutenant-Colonel John Selkirk. This is not his first appearance. We welcome you back, colonel.

Retired Lieutenant-Colonel John Selkirk is the Executive Director of Reserves 2000. We have invited the colonel to appear before the committee to provide an update on the state of Canada's reserve force. According to its website, Reserves 2000 is a coalition of Canadians who wish to preserve the militia as a viable option in Canadian defence capabilities.

This committee issued a report in December 2011 entitled *Answering the Call: The Future Role of Canada's Primary Reserve*, and that report is on our website for anyone who would like to see what our position was in December 2011.

We are very pleased to have Lieutenant-Colonel Selkirk with us this afternoon to update us on the reserves and to talk about emerging issues.

The floor is yours, sir.

Lieutenant-Colonel (Retired) John Selkirk, Executive Director, Reserves 2000: Thank you for this opportunity to share some thoughts on the current state of manning of the militia, or the Army Reserve; that is, the army portion of Canada's Primary Reserve. The Primary Reserve also consists of components from the navy, air force and some headquarters elements.

I am not here to talk about everything that Senator Day mentioned, because I prepared myself to comment in particular on the shortfall that was reported for 2015 of 5,293 Primary Reserve personnel. That was recently reported to the House of Commons. I am happy to talk about that in particular, then to take other questions you may have regarding any aspect of the militia, keeping in mind that I am not and have not been a serving officer for some period of time. But the coalition that Senator

TÉMOIGNAGES

OTTAWA, le lundi 22 février 2016

Le Comité sénatorial permanent de la sécurité nationale et de la défense se réunit aujourd'hui, à 13 heures, pour examiner les politiques, pratiques, conditions et capacités du Canada en matière de sécurité nationale et de défense et pour en rendre compte.

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

[*Traduction*]

Le vice-président : Je déclare la séance ouverte. Il s'agit d'une réunion du Comité sénatorial permanent de la sécurité publique et de la défense. Chers collègues, nous entendrons trois groupes au cours des trois heures et demie qui suivent.

Nous commencerons par entendre le lieutenant-colonel à la retraite John Selkirk. Ce n'est pas la première fois que nous le recevons. Soyez le bienvenu, colonel.

Le lieutenant-colonel à la retraite John Selkirk est le directeur exécutif du groupe Réserves 2000. Nous l'avons invité pour qu'il nous donne un bilan de la situation de la force de réserve canadienne. Selon la description qu'en fait son site web, Réserves 2000 est une coalition de Canadiens désireux de préserver la milice comme solution viable dans le cadre des forces de défense du Canada.

En décembre 2011, le comité a publié un rapport intitulé *Répondre à l'appel : le rôle de la Première réserve du Canada dans l'avenir*, qui se trouve sur notre site web et peut être consulté par tous ceux qui souhaitent savoir quelle était notre position à l'époque.

Nous sommes très heureux d'accueillir le lieutenant-colonel Selkirk cet après-midi et de nous entretenir avec lui des réserves et des enjeux émergents.

Vous avez la parole, monsieur.

Lieutenant-colonel à la retraite John Selkirk, directeur exécutif, Réserves 2000 : Merci de me donner la possibilité de partager quelques réflexions sur la situation actuelle de la dotation de la milice ou, si vous préférez, de la Réserve de l'Armée de terre, c'est-à-dire de la section militaire de la Première réserve du Canada. La Première réserve compte aussi des éléments de la Marine et de l'Armée de l'air et certains éléments du quartier général.

Je ne suis pas ici pour aborder tout ce dont le sénateur Day a parlé, parce que je voulais me concentrer sur la pénurie de personnel réserviste enregistrée en 2005, soit 5 293 personnes. On en a parlé récemment à la Chambre des communes. Je suis content d'aborder ce sujet, et je répondrai aux autres questions que vous souhaiterez me poser sur d'autres aspects de la milice, en vous rappelant que je ne suis plus en activité depuis un certain temps. Mais la coalition dont a parlé le sénateur Day est très large, à

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Day referred to is a wide one, all across this country, and I am in constant contact with our members who provide a good deal of information. I think I have a fairly accurate picture.

Apparently the whole Primary Reserve was at least 5,000 people short in 2015. Last week, the Canadian press reported that the shortfall of the Primary Reserve was now 7,000 people. Given the fact that these represent good, well-paying, part-time jobs, Canadians might well wonder why this should be. Reserves 2000 has been asking that question for a long time.

The last time I appeared before this committee in October 2010, I said that the method being used to issue recruiting quotas was flawed and that many militia units were not being allowed to recruit enough new soldiers to replace the losses they would have in the coming years. I also said that the Canadian Forces Recruiting Group was chronically failing to meet even these small quotas that were issued. I believe I also said that unless these two issues were resolved, militia strength was bound to fall.

In addition to those two fundamental failures at the front end of the strength equation, in the intervening five and a half years the loss rate of trained soldiers has increased, thereby making a bad situation even worse. Some of that increased attrition is due to the fact that reservists no longer have the opportunity to serve on extremely challenging missions like Afghanistan. Certainly there are a few missions outside of Canada, but they are very much diminished from those days. As well, thousands of full-time reserve positions were opened to support the Afghan mission. Those have now been closed off, and many reservists who were in those positions did not choose to return to part-time service. That is a one-off reason why attrition has increased.

It is the opinion of Reserves 2000 that another reason is a lack of exciting and interesting training within units and a lack of suitable summer employment of suitable duration to engage our young soldiers and allow them to make enough money with their reserve service that they don't have to take another job. I have identified this shortcoming by talking to our supporters across the country.

We feel that shortcoming is due, in large part, to a lack of training funding. This is not a lack of pay; there is pay money in the last two or three years. There seems to have been sufficient pay money for soldiers, but you can't have good and exciting training without actually incurring other costs, such as transportation costs to training areas, casual meals and other expenses of that nature. That money was severely restricted about three years ago, and the tap has not really been turned back on yet.

If there's no training, reservists don't get paid. We now have the ironic situation that while pay money has lapsed, we have young soldiers leaving their units because they need more money to keep themselves going, usually through post-secondary

l'échelle du pays, et je suis en contact régulier avec nos membres, qui me fournissent pas mal d'information. Je crois que j'ai une assez bonne idée de la situation.

Il semble que la Première réserve dans son ensemble manquait d'au moins 5 000 personnes en 2005. La semaine dernière, la presse canadienne a fait savoir que la pénurie était désormais de 7 000 personnes. Compte tenu du fait qu'il s'agit de bons emplois à temps partiel, bien payés, les Canadiens ont tout lieu de se demander pourquoi on en est là. Réserves 2000 pose la question depuis longtemps.

La dernière fois que je me suis adressé à ce comité, en octobre 2010, j'ai dit que le mode d'établissement des quotas était défaillant et que de nombreuses unités de la milice n'avaient pas le droit de recruter suffisamment de nouveaux soldats pour remplacer les pertes à venir. J'ai aussi dit que le Groupe du recrutement des Forces canadiennes échouait de façon chronique à même respecter les faibles quotas en vigueur. Je crois avoir également dit que, à moins de régler ces deux problèmes, les effectifs de la milice s'effondreraient fatalement.

Outre ces deux lacunes fondamentales au départ de l'équation concernant les effectifs, au cours des cinq années et demie intermédiaires, le taux de perte de soldats entraînés a augmenté, de sorte que la situation a empiré. Une partie de ces pertes est attribuable au fait que les réservistes n'ont plus l'occasion de servir dans des missions extrêmement exigeantes, comme l'Afghanistan. En fait, il y a peu de missions à l'étranger, mais beaucoup moins qu'à l'époque. Par ailleurs, des milliers de postes de réservistes à temps plein ont été ouverts pour appuyer la mission en Afghanistan. Ils sont maintenant fermés, et beaucoup des réservistes qui les occupaient ne sont pas retournés au service à temps partiel. C'est l'un des éléments ponctuels qui expliquent l'augmentation de l'attrition.

Le groupe Réserves 2000 est d'avis qu'il faut aussi considérer le manque d'entraînement intéressant dans les unités et le manque d'emplois d'été dont la durée incite nos jeunes soldats à s'engager et qui leur permettraient de gagner suffisamment d'argent dans la réserve pour qu'ils n'aient pas à chercher d'autre emploi. J'ai compris ce problème en parlant avec nos partisans dans tout le pays.

Nous pensons que c'est en grande partie dû au manque de fonds consacrés à l'entraînement. Il ne manque pas de salaires; il y a ce qu'il faut depuis deux ou trois ans. Il semble que les soldats soient suffisamment bien payés, mais l'entraînement ne peut pas être intéressant si on n'engage pas effectivement d'autres dépenses, qu'il s'agisse des frais de transport à destination des zones d'entraînement, des repas occasionnels et d'autres frais de ce genre. Ces fonds ont été sévèrement limités il y a environ trois ans, et le robinet n'a pas encore vraiment été rouvert.

S'il n'y a pas d'entraînement, les réservistes ne sont pas payés. Nous sommes maintenant dans la situation ironique où l'on n'a pas dépensé le budget de rémunération, mais que de jeunes soldats quittent leurs unités parce qu'ils ont besoin de plus d'argent pour

education. In particular, the lack of summer jobs for these young Canadians is a cause of well-trained young reservists leaving the militia.

It is the view of Reserves 2000 that these problems could be solved by decentralizing the recruiting, enrolment and training processes. We feel these are best managed at the unit and sometimes at the brigade level. As we all know, Canada is an enormous country, and made-in-Ottawa solutions do not work everywhere. In fact, I dare say that these processes I just mentioned don't even work in Ottawa sometimes. If you want to find out, just go and talk to somebody in the National Capital Region who is serving in a local militia unit. They will tell you the same things.

It is not just Reserves 2000 that has raised flags about problems of this nature. In 2014, the quasi-independent Defence Science Advisory Board produced a particularly damning assessment of the Canadian Forces Recruiting Group. Among other very unfavourable observations, they reported that it took 165 days — that is almost six months — to enrol a reservist. Is it any wonder, then, that young Canadians lose interest in an organization that tolerates wait times like that for a part-time job? It is no wonder that in recent years less than 70 per cent of those already-too-small recruitment quotas I mentioned have been filled.

But a ray of hope did appear in October 2015. Just 10 days before the election, the new Chief of the Defence Staff signed an initiating directive titled "Strengthening the Primary Reserve." I sent a copy of that document to your clerk. If you haven't seen it, it is well worth looking at. In that document, General Vance issued direction to increase the size of the Primary Reserve by 1,500 positions. The Army Reserve's share of that, the militia share, is 950 positions. He wants this done by July 2019. The CDS clearly recognized that there are many factors in the decline of the part-time forces, including those Reserves 2000 has long pointed out, and called for solutions so growth can be achieved.

Given the fact that the whole Primary Reserve may be undermanned by as many as 7,000 today, reaching the goal that the CDS has laid out means an increase from today of 8,500 people in a little over three years.

Considering the failures of the last five years, one must question the ability of the system to shift from net losses of a 1,000 per year for the last five years to net gains of 2,800 per year for the next three and a half years.

As I think we are all aware, the Department of National Defence doesn't turn on a dime. It is our opinion in Reserves 2000 that the only solution is a major policy change, and that major

subvenir à leurs besoins, en s'orientant généralement vers des études postsecondaires. Le manque d'emplois d'été est notamment l'une des raisons pour lesquelles ces jeunes réservistes bien entraînés quittent la milice.

Selon Réserves 2000, on pourrait régler ces problèmes en décentralisant le recrutement, l'enrôlement et l'entraînement. Nous pensons qu'il vaut mieux gérer ces procédures à l'échelle de l'unité, et parfois à l'échelle de la brigade. Comme nous le savons tous, le Canada est un immense pays, et les solutions conçues à Ottawa ne fonctionnent pas partout. En fait, j'oserais dire que les solutions dont je viens de parler ne fonctionnent parfois même pas à Ottawa. Si vous voulez en avoir le cœur net, allez donc parler à quelqu'un de la région de la capitale nationale qui sert dans une unité locale de la milice. On vous dira la même chose.

Il n'y a pas que Réserves 2000 qui a signalé ce genre de problèmes. En 2014, le quasi indépendant Conseil consultatif des sciences appliquées à la défense a produit une évaluation particulièrement accablante du Groupe du recrutement des Forces canadiennes. Entre autres observations très défavorables, le conseil a constaté qu'il fallait 165 jours — presque six mois — pour enrôler un réserviste. Doit-on se surprendre, dans ce cas, que les jeunes Canadiens se désintéressent d'une organisation qui tolère de tels délais pour un emploi à temps partiel? Pas étonnant que, dans les dernières années, on ait comblé moins de 70 p. 100 des quotas de recrutement déjà trop peu élevés dont j'ai parlé.

Mais une lueur d'espoir est apparue en octobre 2015. À peine 10 jours avant l'élection, le nouveau chef d'état-major de la Défense a signé une directive intitulée « Renforcer la Première réserve ». J'ai envoyé un exemplaire de ce document à votre greffière. Si vous ne l'avez pas lu, croyez-moi, il en vaut la peine. On y apprend que le général Vance a émis une directive prévoyant une augmentation de la taille de la Première réserve à raison de 1 500 postes. La part de la Réserve de l'Armée dans ce lot, la part de la milice donc, est de 950 postes. Le général veut que ce soit fait d'ici juillet 2019. Le CEMD a clairement reconnu que de nombreux facteurs entrent en ligne de compte dans le déclin des forces à temps partiel, dont certains sont signalés depuis longtemps par Réserves 2000, et il a appelé à trouver des solutions pour relancer la croissance.

Comme toute la Première réserve manque peut-être aujourd'hui d'environ 7 000 personnes, pour atteindre l'objectif visé par le CEMD, il faudrait augmenter les effectifs d'environ 8 500 personnes en un peu plus de trois ans.

Compte tenu des échecs des cinq dernières années, on peut se demander si le système peut passer d'une perte nette de 1 000 personnes par an depuis cinq ans à une augmentation nette de 2 800 personnes par an dans les trois ans et demi qui viennent.

Je pense que vous savez tous que le ministère de la Défense nationale n'est pas rapide à la détente. Le groupe Réserves 2000 est d'avis que la seule solution est une transformation profonde de

policy change is to decentralize more of these issues and to put them on the armoury floor where they can be done.

However, we also wonder: Is it too late? Has the neglect of the past years doomed the militia? In Minister Sajjan's mandate letter from the Prime Minister, he has been told to "Conduct an open and transparent review process to create a new defence strategy for Canada, replacing the now-outdated Canada First Defence Strategy." He has said, since he was made minister, that the review will determine the future of the reserves. That review has to be finished by the end of this year, by the way, according to his mandate letter.

In the next few months, the future of the reserves is going to be determined. Reserves 2000 fears that given the current state of the militia, there is a real risk that low strength will be used as proof that reserve forces are a failure and therefore should not play a meaningful role in future defence policy.

But we are also ever-optimistic. If the review process is truly open and truly transparent, we are confident that the record of our reserve forces will speak for itself, and Canadians will demand policies that will strengthen the role of their units, in their communities, for the benefit of their country.

Reserves 2000 therefore urges this committee to convey to Minister Sajjan the need to have all stakeholders involved in the review process, including the drafting of terms of reference. We also hope that you will play a leading role in championing the cause of doing more with reserve forces in that review and that this will be reflected in your agenda in the months ahead. Needless to say, I, our small headquarters, and our supporters across the country stand ready to assist in any way possible.

Thank you. I'm pleased to take any questions that you may have.

The Deputy Chair: Thank you, Lieutenant-Colonel Selkirk. Can we take it your comments generally relate to all Primary Reserves, or are you speaking only about the militia, the Army Reserve?

Lt.-Col. Selkirk: No, the strength, recruiting, and enrollment problems are problems across army and navy, and the air force, to a lesser degree, because they generally speaking just accept into the Air Reserve people who have come from the regular air force. That all has to do with training. Certainly, for the army, the navy and the Health Reserve, the comments on recruiting — because they do recruit directly from the population — are all equally valid. They're in the same boat.

la politique et que cette transformation doit prendre la forme d'une décentralisation plus large et que c'est à l'échelle du manège militaire que les problèmes doivent être réglés.

On peut quand même se demander s'il n'est pas trop tard. La négligence qui a caractérisé les dernières années a-t-elle sonné le glas de la milice? Dans sa lettre de mandat adressée au ministre Sajjan, le premier ministre l'invite à « lancer un processus d'examen ouvert et transparent visant à créer une nouvelle stratégie de défense pour le Canada en remplacement de la Stratégie de défense Le Canada d'abord, aujourd'hui désuète ». Il a déclaré, depuis sa nomination, que cet examen déterminera l'avenir des réserves. Je fais remarquer en passant que, selon la lettre de mandat, l'examen est censé être terminé vers la fin de l'année.

L'avenir des réserves sera donc fixé au cours des mois qui viennent. Le groupe Réserves 2000 estime que, compte tenu de la situation actuelle de la milice, il se pourrait très bien qu'on invoque les faibles effectifs pour démontrer que les forces de réserve sont un échec et qu'elles ne devraient donc pas jouer de rôle important dans la future politique de défense.

Mais nous sommes aussi des optimistes invétérés. Si l'examen est vraiment ouvert et transparent, nous sommes convaincus que les antécédents de nos forces de réserve parleront d'eux-mêmes et que les Canadiens exigeront des politiques qui consolident le rôle de leurs unités, dans leurs collectivités, pour le bien de leur pays.

Le groupe Réserves 2000 invite donc instamment le comité à faire valoir auprès du ministre Sajjan la nécessité de faire participer tous les intéressés au processus d'examen, sans oublier d'élaborer un mandat. Nous espérons également que vous jouerez un rôle important dans la défense de notre cause, pour qu'on prévoie une part plus large pour les réserves dans cet examen, et que cela se traduira dans votre agenda des prochains mois. Inutile de dire que notre petit quartier général et moi-même, ainsi que nos partisans dans tout le pays, sommes à votre disposition pour vous apporter de l'aide de quelque façon que ce soit.

Je vous remercie. Je serai heureux de répondre à vos questions.

Le vice-président : Merci, lieutenant-colonel Selkirk. Devons-nous comprendre que vos remarques portent sur toutes les réserves ou seulement sur la milice, la Réserve de l'Armée de terre?

Lcol Selkirk : Non, les problèmes d'effectifs, de recrutement et d'enrôlement sont les mêmes qu'il s'agisse de l'Armée de terre ou de la Marine, et de l'Armée de l'air à un moindre degré, parce que, en général, la Réserve aérienne n'accepte que des recrues de l'Armée de l'air régulière. Tout cela remonte à la question de l'entraînement. Il est clair que, pour l'Armée de terre, la Marine et la Réserve du corps médical, les observations concernant le recrutement — parce qu'il se fait directement dans la population — sont semblables. Tout le monde est dans le même bateau.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

As far as what other condition the Navy Reserve, Health Reserve and Air Reserve are in, I don't have that information. I don't have the details on that. I do know, however, the condition that the militia — the Army Reserve — is in.

The Deputy Chair: The figure you gave us today of 7,000 below strength, is that militia or is that all Primary Reserves?

Lt.-Col. Selkirk: That is everything. I took that figure from a report in the Canadian press by Murray Brewster, and he specifically broke out that the Primary Reserve was short 7,000 and the Regular Force was short another 2,000 or 3,000. I have forgotten the exact number for the Regular Force.

That to me rings true because in 2015 they were 5,000-plus short, and nothing has really improved since then in terms of recruiting and enrolment, and I think attrition is just as bad. That could be a very accurate figure, I think.

The Deputy Chair: What figure is the authorized strength for reserves?

Lt.-Col. Selkirk: Twenty-seven thousand is the authorized strength of the Primary Reserve.

The Deputy Chair: And Mr. Brewster believes, and you accepted his figure, that the reserves are 7,000 below that?

Lt.-Col. Selkirk: That's what he's saying it is today. I don't know what his sources are.

The Deputy Chair: Did you take the Chief of Defence Staff statement just before the election of 1,500 more as 1,500 more on top of 27,000?

Lt.-Col. Selkirk: Yes. He wants it to be 28,500 by 2019.

The Deputy Chair: That's helpful. It clarifies your comments.

Senator White: Thank you very much for being here today.

In 2010-11, this committee's study looked at reserves and the trend among other countries — not only Canada — to have reservists working primarily in the domestic domain. Can you tell us why you think that might have started? Can you give us a little bit about whether we moved directly behind this model, and that's why we had a diminishing number of reservists?

Lt.-Col. Selkirk: I'm not sure I understand your question exactly.

Senator White: In 2010-11 the committee did research on a number of countries, including Canada, which looked at reservists, primarily focusing on domestic operations: emergencies, ice storms, et cetera.

Lt.-Col. Selkirk: You are asking me if I think that's a factor in why —

Quant aux autres aspects de la situation de la Réserve de la Marine, de la Réserve du corps médical et de la Réserve aérienne, je n'ai pas d'information. Je n'ai pas de données précises à ce sujet. Mais je peux parler de la situation de la milice, la Réserve de l'Armée de terre.

Le vice-président : Le chiffre que vous nous avez donné, la pénurie de 7 000 personnes, s'applique-t-il à la milice ou à toutes les premières réserves?

Lcol Selkirk : C'est un chiffre global. Je l'ai trouvé dans un article de Murray Brewster, de la presse canadienne. Il disait que la Première réserve manquait de 7 000 membres et que l'Armée régulière, elle, manquait de 2 000 ou 3 000 soldats. J'ai oublié le chiffre exact pour l'Armée régulière.

Cela me semble juste parce que, en 2015, il manquait plus de 5 000 personnes, et rien n'a vraiment changé depuis du point de vue du recrutement et de l'enrôlement. Je pense que l'attrition est toujours aussi grave. Je pense que c'est un chiffre très juste.

Le vice-président : Quels seraient les effectifs autorisés dans les réserves?

Lcol Selkirk : Vingt-sept mille personnes pour la Première réserve.

Le vice-président : Et M. Brewster pense, et vous le pensez aussi, que les réserves ont 7 000 personnes de moins que cela?

Lcol Selkirk : C'est ce qu'il dit aujourd'hui. Je ne connais pas ses sources.

Le vice-président : Selon vous, le chef d'état-major de la Défense, lorsqu'il parlait de 1 500 personnes de plus juste avant l'élection, parlait-il de 1 500 personnes en plus des 27 000?

Lcol Selkirk : Oui. Il veut que les effectifs passent à 28 500 personnes d'ici 2019.

Le vice-président : Voilà qui est clair, merci bien.

Le sénateur White : Merci beaucoup d'être parmi nous aujourd'hui.

En 2010-2011, nous avons ici examiné la situation des réserves et la tendance, pas seulement au Canada, mais dans d'autres pays, à faire travailler les réservistes principalement sur le territoire national. Pourriez-vous nous dire d'où vient cette tendance selon vous? Pourriez-vous nous dire brièvement si nous avons directement suivi ce modèle et si c'est la raison de la baisse des effectifs de réservistes?

Lcol Selkirk : Je ne suis pas sûr de comprendre votre question.

Le sénateur White : En 2010-2011, le comité a fait une étude sur les réserves de différents pays, dont le Canada, pour constater que les activités des réserves se concentraient sur les opérations internes : urgences, tempêtes de glace, et cetera.

Lcol Selkirk : Vous voulez savoir si je pense que c'est un facteur de...

Senator White: What caused the trend? Is that part of the impact on us going from 27,000 to 20,000 and the concerns you are raising now?

Lt.-Col. Selkirk: I don't think it would have a large impact if everything else was working correctly. I said that I believe that leaving Afghanistan has been a factor here, and it certainly is directly a factor in this sense: During Afghanistan, the Armed Forces at one point called up 12,000 part-time reservists to full-time duty. When those full-time jobs went away — by the way, the number now is 4,500 across all services — they didn't all go at once. It was a gradual drawdown.

Senator White: Yes.

Lt.-Col. Selkirk: When that happened, a number of those people chose not to go back to part-time service and just left, but they were still counted as reservists, so that was attrition. That factor was there as a direct result of leaving Afghanistan.

There are probably some reservists who, without the opportunity to deploy overseas, might have tried it for a couple of years and said, "I'm going," but quite frankly I do not believe that the majority of reservists see domestic employment as any less important than overseas employment.

Senator White: The participation in domestic international operations in recent years has been diminished partially by demand. What impact is that having directly on things like morale within the units? Seven thousand is a lot of people to be short. What impact is it having, from your perspective?

Lt.-Col. Selkirk: I don't think the fact that we are not deploying in large numbers overseas really is affecting morale in the units very much. What I believe does affect morale is a lack of resources to do interesting, exciting training during the winter months and if there are not sufficient resources to do interesting and exciting training during the summer months.

Now that interesting and exciting training may be individuals getting courses to improve their individual skills. It could involve working on ranges and other things that need to be done to support training, and it certainly involves what the militia historically did in the order of two to three weeks each summer, which was to bring units together to practise working as larger formations and teams together.

If you don't have that, I think that does affect morale. This summer, for example, in Ontario, units will be concentrated together, but not for a very long period of time. It is my understanding that rather than militia officers and militia NCOs commanding their own soldiers, basically the officers and NCOs have been told, for want of better words, "Really, we don't have

Le sénateur White : D'où vient cette tendance? Est-ce que cela explique en partie la réduction des effectifs de 27 000 à 20 000 et les préoccupations que vous soulevez maintenant?

Lcol Selkirk : Je ne pense pas que ce serait très important si tout le reste fonctionnait correctement. Je crois, comme je l'ai dit, que notre départ de l'Afghanistan a été un facteur dans ce cas, et c'est certainement un facteur direct en ce sens : au cours de l'intervention en Afghanistan, les Forces canadiennes ont, à un moment donné, appelé jusqu'à 12 000 réservistes à temps partiel à participer à leurs activités à temps plein. Lorsque ces emplois à temps plein ont disparu — au fait, le chiffre actuel est de 4 500 toutes armées confondues —, ils n'ont pas disparu tous en même temps. Cela s'est fait peu à peu.

Le sénateur White : Je vois.

Lcol Selkirk : À l'époque, un certain nombre de personnes ont décidé de ne pas retourner à leur emploi à temps partiel. Elles sont tout simplement parties, mais elles étaient toujours considérées comme des réservistes, et c'était donc de l'attrition. Ce facteur découlait directement de notre départ de l'Afghanistan.

Il y a probablement des réservistes qui, sans possibilité de déploiement à l'étranger, ont pu essayer deux ou trois ans et dire « J'y vais », mais, très franchement, je ne crois pas que les réservistes estiment dans leur majorité que le service interne est moins important que le service à l'étranger.

Le sénateur White : La participation aux opérations internationales internes a partiellement diminué en raison de la demande dans les dernières années. Quel impact direct cela a-t-il sur, par exemple, le moral des troupes dans les unités? Sept mille personnes, c'est une grave pénurie. Quelles conséquences avez-vous constatées?

Lcol Selkirk : Je ne crois pas que le fait que nous ne déployons pas beaucoup de monde à l'étranger ait réellement un effet important sur le moral des troupes. Ce qui les mine, à mon avis, c'est plutôt le manque de ressources pour organiser des entraînements intéressants au cours des mois d'hiver et l'insuffisance des ressources pour organiser des entraînements intéressants durant les mois d'été.

Ces activités intéressantes peuvent être des cours pour améliorer des compétences, de l'entraînement sur des champs de tir, et d'autres choses nécessaires à l'appui de l'entraînement, et cela suppose évidemment ce que la milice a toujours fait durant deux ou trois semaines par été, à savoir réunir les unités pour qu'elles s'exercent en larges formations et en équipes.

Sans cela, le moral est compromis, à mon avis. Cet été, par exemple, en Ontario, des unités seront regroupées, mais pour très peu de temps. À ce que j'ai compris, au lieu que les officiers et sous-officiers de la milice commandent leurs propres soldats, on leur a dit pour l'essentiel, si je peux m'exprimer ainsi : « En fait, on n'a rien à vous faire faire, les gars. On veut que vos soldats et

anything for you guys to do. We want your privates and corporals to flesh out regular units for that period of training." I can tell you I don't think that's good for morale.

[*Translation*]

Senator Dagenais: Thank you very much for your testimony, Mr. Selkirk. For your information, I was a reservist at the Royal Canadian Hussars and at the 2nd Field Artillery Regiment. Training was for two and a half months during the summer, which was very good, and it was either at Farnham or Gagetown. Then we had training every weekend. It was a very good experience. That may be how I became disciplined enough for the Senate. Maybe my colleagues would like me to go back for more training!

If I understood your presentation correctly, there were problems with recruitment or attracting candidates. A study was done in 2010-11 on the current and future state of the Canadian reserves. I would like you to elaborate on the ongoing problems you are dealing with, either with attracting new people or retaining them. What do you believe could be done to improve the situation?

[*English*]

Lt.-Col. Selkirk: From the point of view of attraction, I don't believe that there is a great problem out there, especially given the fact that we are not calling for large numbers. The whole militia now is only between 16,000 and 17,000 people, across 120 units. So every unit is not calling for hundreds of people to appear at the armoury door.

Attraction seems not to be the problem, and attraction is a unit responsibility. A little bit of advertising occurs on a central basis, but for the most part, units are attractive to young Canadians.

The problem is with the process thereafter. As I said, a report from 2014 said it took, on average, 160-plus days after the attraction has occurred, once somebody expresses an interest, until that individual is enrolled and can actually start training. That is a very serious problem.

The Chief of the Defence Staff recognizes that. In his directive, he has directed that that period must be shortened. I think he's calling for 90 days, but even 90 days is an awfully long time when you consider that the competition for these bright young Canadians who want to join can sign them up and have them working somewhere else within a week or two weeks, perhaps.

There is a very serious problem with the young Canadian who is interested and attracted. He or she looks at this will go somewhere else after a while. They're not going to wait. This is a part-time job, after all. People that want to join the Regular Force, who are going to get a pension at the end of it and all that stability and everything that entails, will wait 160 days. I'm not too sure that this appeals very much to a high school kid that we are trying to attract.

vos caporaux grossissent les rangs dans les unités régulières pendant cette période. » Je peux vous dire que ce n'est pas génial pour le moral, à mon avis.

[*Français*]

Le sénateur Dagenais : Merci beaucoup, monsieur Selkirk, pour votre témoignage. Pour votre information, j'ai été réserviste au Royal Canadian Hussars et au 2e Régiment d'artillerie de campagne. L'entraînement se faisait durant deux mois et demi l'été, ce qui était très intéressant, à Farnham ou à Gagetown. Par la suite, nous étions en entraînement toutes les fins de semaine. C'était une très bonne expérience. C'est peut-être ce qui m'a discipliné pour le Sénat; d'ailleurs, je crois que mes collègues voudraient que j'y retourne!

J'ai cru comprendre dans votre présentation qu'il y avait des problèmes de recrutement, entre autres, ou des problèmes d'attraction. Une étude a été faite en 2010-2011 sur l'état actuel et futur de la réserve canadienne. J'aimerais vous entendre à nouveau au sujet des problèmes constants auxquels vous faites face, soit pour attirer les gens ou tout simplement pour les garder. Selon vous, que pourrait-on faire pour améliorer cette situation?

[*Traduction*]

Lcol Selkirk : Pour ce qui est d'attirer des candidats, je ne crois pas que ce soit un gros problème, surtout que nous n'en cherchons pas un très grand nombre. Les 120 unités de la milice comptent actuellement entre 16 000 et 17 000 personnes. Donc, chaque unité ne convoque pas des centaines de personnes au manège militaire.

Ce n'est pas un problème d'attirer des candidats, et c'est la responsabilité de chaque unité. On fait un peu de publicité à l'échelle centrale, mais, le plus souvent, les unités intéressent les jeunes Canadiens.

Le problème, c'est la procédure qui suit. Comme je l'ai dit, selon un rapport publié en 2014, il faut attendre en moyenne plus de 160 jours avant de pouvoir enrôler et commencer à entraîner quelqu'un qui a manifesté son intérêt. C'est vraiment un problème.

Le chef d'état-major de la Défense en est conscient. Dans sa directive, il ordonne que ce délai soit raccourci. Je pense qu'il voudrait obtenir 90 jours, mais 90 jours, c'est encore terriblement long quand on pense à la concurrence qui offre à ces jeunes et brillants candidats la possibilité de travailler ailleurs dans un délai de peut-être une semaine ou deux.

C'est un problème très sérieux pour les jeunes Canadiens qui sont attirés par la réserve. Ils iront ailleurs au bout d'un certain temps, ils ne vont pas attendre. C'est un emploi à temps partiel, après tout. Les gens qui veulent entrer dans l'Armée régulière, qui auront une pension en fin de carrière et qui jouiront d'une stabilité d'emploi et de tout ce que cela suppose, eux attendront 160 jours. Je ne suis pas sûr que ce soit un bon moyen d'intéresser un jeune du secondaire que nous désirons attirer dans nos rangs.

Therein lies a very serious problem. This problem has been pointed out and talked about and talked about, and nothing ever really seems to get done.

Within those 160 days, many steps could be taken back into the armoury so that the process can be sped up. For example, the Canadian Forces Recruiting Group insists that a lot of the actual processing has to happen in their offices. Well, take the case of the 49th Field Regiment, Royal Canadian Artillery, in Sault Ste. Marie. The recruiting office in Sault Ste. Marie was closed in about 2012, I believe. Since then, they have had to take their young recruits, high school students who have to go to school the next day, and bus them or drive them all the way to Sudbury to fill out a whole bunch of stuff and do a bunch of stuff. That might happen two or three times before those kids are enrolled.

Well, if I were a parent of those kids and they had to go to school — that's about a five-hour drive by the way — I wouldn't want them doing that. There are impediments such as that that are just outrageous as far as I'm concerned.

[*Translation*]

Senator Dagenais: So if I understand correctly, Mr. Selkirk, the problem may be in the structure, in how to manage enrolment or transportation. I understand that you talked about this with the people in charge, but have you found ways to address the lengthy enrolment period, which sometimes discourages candidates from joining the reserves?

[*English*]

Lt.-Col. Selkirk: Senator, since I have been involved in this, and it has been a long, long time, the problem became worse as the process was more and more centralized. However, since it got to this point of 160 days or so, I don't believe there has been any dramatic improvement. I don't think it has improved in the last four or five years.

Indeed, the Canadian Forces Recruiting Group has actually closed more recruiting offices in that period of time. It closed the recruiting office in Oshawa or at least reduced the hours. It closed the recruiting office in Cape Breton. I guess that was Sydney. And it closed one in Corner Brook. I can't see that any of that is helping this problem.

I spoke to a very senior person in the recruiting group and talked to him about this issue. I said to him, "Look, you seem to be able to meet the Regular Force recruitment quotas you have given every year, but for years they have only managed to reach about 70 per cent of the reserve quotas. Why is that? Do you need more people? What is it?" Basically, the answer was, "Well, we have to do the Regular Force. We look after that first. If we have got time and resources left over, then we apply it to the reserve quotas."

Voilà donc un très sérieux problème. Et on l'a déjà signalé, on en a parlé et reparlé, mais rien ne semble vraiment changer.

Durant ces 160 jours, beaucoup de choses pourraient être faites à l'échelle du manège militaire pour accélérer le processus. Par exemple, le Groupe du recrutement des Forces canadiennes tient mordicus à ce qu'une grande partie du processus ait lieu dans ses bureaux. Eh bien, prenons le cas du 49e Régiment d'artillerie de campagne, Artillerie royale du Canada, à Sault Ste. Marie. Le bureau de recrutement de Sault Ste. Marie a été fermé en 2012, je crois. Depuis, les jeunes recrues, des étudiants du secondaire qui doivent aller à l'école le lendemain, doivent être emmenées en autobus ou en voiture à Sudbury pour y remplir toutes sortes de formulaires et y faire toutes sortes de choses. Cela peut se produire deux ou trois fois avant que ces jeunes soient enrôlés.

Quant à moi, si c'était mes enfants et qu'ils doivent aller à l'école — au fait, on parle d'un trajet d'environ cinq heures —, je ne voudrais pas qu'ils le fassent. Il y a des obstacles de ce genre que je trouve complètement aberrants.

[*Français*]

Le sénateur Dagenais : Si je comprends bien, monsieur Selkirk, le problème est peut-être dans la structure, autrement dit dans les délais liés à la façon de gérer l'enrôlement ou le transport. Je comprends que vous avez dû parler de cette situation avec les responsables, mais avez-vous trouvé des façons de remédier à ces longueurs dans la période d'enrôlement, qui font que, parfois, le candidat peut se décourager avant de rejoindre la réserve?

[*Traduction*]

Lcol Selkirk : Monsieur le sénateur, depuis que je participe à tout cela, et cela fait très, très longtemps, la situation a empiré, car le processus est devenu de plus en plus centralisé. Mais, depuis qu'on a ce délai d'environ 160 jours, je ne crois pas qu'il y ait eu d'amélioration importante. Je ne crois pas que les choses se soient améliorées dans les quatre ou cinq dernières années.

En fait, le Groupe du recrutement des Forces canadiennes a fermé encore plus de bureaux de recrutement durant cette période. Il a fermé celui d'Oshawa ou du moins en a réduit les heures d'ouverture. Il a fermé celui du Cap Breton. Je pense que c'était celui de Sydney. Et il a fermé celui de Corner Brook. Je ne vois pas en quoi cela a pu améliorer la situation.

J'ai discuté avec un membre très ancien du Groupe du recrutement et je lui ai parlé de ce problème. Je lui ai dit : « Écoute, on dirait bien que vous pouvez remplir les quotas qu'on vous donne tous les ans, mais, depuis des années, on n'atteint qu'environ 70 p. 100 des quotas de la réserve. Pourquoi? Est-ce que vous avez besoin de plus de monde? Qu'est-ce qui se passe? » Pour l'essentiel, la réponse a été : « Eh bien, nous devons nous occuper de l'Armée régulière. C'est elle d'abord. Si on a du temps et des ressources après cela, on s'occupe des quotas de la réserve. »

There is another part of the problem. This over-centralization, one-size-fits-all, really doesn't fit all. It is our opinion that the reserve part of all that should be given back to reservists to do as close as possible to the actual unit.

[*Translation*]

Senator Carignan: I have a few questions. I will close on the issue of recruitment, but then I will come back to the recruitment strategy, something that I find very interesting.

Is there not a problem related to targeting potential clients or young people who might want to apply to be a reservist? I will give you an example. Senator Dagenais said he became a reservist, but why was that? Maybe he wanted to be involved in the field of security. Maybe he was having a hard time finding a job in the field, decided to start this way, and wanted to gain this experience.

This is not uncommon among young people working in security, just like young volunteer firefighters who have part-time jobs and want to complete their training or fill their available time with a job like this. The problem is that no one is recruiting them.

Are there any real strategies? What happens with young cadets in high school? Back home there were Kiwanis air cadets, but they seem to have vanished because no one followed up to recruit them. Is anyone really making an effort to target candidates in this recruitment strategy?

[*English*]

Lt.-Col. Selkirk: That's an interesting question, senator.

You're familiar with a Kiwanis Club sponsoring a cadet core. I'd say that every militia unit sponsors their own cadet corps, yet the uptake of cadets into the Primary Reserve is not that great. Why is that? I believe some of it is the very keenness of the cadets. The age that an individual can be enrolled in the militia or the Primary Reserve starts at 17. The keenest cadets can stay with their cadet corps until they are 18 or maybe 19. They are the ones you think might want to come, but they're now big wheels in the cadet corps, and perhaps they don't want to go from being a fish in a small pond to being a little fish in a big pond.

Interestingly enough, a lot of those senior cadets go to RMC. Perhaps even Senator Day was a senior cadet at one time. They will go directly into the Regular Force and skip the reserve part of it. I believe it's got something to do with the age you can get them at, but that's only part of the answer.

C'est un autre aspect du problème. Cette centralisation excessive, ce modèle universel, ne convient pas à tout le monde. Nous pensons que ce qui revient à la réserve dans tout cela doit être rendu aux réservistes pour que les choses se passent aussi près que possible des unités réelles.

[*Français*]

Le sénateur Carignan : J'ai quelques questions à poser. Je terminerai avec la question du recrutement, mais je reviendrai ensuite sur la stratégie de recrutement, sujet que je trouve intéressant.

Est-ce qu'il n'y aurait pas un problème lié au ciblage des clients potentiels ou des jeunes qui pourraient se présenter comme réservistes? Je vous donne un exemple. Le sénateur Dagenais a dit qu'il est devenu réserviste, mais pourquoi est-il devenu réserviste? C'est probablement parce qu'il avait la volonté de s'impliquer dans le domaine de la sécurité. De plus, peut-être qu'il avait de la difficulté à trouver un emploi dans le milieu, qu'il commençait dans ce domaine et qu'il voulait acquérir cette expérience.

On constate souvent ce phénomène chez les jeunes qui travaillent dans le domaine de la sécurité, comme chez les jeunes pompiers volontaires qui occupent des emplois à temps partiel et qui désirent compléter leur formation ou combler leur temps de disponibilité avec un emploi comme celui-là. Le problème, c'est qu'on ne va pas les chercher.

Est-ce qu'il existe véritablement des stratégies? Qu'est-ce qui se passe avec les jeunes cadets du secondaire? Chez nous, il y avait les cadets de l'air Kiwanis, mais ils semblent disparaître, parce qu'il n'y a pas de suivi qui est fait pour les recruter. Est-ce qu'on fait réellement un effort pour cibler les candidats dans cette stratégie de recrutement?

[*Traduction*]

Lcol Selkirk : C'est une question intéressante, monsieur le sénateur.

Vous connaissez bien un club Kiwanis qui parraine un groupe de cadets. Je dirais que chaque unité de la milice parraine son propre corps de cadets, et pourtant l'admission de cadets dans la Première réserve n'est pas si remarquable. Pourquoi cela? Je crois qu'une partie de la réponse tient à l'enthousiasme des cadets. L'âge minimum auquel une personne peut être enrôlée dans la milice ou dans la Première réserve est 17 ans. Les cadets les plus enthousiastes peuvent rester dans leur corps de cadets jusqu'à l'âge de 18 ou 19 ans. Vous pensez qu'ils voudront venir, mais ils sont maintenant des gens importants dans le corps de cadets, et peut-être qu'ils n'ont pas envie de passer du statut de poissons dans un petit lac à petits poissons dans un grand lac.

Remarquez que beaucoup de ces cadets supérieurs entrent dans la GRC. Peut-être même que le sénateur Day a été autrefois un cadet supérieur. Ils vont directement dans l'Armée régulière et sautent la partie réserve. Je crois que cela a un rapport avec l'âge auquel on les enrôle, mais ce n'est qu'une partie de la réponse.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Do we target those folks? Any smart unit does, but the success I've seen is certainly not 100 per cent, not even 50 per cent. It's an interesting phenomenon. I don't know why there is a disconnect, but there seems to be.

[*Translation*]

Senator Carignan: I would like to further explore the numbers because we are talking about 28,500 reservists, if the targets are met. In your view, what would be the ideal number for a fully effective and efficient reserve?

[*English*]

Lt.-Col. Selkirk: Senator, the number that we have put forward for a long time is 45,000. In fact, Senator Segal, one of your retired colleagues, is involved with the North Atlantic Council that has produced a paper in which he uses that same number. We did a study years ago and felt that 45,000 were required primarily to support the size of the expeditionary force being studied at the time. Since then, we've revised our thought to some degree and feel that rather than expeditionary, the real need would be here in Canada.

When we first started producing these numbers, it was before 9/11. Today, we feel that the real threat to our way of life is domestic, and that the disruption caused would require a tremendous amount of consequence management. Although we have large security forces, they are nowhere near large enough to provide that consequence management on a 24/7 basis that might be required.

Our feeling still is that 45,000 army reservists. I don't know what the figure might be for the navy, the air force or health care, but that is our number. If that were to be the case, then those 120 militia units could be of sufficient mass that they could be much more efficient than they are today.

They're too small today. There just isn't enough mass to actually do everything. One reason I suspect that perhaps there is not as much interesting training going on at the armoury level is the fact that we do not have enough officers or NCOs. There're many reasons that is true, but we just have not recruited enough young officers at this level to have, 20 years later, enough majors and lieutenant-colonels to organize and control some of the more interesting things that could be done. It's the same, to some degree, with non-commissioned officers.

We need a larger militia in order to have a centre of gravity that is big enough, and if you have that, you can do a lot more.

Senator Beyak: Thank you, Lieutenant-Colonel Selkirk. Your presentation was excellent.

My question is on major personnel pressures linked to retention and attrition. You answered that in the presentation. You also identified the decentralization to the unit, even to the

Est-ce qu'on vise ces personnes? Toutes les unités intelligentes le font, mais elles ne réussissent pas à 100 p. 100, et même pas à 50 p. 100. C'est un phénomène intéressant. Je ne sais pas pourquoi cela n'accroche pas, mais c'est ce qui se passe.

[*Français*]

Le sénateur Carignan : J'aimerais traiter davantage de la question du nombre, parce qu'on parle de 28 500 réservistes, si les objectifs sont atteints. Selon vous, quel devrait être le chiffre idéal d'une réserve qui serait pleinement efficace et efficiente?

[*Traduction*]

Lcol Selkirk : Monsieur le sénateur, le nombre avancé depuis longtemps est de 45 000. En fait, le sénateur Segal, un de vos collègues à la retraite, participe aux travaux du Conseil de l'Atlantique Nord, qui a publié un document où l'on trouve le même chiffre. Nous avons fait une étude, il y a bien des années, et nous pensions alors qu'il fallait 45 000 personnes principalement pour les opérations du corps expéditionnaire étudié à l'époque. Depuis, nous avons modifié un peu notre perspective et nous pensons plutôt que les besoins sont ici au Canada.

Ces chiffres sont antérieurs aux attentats du 11 septembre. Aujourd'hui, nous pensons que la menace réelle qui pèse contre notre mode de vie est interne et que les troubles qui seraient causés exigeraient une énorme gestion des conséquences. Nous avons d'importantes forces de sécurité, mais elles ne sont absolument pas suffisantes pour assurer la gestion des conséquences 24 heures par jour, 7 jours 7, dont on pourrait avoir besoin.

Nous pensons toujours qu'il faudrait 45 000 réservistes. Je ne sais pas ce qu'il faudrait pour la Marine, l'Armée de l'air ou le Corps médical, mais pour nous, c'est cela. Si nous les avions, les 120 unités de la milice auraient une masse telle qu'elles pourraient être beaucoup plus efficaces qu'elles ne le sont actuellement.

Elles sont trop petites aujourd'hui. Il n'y a tout simplement pas assez de gens pour tout faire. L'une des raisons pour lesquelles, peut-être, du moins je le pense, il n'y a pas autant d'entraînement intéressant à l'échelle locale est le fait que nous n'avons pas assez d'officiers et de sous-officiers. Il y a bien des raisons à cela, mais nous ne recrutons pas assez de jeunes officiers à ce niveau pour avoir, 20 ans plus tard, suffisamment de majors et de lieutenants-colonels pour organiser et contrôler une partie des choses les plus intéressantes à faire. C'est la même chose, jusqu'à un certain point, pour les sous-officiers.

Nous avons besoin d'une milice nombreuse pour avoir un centre de gravité suffisamment large, et, si on a cela, on peut faire beaucoup plus.

La sénatrice Beyak : Merci, lieutenant-colonel Selkirk. C'était un excellent exposé.

Ce qui m'intéresse, ce sont les principales pressions exercées sur le personnel en matière de rétention et d'attrition. Vous en avez parlé dans votre exposé. Vous avez également parlé de

brigade. When you answered Senator Dagenais, you mentioned the 165 days again and that General Vance wants 90 days. Until we identify why that's happening, it won't be solved.

Can you tell me if there've been any studies or audits that show why it takes 165 days? And 90 is too long as well.

Lt.-Col. Selkirk: Senator, the study I quoted, and I have not read it for quite a while, contains a lot of detail. That would be useful if you want to understand what was going on and, as far as I know, is still going on. There's a lot of file shuffling and people can be away. The Canadian Forces recruiting offices have a full-time mentality and work five days a week, yet the reservists are not available during working hours five days a week. There are long delays between files getting the right boxes ticked off and that sort of thing because the reservist just isn't available.

At one point, and I think this still exists, every medical for every reservist who joined was signed off by a medical officer in one office in Camp Borden. I have no way of proving this, but I've been told when that guy went on leave in the summertime, nothing happened for his period of leave; things like that. It just seems incredible that this is the way it operates, but that seems to be the case.

All that said, I know that some units have really good working relationships with the local recruiting office. Fortunately, the office in Oshawa was one of those. They had a really good relationship there, and that office would stay open or open up on a Saturday for them. For every one good story like that there are five or six horror stories about how the recruiting group does not look after our part-time service.

Senator Beyak: Thank you very much for that very good answer. It seems like that's the problem we have to address.

Lt.-Col. Selkirk: It certainly is a very large problem. Coupled with that, as I said in my opening remarks, is the setting of recruitment quotas. Before it was totally centralized, and it has been totally centralized for about five years, quotas were set out there. They weren't necessarily set right at the unit level, but brigade and areas would decide more. Now the process has been so centralized that it doesn't take into account a lot of factors, and that's why those numbers are so low. Again, General Vance recognizes that there is a problem. How they're going to fix it I don't know, because the desire to centralize everything is still there, as far as I'm concerned.

What we are advocating is a culture shift that recognizes that centralization, while it has some benefits, does not serve a big country like Canada particularly well sometimes and this is a particular case.

décentralisation à l'échelle de l'unité, voire de la brigade. Lorsque vous avez répondu au sénateur Dagenais, vous avez parlé du délai de 165 jours et de la directive du général Vance pour ramener ce délai à 90 jours. Tant qu'on ne connaîtra pas les raisons de ce délai, le problème ne sera pas réglé.

Pourriez-vous me dire si on a fait des études ou des vérifications permettant de savoir pourquoi cela prend 165 jours? Et 90 jours, c'est trop long aussi.

Lcol Selkirk : Madame la sénatrice, l'étude dont j'ai parlé, et je ne l'ai pas relue depuis un certain temps, contient beaucoup d'information. Elle serait utile pour comprendre ce qui se passait alors et ce qui se passe toujours pour autant que je sache. Il y a beaucoup de brassage de dossiers, et les gens peuvent être absents. Les employés des bureaux de recrutement des Forces canadiennes ont une mentalité d'employés à temps plein et travaillent cinq jours par semaine, mais les réservistes, eux, ne sont pas disponibles durant les heures ouvrables cinq jours par semaine. Il faut beaucoup de temps avant que les différentes cases des formulaires soient remplies et tout cela, parce que les réservistes ne sont tout simplement pas disponibles.

À une certaine époque, et je crois que c'est encore le cas, les formulaires médicaux de tous les réservistes étaient approuvés par un médecin d'un bureau de Camp Borden. Je n'ai aucun moyen de le prouver, mais on m'a dit que, quand ce type prenait ses vacances au cours de l'été, il ne se passait rien pendant son congé. Des choses comme cela. On a du mal à croire que ça se passe comme ça, mais ça semble bien être le cas.

En même temps, je sais que certaines unités ont d'excellentes relations avec le bureau de recrutement local. Et c'était heureusement le cas de celui d'Oshawa. Les relations étaient vraiment excellentes, et le bureau restait ouvert ou ouvrait le samedi au besoin. Pour chaque cas positif comme celui-là, il y a cinq ou six histoires d'horreur sur la façon dont le groupe de recrutement se désintéresse des engagés à temps partiel.

La sénatrice Beyak : Je vous remercie de cette réponse très intéressante. Il semble que ce soit bien le problème à régler.

Lcol Selkirk : C'est effectivement un problème de grande portée. Il faut aussi tenir compte, comme je l'ai dit au début, de l'établissement des quotas de recrutement. Auparavant, c'était complètement centralisé. Depuis environ cinq ans, les quotas sont décidés centralement. Auparavant, ils n'étaient pas nécessairement établis à l'échelle des unités, mais les brigades et les secteurs avaient un plus grand pouvoir décisionnel. Aujourd'hui, le processus est si centralisé qu'il ne tient pas compte de toutes sortes de facteurs, et c'est pour cela que les chiffres sont si bas. Là encore, le général Vance est conscient du problème. Reste à savoir comment ils vont le régler, parce que, autant que je sache, le désir de tout centraliser est toujours là.

Ce que nous recommandons, c'est un changement de culture : qu'on reconnaisse que la centralisation, malgré ses avantages, ne sert parfois pas très bien un pays grand comme le Canada, et c'est le cas ici.

Senator Beyak: Thank you very much.

Senator Mitchell: I'm interested in the point you made about decentralizing training. At face value that sounds like a good idea. Does it not, however, run into a contradiction when you say one of the problems now is that there are insufficient officers and NCOs in various depots to really provide the training? How would you accommodate that and make it work?

Lt.-Col. Selkirk: That's the real question, and the more that the militia has lacked officers and NCOs, the more the absolute requirement to centralize has been there. However, the more training that can actually be done at the unit for these part-time young Canadians is absolutely the best.

If you're in downtown Toronto and there are armouries there that have four or five units, centralizing some things and using everyone to work together makes a lot of sense because the young soldiers that are being trained are coming in from a vast surrounding area, but they also have access to good public transportation and it's not too much of a problem.

But take a more isolated unit such as Sault Ste. Marie. How will you centralize in Sault Ste. Marie? Those are in areas that really require new solutions to this problem. And, if we look across this country, units in large urban areas are not faring as badly as units in rural areas. In fact, it's the rural units that we fear for because they are the ones that are more under strength than anyone else. The constant, "Oh, we have to have economies of scale," could mean that a large number of rural units, if you carry on with the notion that economies of scale are the answer to everything, could disappear. I don't think that would be politically palatable across this country.

Senator Mitchell: To some extent it's not a coincidence or you might argue it's not a coincidence that the number of reservists has dropped off as we've gotten out of Afghanistan. Deploying a large number of people to a war creates a real sense of urgency. No matter what we do, there is not that sense of urgency when we're not doing that. It is a question of what you do to occupy people.

Our committee did a report in 2011 in which we suggested that one of the things that could be looked at for the reserves would be working on the cyber-threat. Have you given any thought to pursuing that as an activity for reservists and how that might be structured? You can see where it needs continuity, but is there a way that that could create a demand and a greater sense of urgency for the reserves?

Lt.-Col. Selkirk: That is the kind of thing we need to be looking at. Again, if you look at this CDS initiating directive, there is a piece in there about getting into areas — I don't know whether that's a non-traditional area, but I guess it is. We do have electronic warfare reserve units, and the CDS recognizes that that is an area in which reservists could be well employed.

La sénatrice Beyak : Je vous remercie.

Le sénateur Mitchell : Je reviens sur ce que vous avez dit au sujet de la décentralisation de l'entraînement. C'est une bonne idée à première vue, mais est-ce que cela ne contredit pas ce que vous dites par ailleurs, à savoir qu'il manque d'officiers et de sous-officiers dans différents dépôts pour qu'on puisse vraiment offrir de l'entraînement? Comment concilier cela pour que cela fonctionne?

Lcol Selkirk : C'est cela la question, et plus la milice manque d'officiers et de sous-officiers, plus il faut centraliser. Mais la meilleure solution, quoi qu'il en soit, est de pouvoir offrir de l'entraînement à ces jeunes Canadiens employés à temps partiel à l'échelle des unités.

Si vous êtes au centre-ville de Toronto et qu'il y a des manèges militaires comptant quatre ou cinq unités, la centralisation de certaines choses et le travail collectif sont une bonne solution parce les jeunes soldats qui suivent l'entraînement viennent d'une vaste région, mais ils ont aussi accès à du transport en commun, et il n'y a pas vraiment de problème.

Mais prenons une unité plus isolée, comme celle de Sault Ste. Marie. Comment centraliser à Sault Ste. Marie? Certaines zones ont vraiment besoin de nouvelles solutions. Et, si on réfléchit à l'échelle du pays, les unités des grandes zones urbaines s'en tirent bien moins mal que les unités des zones rurales. En fait, c'est pour les unités rurales que nous nous inquiétons, parce que ce sont elles qui manquent le plus de personnel. L'invocation constante des « économies d'échelle » pourrait entraîner la disparition des unités rurales si vous continuez à penser que les économies d'échelle sont la réponse à tout. Je ne crois pas que cette solution serait politiquement digeste pour les Canadiens.

Le sénateur Mitchell : J'imagine que ce n'est pas une coïncidence jusqu'à un certain point, en tout cas on pourrait défendre l'idée que ce n'est pas par hasard que le nombre de réservistes a baissé depuis que nous avons quitté l'Afghanistan. Le déploiement d'un grand nombre d'appelés dans une zone de guerre crée un vrai sentiment d'urgence. Quoi qu'on fasse, ce sentiment n'existe pas en dehors de ça. La question est ce que vous faites pour occuper les gens.

En 2011, nous avons publié un rapport où nous suggérions, entre autres, de confier aux réserves le soin de travailler sur les cybermenaces. Avez-vous donné suite à cette idée et réfléchi à la manière dont ça pourrait être structuré? On peut comprendre le besoin de continuité, mais y a-t-il moyen de créer ainsi une demande et un plus grand sentiment d'urgence parmi les réservistes?

Lcol Selkirk : C'est le genre de choses auxquelles nous devons réfléchir. Là encore, si on examine la directive du CEMD, il est question d'investir dans certains secteurs... je ne sais pas si c'est un secteur non traditionnel, mais j'imagine que c'est le cas. Nous avons des unités de réserve consacrées à la guerre électronique, et le CEMD est conscient que c'est un secteur où les réservistes pourraient être utiles.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

There is another advantage to doing more with reservists in that if we target capabilities like that, there is a lot of experience out there in the civilian world. So you could take those folks and apply them, and that makes a lot of sense as far as I'm concerned.

Senator Mitchell: Some time ago, and I'm not sure whether it was in the context of reservists but generally in the context of the military, the problem was raised with the committee that you can learn a trade in the military, but it doesn't necessarily get you a ticket in the civilian world. You could see where reservists could be attracted if they could actually begin to develop their electrician's ticket, or whatever, at 18. Has your organization given any thought to that or assessed it? Has progress been made?

Lt.-Col. Selkirk: We've given thought to it and agree that that is the most desirable situation, where those qualifications are transferable both ways. I know that work has been done on this, but I honestly don't know at this stage how much progress has been made. I know that in Alberta, some of your advocates out there were working on this and are very interested and concerned about it. I think I can say that some progress has been made, but I don't think it's as much as should be done because they can't go back and forth. It doesn't seem to work.

Senator Kenny: Welcome colonel.

I'm a bit confused with your testimony so far. You were making a case earlier about wanting 45,000 Class A reservists, and then you started talking about Sault Ste. Marie and making the opposite argument about economies of scale. Can you help me out?

Lt.-Col. Selkirk: I'm not sure that I understand exactly what you're asking.

Senator Kenny: You started out by arguing in favour of economies of scale by having 45,000 Class A reservists, and then you said the real problem is the opposite.

Lt.-Col. Selkirk: Well, if I said that, then I certainly misspoke.

Reserves 2000 feels that Canada needs to have 45,000 part-time reserve army soldiers. Having that many people would mean that units could be at least double the size they are now, more so in some cases. They need that in order to be viable and survive into the future. I don't see a contradiction there.

Senator Kenny: How about the proposition that reservists should be responsible for their own recruiting? What are the pros and cons of that?

Lt.-Col. Selkirk: The pro is that without the delays of having to visit recruiting offices, and the distances often involved, the process could be reduced. In years gone by, 20 to 30 years ago, it was done locally in the units, and it was done within a pretty short period of time.

Il y a un autre avantage à occuper les réservistes, c'est que, si on vise des ressources comme celles-là, il y a beaucoup d'expérience parmi les civils. On pourrait donc faire appel à ces gens et les mettre au travail, et ce serait très efficace à mon avis.

Le sénateur Mitchell : Il n'y a pas très longtemps, je ne sais plus très bien si on parlait des réservistes, mais en tout cas on parlait de l'armée en général, le problème a été soulevé au comité : on peut apprendre un métier dans l'armée, mais ça ne vous ouvrira pas nécessairement des portes dans le civil. On peut comprendre que des jeunes soient attirés par la réserve s'ils peuvent vraiment commencer à développer leurs compétences en électricité ou dans un autre domaine à 18 ans. Votre organisation a-t-elle réfléchi à cette solution ou en a-t-elle fait une évaluation? A-t-on fait des progrès?

Lcol Selkirk : Nous y avons réfléchi et nous pensons aussi que c'est la solution la plus souhaitable, avec des qualifications transférables dans les deux sens. Je sais qu'on y travaille, mais, honnêtement, je ne sais pas où en est la situation ni dans quelle mesure on a progressé. Je sais que, en Alberta, certains de vos partisans locaux y ont travaillé et qu'ils s'y intéressent et s'en inquiètent. Je crois que je peux dire qu'il y a eu un certain progrès, mais je ne pense pas que ce soit autant qu'il faudrait parce qu'ils ne peuvent pas faire du va-et-vient. Ça ne semble pas fonctionner.

Le sénateur Kenny : Bienvenue parmi nous, colonel.

Votre témoignage me laisse un peu perplexe jusqu'ici. Vous disiez tout à l'heure que vous vouliez 45 000 réservistes de classe A, et puis vous avez commencé à parler de Sault-Ste-Marie et fait valoir un argument inverse au sujet des économies d'échelle. Pourriez-vous clarifier?

Lcol Selkirk : Je ne suis pas certain de comprendre votre question.

Le sénateur Kenny : Vous avez commencé par vous dire en faveur d'économies d'échelle en ayant 45 000 réservistes de classe A, puis vous avez dit que le vrai problème est l'inverse.

Lcol Selkirk : Eh bien, si j'ai dit ça, je me suis certainement mal exprimé.

Le groupe Reserves 2000 estime que le Canada a besoin de 45 000 réservistes à temps partiel. À ce compte, les effectifs des unités pourraient être doublés, voire plus dans certains cas. C'est ce dont elles ont besoin pour fonctionner et survivre. Je ne vois pas de contradiction ici.

Le sénateur Kenny : Parlons de l'idée de confier aux réservistes la responsabilité de leur propre recrutement? Quels sont les arguments pour et contre?

Lcol Selkirk : L'avantage est qu'on pourrait réduire la durée du processus parce qu'il ne serait pas nécessaire de se rendre aux bureaux de recrutement et que la distance ne serait plus un problème. Auparavant, il y a 20 ou 30 ans, ça se faisait localement, dans les unités, et c'était très rapide.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Now, that will take more resources. For example, in those days every unit had a medical officer who could do the medicals. There are not enough reserve medical officers today to do that. However, those medicals can be contracted out. There are lots of doctors who I'm sure would like to make a few extra bucks. There are ways of getting around it.

Senator Kenny: Give me the pros and cons, then.

Lt.-Col. Selkirk: The pros are that history and experience tell us that the time between the individual showing an interest in joining and the time that he is actually enrolled and can start training, getting some money and doing interesting things is shortened up.

Senator Kenny: I get that, sir. I understand that, but you haven't told me any of the negatives, and every proposal has negatives. What are the problems when you revert to the old system?

Lt.-Col. Selkirk: I suspect one of the desires to centralize things was that they — "they" being the system — felt that a higher degree of quality control was more achievable because you had standards that few people in that organization were applying to a whole bunch of recruits. Whereas the opposite, if you're doing it on a disbursed basis, you have more people, and therefore the possibility of the standards not being exactly the same are higher.

I think quality control was one impetus behind centralization. I would say we need to be capable of accepting a bit of risk.

What are the risks? I assume there were risks in terms of liability, if somebody was accepted for training and turned out to have some medical problem that should have been caught, things like that. But I don't know because I didn't design the system.

Senator Kenny: What I'm saying is what would you have this committee do? Would you have us recommend a return to the old system?

Lt.-Col. Selkirk: Yes, that's exactly what we would ask for. As I say, to keep it short and to put it in a few sweet words, we feel that the policies of centralization that are so beloved at NDHQ should be relaxed and there should be much more decentralization.

Senator Kenny: Thank you.

The Deputy Chair: Colonel, can you tell us the position of Reserves 2000 with respect to the suggestion that has been made on a number of occasions recently of trying to re-instigate, re-implement the Reserve Officers' Training Corps at universities to try to get the future officers training during the winter? Some of them, as you point out, especially in the rural areas and in

Aujourd'hui, ça prend plus de ressources. Par exemple, à l'époque, chaque unité avait un médecin militaire qui pouvait s'occuper des certificats. Aujourd'hui, il n'y a plus assez de médecins militaires pour faire ce travail. Mais ces tâches pourraient être confiées à l'extérieur. Il y a beaucoup de médecins qui aimeraient se faire un peu d'argent supplémentaire. Il y a moyen de contourner le problème.

Le sénateur Kenny : Parlez-moi des avantages et inconvénients, alors.

Lcol Selkirk : L'avantage, c'est qu'on raccourcit le délai entre le moment où la personne manifeste son intérêt et celui où elle est effectivement enrôlée et peut commencer l'entraînement, gagner un peu d'argent et faire des choses intéressantes.

Le sénateur Kenny : Je comprends bien, monsieur. Je comprends ça, mais vous ne m'avez pas parlé des aspects négatifs éventuels, et toute proposition comporte des inconvénients. En quoi le retour à l'ancien système pourrait-il être problématique?

Lcol Selkirk : Je suppose que le désir de centraliser est, entre autres, motivé par le fait qu'ils — par « ils », je veux dire le système — pensent qu'on peut ainsi mieux contrôler la qualité parce qu'il y a des normes appliquées par moins de gens à tout un tas de recrues. À l'inverse, si on décentralise, il y a plus de gens en cause, et le risque que les normes ne soient pas appliquées exactement de la même façon est plus grand.

Je pense que le contrôle de la qualité est l'un des ressorts de la centralisation. Je dirais que nous devons être capables d'accepter une certaine part de risque.

Quels sont les risques? Probablement des risques en termes de responsabilité, par exemple si une personne a été acceptée pour l'entraînement et qu'il se trouve qu'elle a un problème médical qu'on aurait dû repérer, des choses comme ça. Mais je ne sais pas, car ce n'est pas moi qui ai conçu le système.

Le sénateur Kenny : Ce que je demande, c'est ce que vous souhaitez que fasse le comité. Voudriez-vous que nous recommandions le retour à l'ancien système?

Lcol Selkirk : Oui, c'est exactement ce que nous demanderions. Je le répète, pour dire les choses en bref et en douceur, nous pensons que les politiques chères au cœur du QGDN devraient être assouplies, et les choses devraient être beaucoup plus décentralisées.

Le sénateur Kenny : Je vous remercie.

Le vice-président : Colonel, pourriez-vous nous parler de la position de Reserves 2000 concernant l'idée souvent proposée dernièrement d'essayer de relancer, de remettre en vigueur le Corps-école des officiers de réserve dans les universités pour inciter les futurs officiers à s'entraîner durant l'hiver? Certains d'entre eux, comme vous l'avez fait remarquer, notamment dans

New Brunswick — for example, going from the University of New Brunswick to Saint John to meet with the unit once a week is pretty tough for a student. Can you help us with that?

Lt.-Col. Selkirk: There is a private initiative. There is a name for the program, which escapes me at the moment; however, it is mentioned in the document from the CDS. It is, for want of a better term, the return of a COTC type of program. The program would not be just officers, however, because it's recognized that today a lot of non-commissioned members are also attending universities and other post-secondary institutions.

We are all in favour of it. Anything that will increase the number of leaders at the unit level is very desirable from our point of view, because right now it just isn't working. There are not enough leaders. We are all in favour.

A pilot project at the University of Alberta is under way now, Senator Mitchell. It's being expanded to Quebec and I believe to Halifax as well. The navy is quite interested in that program.

The Deputy Chair: I'm glad to hear that. When we have the navy in, we'll ask them how that's going.

You talked about the mandate of the new minister to look into the Armed Forces and, in particular, the reserve element. Has Reserves 2000 been approached by the minister yet with respect to that review?

Lt.-Col. Selkirk: No, we have not, and of course the review is defence policy. No, we have not been approached, but we have approached his office and said, "We want to be part of it," but I've heard nothing back at this point.

The Deputy Chair: Thank you.

Senator White: Thank you again for being here.

A number of countries identify that the six-month required or voluntary exposure to the military in those countries by 18-year-olds is very helpful to them filling their requirements for militia and other reservists. In Canada, back about 30 years ago, we had a similar program, but it was two months and we would fill militia units across the country. In fact, at the end of those two months, a lot of militia units would be told, "There are 200 applicants and you can take 25." That's how many there were.

You haven't said it outright, but a movement back to what worked for keeping those numbers at the top. Really, exposure is what will get kids interested in reservists — 16-year-olds, and then doing it at 17 and 18, going to university and maybe even joining the military full time. Would you agree that that's really where we're going to work?

les zones rurales et au Nouveau-Brunswick... par exemple, il est plutôt difficile pour un étudiant de l'Université du Nouveau-Brunswick de se rendre à Saint-Jean pour y rejoindre son unité une fois par semaine. Pourriez-vous nous en parler?

Lcol Selkirk : C'est une initiative privée. Ce programme a un nom qui m'échappe pour l'instant, mais on en parle dans le document du CEMD. Il s'agit, faute de mieux dire, du retour d'un programme du genre du Corps-école des officiers canadiens. Mais ce programme ne s'adresserait pas seulement aux officiers, parce qu'on sait que, de nos jours, beaucoup de sous-officiers fréquentent aussi l'université et d'autres établissements postsecondaires.

Nous sommes tous en faveur de ça. Tout ce qui permettra d'augmenter le nombre de chefs à l'échelle des unités est très souhaitable selon nous, parce que, actuellement, ça ne fonctionne pas. Il n'y a pas assez de chefs. Nous sommes tout à fait pour.

Je dois vous dire, sénateur Mitchell, qu'il y a un projet pilote en cours à l'Université de l'Alberta. On est en train de le lancer au Québec et à Halifax aussi, je crois. La Marine s'y intéresse beaucoup.

Le vice-président : Je suis heureux d'entendre ça. Lorsque nous aurons des témoins de la Marine, nous leur demanderons comment ça se déroule.

Vous avez parlé du mandat du nouveau ministre, qui comprend un examen des Forces canadiennes et plus particulièrement de la Réserve. Est-ce que le groupe Reserves 2000 a déjà été approché par le ministre à cet égard?

Lcol Selkirk : Non, et, bien sûr, cet examen fait partie de la politique du ministère de la Défense. Non, il ne nous a pas approchés, mais nous avons fait savoir à son cabinet que nous voulons participer. Il n'y a pas eu d'autre communication jusqu'ici.

Le vice-président : Je vous remercie.

Le sénateur White : Merci encore d'être parmi nous aujourd'hui.

Un certain nombre de pays ont constaté que le service militaire de six mois obligatoire ou volontaire des jeunes de 18 ans contribue largement à faciliter le recrutement dans la milice et les autres réserves. Au Canada, nous avons eu un programme semblable il y a une trentaine d'année, mais il durait deux mois, et on remplissait les unités de la milice d'un bout à l'autre du pays. En fait, au bout des deux mois, on disait à beaucoup d'unités : « Il y a 200 candidats, et vous pouvez en prendre 25. » C'était dans cet ordre de grandeur.

Vous ne l'avez pas dit carrément, mais le retour à ce qui permettait d'enregistrer ce genre de chiffres... en réalité, c'est le contact qui permet d'attirer ces jeunes dans la Réserve, quand ils ont 16 ans, ensuite ils s'engagent à 17 ou 18 ans, ils vont à l'université et ils s'engagent même parfois à temps plein dans l'armée. Ne pensez-vous pas que c'est vraiment comme ça que ça marche?

Lt.-Col. Selkirk: Absolutely. I was a cadet and then I joined the militia when I was 16. As soon as I left high school I joined the regular army. I served for 20 years and then I went right back to the militia. That's exactly the model I went through. It was called the Student Militia Training Program.

Senator White: The same model I went through.

Lt.-Col. Selkirk: It was a wonderful program. Why it was discarded, I have no idea.

Senator White: Thank you very much.

[*Translation*]

Senator Carignan: I was looking at the Government of Canada's job search websites. The Government of Canada's Job Bank is a single window website. If I were looking for a job that is the site I would go to. That is also the site I would go to if I were an employer looking for candidates who are looking for a job. If I do a search with the word "army," there is only one section in British Columbia that has postings for reservists. The job posting says that the salary is $90 a day. How badly does the Department of National Defence want to hire reservists? Do you think the department truly wants new recruits? If so, that is definitely not coming across in the basic recruitment tools.

[*English*]

Lt.-Col. Selkirk: Senator, I agree with you. You have to wonder if indeed the leadership wants the reservists to succeed. I agree with you entirely. I think the proof of that is in the fact that the strength is 5,000 under. If the reserves were really valued, would there not have been action taken in the last five years to prevent that?

Your question is excellent, to which I do not have the answer. All I can say is look at the evidence.

Senator Kenny: My understanding was that the principal problem facing the Class A reserves was a cut to their O&M. The rest of the Armed Forces have had a similar cut, and the budgets that different regiments have just isn't sufficient. If you take 20 per cent away, there's not enough dough to do anything, and that's why we're not seeing programs that interest people or training that people want to engage in. That's why we've had a drop in members. Is that your assessment?

Lt.-Col. Selkirk: Yes, that is my assessment, except we're in this remarkable situation now where units — and I have had this reported to me from across the country — have more Class A pay money than they can spend.

Lcol Selkirk : Absolument. J'ai été cadet et je me suis engagé dans la milice à 16 ans. Dès que j'ai quitté l'école secondaire, je me suis engagé dans l'armée régulière. J'ai servi pendant 20 ans, puis je suis retourné à la milice. C'est exactement la démarche que j'ai suivie. Ça s'appelait le programme d'entraînement de la milice pour étudiants.

Le sénateur White : J'ai suivi la même démarche.

Lcol Selkirk : C'était un programme magnifique. Je ne sais absolument pas pourquoi on l'a éliminé.

Le sénateur White : Je vous remercie.

[*Français*]

Le sénateur Carignan : Je consultais les sites Internet du gouvernement du Canada qui sont consacrés à la recherche d'emploi; lorsqu'on y recherche un emploi, il y a un guichet unique : le site Guichet-Emplois du gouvernement du Canada. Si j'étais à la recherche d'un emploi, c'est ce site que je consulterais. C'est également sur ce site que je devrais m'afficher à titre d'employeur dans le but d'attirer des candidats qui sont à la recherche d'un emploi. Si j'y fais une recherche avec le mot « armée », je trouve seulement une section qui se trouve en Colombie-Britannique et qui offre des postes de réservistes. Or, lorsque je consulte l'offre d'emploi, on y indique un salaire de 90 $ par jour. Le ministère de la Défense nationale désire-t-il vraiment se doter de réservistes? Percevez-vous vraiment une volonté de recruter de la part du ministère? Si oui, manifestement, cela ne se traduit pas dans les outils de base de recrutement.

[*Traduction*]

Lcol Selkirk : Je suis d'accord avec vous, monsieur le sénateur. On en vient à se demander si les dirigeants veulent vraiment que les réservistes réussissent. Je suis entièrement d'accord avec vous. Je pense qu'on en a la preuve dans le fait que les effectifs sont privés de 5 000 personnes. Si les réserves étaient vraiment appréciées, est-ce qu'on n'aurait pas pris des mesures pour empêcher cette baisse depuis cinq ans?

C'est une excellente question, à laquelle je ne peux pas répondre. Tout ce que je peux dire, c'est : considérez les faits.

Le sénateur Kenny : J'ai cru comprendre que la principale difficulté des réserves de classe A était les coupures effectuées dans leurs budgets d'exploitation et de maintenance. Les autres divisions des Forces canadiennes ont subi les mêmes coupures, et les budgets des différents régiments ne sont tout simplement pas suffisants. Si on enlève 20 p. 100, il n'y a pas assez de levure pour faire lever quoi que ce soit, et c'est pourquoi il n'y a pas de programmes susceptibles d'intéresser des gens ni d'entraînement qui donne envie à des gens de s'y engager. C'est pour ça qu'on perd des militaires. C'est ce que vous pensez?

Lcol Selkirk : Oui, c'est ce que je pense, sauf que nous sommes actuellement dans une situation remarquable où les unités — et c'est ce qu'on m'a dit à travers le pays — ont maintenant plus d'argent qu'elles ne peuvent en dépenser pour payer des réservistes de classe A.

Senator Kenny: But they don't have —

Lt.-Col. Selkirk: They just don't have the O&M money.

Senator Kenny: Right, so one without the other is like toast without jam.

Lt.-Col. Selkirk: Exactly. So now we have this ironic position where there is money, but the young kids can't get it because they're not doing training, so they say, "I'm going to work at McDonald's or somewhere else."

The Deputy Chair: Thank you very much. It is good we got that on the record. Class A reserve is the typical reservist who works one night per week and appears usually one weekend per month. That's a Class A reserve as Senator Kenny referred to.

Lt.-Col. Selkirk: Yes.

The Deputy Chair: There are other classes that we don't need to get into, but I just wanted to clarify the record.

The other point was, if I'm not misquoting Julie Lindhout, who was here last week, the group is now called NATO Council of Canada. It was the North Atlantic Council. They've changed their name to NATO Council. Do you agree with that?

Lt.-Col. Selkirk: Yes, I do. I keep getting confused.

The Deputy Chair: I just wanted to clarify the record, in case somebody was looking for the name.

Lt.-Col. Selkirk: That's the organization I was referring to.

The Deputy Chair: It is now chaired by a former senator of this committee, Senator Segal, and prior to that Bill Graham was chair of that committee.

Lt.-Col. Selkirk: That's right.

The Deputy Chair: Colonel, thank you very much for being here and for the work that Reserves 2000 is doing to help keep this issue of reservists alive. The fact that we did a report is an indication that we as a committee in the Senate are very interested and concerned about the reserves. We look forward to working with you in the future to make sure that some of the concerns you have expressed today don't come about.

Lt.-Col. Selkirk: Thank you very much, senator. Thank you for having me.

The Deputy Chair: Honourable senators, now we have with us our second panel for today.

The Security Intelligence Review Committee tabled in 2014-15 its annual report to Parliament on January 28 of this year, less than a month ago. SIRC's reviews included insider threats, foreign fighters and the collection of information from the Canada Revenue Agency, all subjects of concern and interest to this committee.

Le sénateur Kenny : Mais elles n'ont pas...

Lcol Selkirk : Elles n'ont pas de budget d'exploitation et de maintenance.

Le sénateur Kenny : C'est ça, donc l'un sans l'autre, c'est comme une tranche de pain sans confiture.

Lcol Selkirk : Exactement. Donc, maintenant, on est dans une situation ironique où on a de l'argent, mais où les jeunes ne peuvent pas y avoir accès parce qu'ils n'ont pas d'entraînement, et ils se disent : « Je vais aller travailler chez McDonald ou ailleurs. »

Le vice-président : Merci beaucoup. C'est une bonne chose qu'on ait enregistré ça. Le réserviste de classe A est généralement quelqu'un qui vient travailler un soir par semaine et se présente le plus souvent un week-end par mois. C'est le réserviste de classe A tel qu'en parlait le sénateur Kenny.

Lcol Selkirk : C'est ça.

Le vice-président : Il y a d'autres catégories dont il n'est pas nécessaire de parler ici, mais je voulais simplement le préciser.

L'autre problème, et j'espère citer correctement Julie Lindhout, qui était ici la semaine dernière, c'est que le groupe s'appelle désormais Conseil de l'OTAN du Canada. C'était auparavant le Conseil de l'Atlantique Nord. Ils ont remplacé ça par Conseil de l'OTAN. Qu'en pensez-vous?

Lcol Selkirk : Je suis d'accord, mais que voulez-vous dire?

Le vice-président : Je voulais seulement préciser les choses, au cas où quelqu'un chercherait le nom.

Lcol Selkirk : C'est bien l'organisme dont je parlais.

Le vice-président : Il est maintenant présidé par un ex-sénateur du comité, le sénateur Segal. Auparavant, c'était Bill Graham qui présidait le comité.

Lcol Selkirk : C'est exact.

Le vice-président : Colonel, nous vous remercions de votre visite et du travail que fait le groupe Réserves 2000 pour rappeler la situation des réservistes. Le fait que le comité sénatorial ait publié un rapport témoigne de notre souci et de nos inquiétudes à l'égard des réserves. Nous aurons plaisir à collaborer avec vous dans l'avenir pour veiller à ce que certaines des préoccupations que vous avez exprimées aujourd'hui trouvent une solution.

Lcol Selkirk : Merci beaucoup, monsieur le sénateur. Merci de m'avoir reçu.

Le vice-président : Honorables sénateurs, passons maintenant à notre deuxième groupe de témoins.

Le Comité de surveillance des activités de renseignement de sécurité a déposé son rapport annuel 2014-2015 au Parlement le 28 janvier de cette année, il y a moins d'un mois. L'examen du comité a porté, entre autres, sur les menaces internes, les combattants étrangers et la collecte d'information auprès de l'Agence du revenu du Canada, tous sujets intéressant notre comité.

The Office of the Communications Security Establishment Commissioner tabled its 2014-15 annual report to Parliament on the same date, January 28, 2016. The report reviews included metadata, information technology security, and disclosures of Canadian identity information. Those subjects are covered in their reports, and we're looking forward to hearing from our witnesses and representatives of each of those groups at this time.

From the Security Intelligence Review Committee, we welcome the Honourable Pierre Blais, Chairman; and Michael Doucet, Executive Director. From the Office of the Communications Security Establishment Commissioner, we welcome the Honourable Jean-Pierre Plouffe, Commissioner; and J. William Galbraith, Executive Director.

Which group would like to begin?

Hon. Pierre Blais, Chair, Security Intelligence Review Committee: Good afternoon. Thank you for the opportunity to speak to you about the work that SIRC has been doing.

SIRC's annual report for the fiscal year 2014-15 was tabled in Parliament in January, as you mentioned. It was in fact delayed due to the federal election. Normally, it is tabled in October, so SIRC will likely table two annual reports this year.

The Deputy Chair: One for the former government and one for this government?

Mr. Blais: We will complete our year in a few weeks.

The annual report contains unclassified summaries of SIRC's reviews and complaints investigations, including recommendations and CSIS's response to those recommendations.

Of note in 2014-15, SIRC noted an improvement from last year with respect to the timely disclosure of information to SIRC by CSIS. In most of its work this year, including the certificate, nine reviews and five finalized complaint investigations, SIRC was satisfied with the manner in which CSIS carried out its mandate to investigate threats to the security of Canada.

However, in two reviews, SIRC felt that the significance of the issues it found warranted sending the reports directly to the Minister of Public Safety as special reports under section 54 of the CSIS Act. I will speak to those shortly, but we will begin with the certificate and also discuss a special examination we conducted at the request of the director.

Le Bureau du commissaire du Centre de la sécurité des télécommunications a déposé son rapport annuel 2014-2015 au Parlement à la même date, le 28 janvier 2016. Il porte, entre autres, sur les métadonnées, la sécurité des technologies de l'information et la divulgation de renseignements sur l'identité des Canadiens. Ces sujets sont abordés dans leurs rapports, et nous aurons maintenant le plaisir d'entendre des témoins et représentants de chacun de ces groupes.

Pour représenter le Comité de surveillance des activités de renseignement de sécurité, nous accueillons l'honorable Pierre Blais, son président, et Michael Doucet, son directeur exécutif. Pour représenter le Bureau du commissaire du Centre de la sécurité des télécommunications, nous accueillons l'honorable Jean-Pierre Plouffe, son commissaire, et J. William Galbraith, son directeur exécutif.

Quel groupe voudrait commencer?

L'honorable Pierre Blais, président, Comité de surveillance des activités de renseignement de sécurité : Bonjour et merci de m'avoir invité à venir vous parler du travail du CSARS.

Le rapport annuel du CSARS pour l'exercice 2014-2015 a été déposé au Parlement en janvier, comme vous l'avez dit. Le dépôt en a, en fait, été retardé par l'élection fédérale. En principe, il est déposé en octobre. Il est donc probable que le CSARS déposera deux rapports annuels cette année.

Le vice-président : Un pour l'ancien gouvernement et un pour le nouveau?

M. Blais : Notre exercice se termine dans quelques semaines.

Le rapport annuel contient des résumés non confidentiels des examens et enquêtes du CSARS ainsi que de ses recommandations et des réponses du SCRS à ces recommandations.

Le CSARS a noté que, en 2014-2015, la situation s'est améliorée par rapport à l'année précédente du point de vue de la communication de renseignements du SCRS au CSARS. La plupart du temps cette année, y compris à l'égard du certificat, de neuf examens et de cinq enquêtes faisant suite à des plaintes, le CSARS a été satisfait de la façon dont le SCRS a rempli son mandat dans le cadre des enquêtes sur les menaces pesant sur la sécurité du Canada.

Mais, dans le cas de deux examens, le CSARS a estimé que l'importance des enjeux soulevés justifiait l'envoi direct de rapports spéciaux au ministre de la Sécurité publique en vertu de l'article 54 de la Loi sur le SCRS. J'en parlerai dans un moment, mais nous commencerons par le certificat et nous discuterons aussi d'un examen spécial que nous avons effectué à la demande du directeur.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*Translation*]

This year, with one exception, our certificate found that the activities described in the CSIS director's annual report did not contravene the CSIS Act or ministerial direction, and were reasonable and necessary.

SIRC decided to ground its satisfaction of the director's report in a broader appreciation of its original intent, namely, to support the minister in his role. This reflection led us to recommend the issuance of a renewed ministerial direction that would outline more explicit instructions to the service with respect to the format, content and timing of the director's report.

For this accountability mechanism to work, there needs to be an effective system of communication between the service and the minister and his or her deputy, to ensure that the minister is informed of CSIS activities that raise questions of legality or propriety.

It remains the case today. However, the director's report, in its present form, contains long descriptions of the main investigations that do not change substantially from year to year. Far from being an aid to ministerial accountability, the level of detail has the effect of obscuring the more important information for ministerial consideration, including serious issues, challenges, and potentially controversial activities.

[*English*]

SIRC recommended that the minister make his expectation known to CSIS with respect to the form and structure of the director's report, as well as with respect to being notified of CSIS high-risk activities.

[*Translation*]

SIRC's reviews provide a retrospective examination and assessment of a representative sample of CSIS investigations and activities. Each review results in a snapshot of the service's actions in a specific case. This approach allows SIRC to manage the risk inherent in being able to review only a small number of CSIS activities in any given year.

In the year that just ended — 2014-15 —

[*English*]

SIRC conducted two studies which warranted sending the report directly to the Minister of Public Safety and special reports under section 54 of the CSIS Act.

The first report stemmed from examination of CSIS's management of insider threats. SIRC's review identified concerns regarding the training, access and documentation of insider threat investigations and identified one case that it felt was not sufficiently resolved.

[*Français*]

Cette année, tout en tenant compte d'une exception, nous avons constaté, lors du processus de remise du certificat, que les activités décrites étaient conformes à la Loi sur le SCRS et aux directives ministérielles, et qu'elles ne constituaient pas un exercice abusif ou inutile par le service de ses pouvoirs.

Le CSARS a décidé d'entreprendre l'exercice du certificat d'une manière plus large, notamment dans l'intention de soutenir le ministre dans son rôle. C'est dans cette optique que nous avons recommandé que soit émise une nouvelle directive ministérielle qui donnerait au service des instructions plus claires sur le format, le contenu et l'échéancier du rapport annuel du directeur.

Pour que ce mécanisme de reddition de comptes fonctionne, il faut qu'il existe un système efficace de communication entre le service et le ministre, et également son sous-ministre, et ce, pour que le ministre soit informé de toute activité du SCRS qui soulève des questions portant sur son caractère opportun et légal.

Ceci est toujours d'actualité. Toutefois, le rapport du directeur, dans sa formule actuelle, est rempli de longues descriptions des enquêtes principales, auxquelles peu de changements sont apportés d'une année à l'autre. Loin d'accroître la responsabilité ministérielle, cette approche noie dans une foule de détails des informations majeures qui devraient être portées à l'attention du ministre, comme des enjeux clés, les grands défis ou des activités potentiellement sujettes à controverse.

[*Traduction*]

Le CSARS a recommandé au ministre de faire connaître ses exigences au SCRS quant à la forme et la structure du rapport du directeur et de préciser qu'il devait être informé des activités à haut risque du Service.

[*Français*]

Les études du CSARS fournissent un examen rétrospectif et une évaluation d'un échantillon représentatif d'enquêtes et d'activités du service. Chaque étude est un instantané des agissements du SCRS dans une affaire précise. Cette approche permet au comité de gérer le risque inhérent à ne pouvoir examiner qu'un nombre restreint des activités du SCRS au cours d'une année donnée.

Dans l'année qui s'est terminée, 2014-2015...

[*Traduction*]

Le CSARS a effectué deux études dont les résultats justifiaient l'envoi direct du rapport au ministre de la Sécurité publique et l'établissement de rapports spéciaux en vertu de l'article 54 de la Loi sur le SCRS.

Le premier rapport découlait de l'examen de la gestion des menaces internes par le SCRS. Le CSARS a circonscrit des difficultés concernant la formation, l'accès, et la documentation des enquêtes sur les menaces internes, dont un cas qui, selon le comité, n'avait pas été réglé suffisamment bien.

The second report examined CSIS's relationship with the Department of Foreign Affairs, Trade and Development. SIRC raised serious concerns with the application of the United Nations Al-Qaida and Taliban Regulations, which is known as UNAQTR. I will discuss each of these in a bit more detail.

[*Translation*]

In the aftermath of high-profile classified documents leaks such as those attributed to WikiLeaks, Edward Snowden, and Sub-Lt. Jeffrey Paul Delisle — in Canada in the latter case — the "Five Eyes" community has elevated the concern posed by the "insider threat" to a higher level. Intelligence agencies are paying increased attention to the insider threat in order to reduce its potential rate of occurrence and, failing that, to help limit the damage that can be caused by a malicious internal actor. This review set out to examine the service's efforts to mitigate insider threats, in particular with respect to information management.

[*English*]

SIRC found that there are some unsatisfactory thresholds for internal investigations. SIRC recommended that CSIS create more detailed policy on the conduct of internal security investigations into suspected violations and/or breaches of security. SIRC also recommended that CSIS take immediate action to appropriately document all decisions made pertaining to internal investigations in accordance with the standard requirement set by Treasury Board guidelines.

Finally, SIRC recommended that internal security forward final investigation reports to a group outside of its unit for review to help ensure that the investigation is complete, objective and well documented.

CSIS agreed with most of the recommendations and will create more detailed policy on the conduct of internal security investigations and will undertake a review to clarify definitions, timelines and techniques as well as develop clear procedures to ensure that all decision-making pertaining to internal investigations is documented appropriately.

In the second section 54 review, SIRC examined CSIS's relationship with the Department of Foreign Affairs, Trade and Development, now called Global Affairs Canada. Overall, SIRC found CSIS's relationship with DFATD overseas missions to be positive. However, SIRC raised a potential legal concern with respect to CSIS activities and a United Nations Al-Qaida and Taliban Regulation. In fact, CSIS lacks a procedure to systematically verify whether past or ongoing human-source operations conducted against al Qaeda and Taliban threats are in contravention of the United Nations AQTR.

Dans le second, il était question des relations entre le SCRS et le ministère des Affaires étrangères, du Commerce et du Développement. Le CSARS s'est dit très inquiet de la mise en œuvre du Règlement d'application des résolutions des Nations Unies sur Al-Qaïda et le Taliban, ou RNUAQT. Je parlerai de chacun de ces rapports un peu plus en détail.

[*Français*]

À la suite de fuites importantes de documents classifiés, comme celles qu'on a attribuées à WikiLeaks, à Edward Snowden et au sous-lieutenant Jeffrey Paul Delisle — au Canada, dans ce dernier cas —, la communauté du Groupe des cinq a placé le problème posé par la menace interne au sommet de ses préoccupations. Il s'agit là d'un risque auquel les organismes de renseignement prêtent une attention accrue, et ce, pour le réduire ou, à défaut, pour limiter les dommages qui peuvent être causés par un agent interne malveillant. Cette étude s'est attachée à passer au crible les efforts du Service canadien du renseignement de sécurité pour atténuer le risque de menace interne, en particulier dans le cadre de la gestion de l'information.

[*Traduction*]

Le CSARS a estimé que certains seuils applicables aux enquêtes internes sont insatisfaisants. Il a recommandé au SCRS de se doter d'une politique plus détaillée sur le déroulement des enquêtes internes portant sur les violations et/ou infractions présumées en matière de sécurité. Il lui a également recommandé de prendre immédiatement des mesures pour justifier correctement par des documents toutes les décisions relatives aux enquêtes internes, conformément aux exigences habituelles énoncées dans les lignes directrices du Conseil du Trésor.

Enfin, le CSARS a recommandé que la sécurité interne adresse les rapports d'enquête définitifs à un groupe extérieur à son unité pour que celui-ci vérifie que l'enquête est complète, objective et bien documentée.

Le SCRS a accepté la plupart des recommandations et se dotera d'une politique plus détaillée sur le déroulement des enquêtes de sécurité interne. Il procédera également à un examen pour clarifier les définitions, les délais et les techniques et élaborera des procédures claires pour veiller à ce que toutes les décisions relatives aux enquêtes internes soient correctement documentées.

Dans son deuxième examen en vertu de l'article 54, le CSARS a examiné les relations entre le SCRS et le ministère des Affaires étrangères, du Commerce et du Développement, qui s'appelle désormais Affaires mondiales Canada. Il a conclu que, dans l'ensemble, les relations entre le SCRS et les missions du ministère à l'étranger sont positives. Mais il a circonscrit un problème juridique potentiel concernant les activités du SCRS et un Règlement des Nations Unies portant sur Al-Qaïda et le Taliban. En fait, le SCRS a besoin d'une procédure lui permettant de vérifier systématiquement si ses opérations

SIRC recommended that CSIS put in place formal internal mechanisms to ensure that none of its human-source operations are in contravention of the United Nations AQTR or any similar Canadian statutes or regulations. SIRC also felt that CSIS needed to examine the full scope of potential violations. Therefore, the committee directed the service to conduct a section 40 review and report the result to the Minister of Public Safety, which CSIS has agreed to do. SIRC will examine the methodology and findings of the CSIS review and provide an assessment both to the Minister of Public Safety and to Parliament.

Regarding the special request, in 2014-15 SIRC also took on, at the request of the CSIS director, an additional examination. In August 2014, the CSIS director notified SIRC's interim chair of an incident involving a CSIS intelligence officer who obtained taxpayer information from the Canada Revenue Agency without a Federal Court warrant. CSIS requested that SIRC review the circumstances surrounding the incident and make recommendations as necessary and appropriate to ensure proper accounting.

SIRC takes very seriously CSIS obtaining taxpayer information improperly. SIRC made a number of findings that lead to several recommendations; namely, that CSIS conduct an audit and a postmortem, clarify the scope of the incident to the Federal Court and the Minister of Public Safety, and advise the Privacy Commissioner.

[*Translation*]

The committee determined it was not able to make recommendations aimed at preventing such a future occurrence because SIRC was not provided with any explanation to account for the full scope of the improper collection of taxpayer information.

Therefore, though the immediate action taken by the CSIS Executive — to issue a stern reminder to all employees of the need for a warrant to collect taxpayer information — was appropriate in the circumstances, it may not be sufficient.

The committee considers that, if the sharing of taxpayer information from CRA to CSIS is put on a new footing as a result of the new Security of Canada Information Sharing Act, a routine audit of those activities through a renewed memorandum of understanding could be even more important.

The past year witnessed significant legislative developments in the national security area, with the adoption of new laws that brought important amendments to the CSIS Act. For example,

antérieures ou en cours faisant appel à des sources humaines et dirigées contre les menaces exercées par Al-Qaïda et le Taliban ne contreviennent pas au RNUAQT.

Le CSARS a recommandé au SCRS d'instaurer des mécanismes internes officiels permettant de veiller à ce qu'aucune de ses opérations faisant appel à des sources humaines ne contrevient au RNUAQT ni à aucun règlement ou loi du Canada. Il estimait également que le SCRS devait examiner tout l'éventail des violations potentielles. Le comité lui a donc recommandé de procéder à un examen en vertu de l'article 54 et de rendre compte de son résultat au ministre de la Sécurité publique, ce que le SCRS a accepté de faire. Le CSARS examinera la méthodologie et les conclusions de cet examen et adressera une évaluation à la fois au ministre de la Sécurité publique et au Parlement.

Concernant la demande spéciale, le CSARS a également procédé, en 2014-2015, à un examen supplémentaire à la demande du directeur du SCRS. En août 2014, le directeur du SCRS a informé le président intérimaire du CSARS d'un incident mettant en cause un agent du renseignement qui avait obtenu des renseignements sur un contribuable auprès de l'Agence du revenu du Canada sans mandat de la Cour fédérale. Le SCRS a demandé au CSARS d'examiner les circonstances de l'incident et de faire les recommandations nécessaires et utiles pour garantir une bonne reddition de comptes.

Le CSARS prend très au sérieux le fait que des renseignements sur un contribuable aient pu être obtenus par le SCRS de façon illicite. Il a tiré un certain nombre de conclusions donnant lieu à plusieurs recommandations, à savoir que le SCRS devra procéder à une vérification et à une évaluation post-mortem, qu'il devra clarifier la portée de l'incident avec la Cour fédérale et le ministre de la Sécurité publique et qu'il devra informer le commissaire à la protection de la vie privée.

[*Français*]

Le comité a déterminé qu'il n'était pas en mesure d'émettre de recommandations qui permettraient d'éviter qu'un tel incident se reproduise. On ne lui a fourni aucune explication concernant l'étendue de la collecte inappropriée des renseignements sur les contribuables.

Par conséquent, même si les mesures immédiates prises par les cadres du SCRS, soit l'envoi d'un rappel à l'ordre sévère à tous les employés sur la nécessité d'un mandat pour collecter des renseignements sur les contribuables, étaient appropriées dans le cadre des circonstances, elles demeurent insuffisantes.

Le comité considère que si cette activité reçoit une nouvelle assise dans le cadre de la nouvelle Loi sur la communication d'information ayant trait à la sécurité du Canada, l'élaboration d'un nouveau protocole d'entente comprenant une vérification de routine des activités pourrait s'avérer cruciale.

Des évolutions législatives majeures dans le domaine de la sécurité nationale ont été amorcées cette année avec l'adoption de nouvelles lois qui ont apporté d'importantes modifications à la

our committee, SIRC, now has the statutory obligation to annually review at least one aspect of the service's performance in taking measures to reduce threats to the security of Canada.

This responsibility will require a significant resource commitment from SIRC because threat reduction activities are by their very nature potentially controversial and/or high risk, meaning SIRC will need to ensure these activities are examined annually in a focused and dedicated manner.

[*English*]

While additional funding for SIRC was announced in the Government of Canada's Economic Action Plan in April 2015, it was not until the end of January 2016 that the funding was a proven practice. For staffing purposes, SIRC only has funding for one year.

[*Translation*]

Nonetheless, SIRC is clearly willing and able to meet rising expectations. SIRC's work has evolved significantly in past years and, with recent developments, our pace of change will undoubtedly hasten in the months and years ahead. In this transformative process, however, we will remain focused on the principle that has guided our work since 1984 and that is to serve as a cornerstone for ensuring the accountability of Canada's security intelligence activities.

[*English*]

Thank you very much. I welcome any questions you may have about our full report.

[*Translation*]

The Deputy Chair: Thank you, Mr. Blais. We will follow up with Mr. Plouffe and then senators may ask you some questions. Mr. Plouffe, you have the floor.

Hon. Jean-Pierre Plouffe, Commissioner, Office of the Communications Security Establishment Commissioner: Chair, honourable senators, I am pleased to appear once again before this honourable committee.

I welcome this opportunity to discuss the work of my office and how it contributes to effective governance and accountability of the Communications Security Establishment, or CSE's operational activities.

It is especially important at this time when changes to intelligence review and oversight are being considered by the government and being discussed by academics and others of the interested public.

Loi sur le SCRS. Par exemple, notre comité, le CSARS, a maintenant l'obligation légale d'examiner à chaque exercice au moins un aspect de la prise par le service de mesures pour réduire les menaces envers la sécurité du Canada.

Cette responsabilité mobilisera, dans une large mesure, les ressources du comité, car il s'agit d'activités qui sont, par nature, sujettes à de potentielles controverses et/ou à haut risque. Cela signifie qu'elles devront être examinées tous les ans de manière ciblée et adéquate.

[*Traduction*]

Des fonds supplémentaires ont été annoncés à l'intention du CSARS dans le Plan d'action économique du gouvernement du Canada en avril 2015, mais ce n'est qu'à la fin de janvier 2016 que le financement a été effectif. Pour la dotation en personnel, le CSARS dispose d'un budget sur un an.

[*Français*]

Néanmoins, le SCARS est clairement désireux et capable de satisfaire aux attentes croissantes. Son travail a considérablement évolué au cours des dernières années, au fil des récents changements, et les choses vont certainement s'accélérer dans les mois et années à venir. Nous garderons toutefois le cap sur le principe qui nous guide depuis 1984, notre rôle de pierre angulaire, d'un mécanisme qui permet d'assurer une reddition de comptes des activités du renseignement de sécurité au Canada.

[*Traduction*]

Merci beaucoup. Je répondrai avec plaisir à vos questions sur l'ensemble du rapport.

[*Français*]

Le vice-président : Merci, monsieur Blais. Nous allons enchaîner avec M. Plouffe et, par la suite, les sénateurs pourront vous poser des questions. Monsieur Plouffe, vous avez la parole.

L'honorable Jean-Pierre Plouffe, commissaire, Bureau du commissaire du Centre de la sécurité des télécommunications : Monsieur le président, honorables sénateurs, dans un premier temps, je suis heureux de témoigner à nouveau devant cet honorable comité.

Je me réjouis de l'occasion qui m'est offerte de m'entretenir du travail de mon bureau et de la mesure dans laquelle il contribue à assurer une gouvernance et une reddition de comptes efficace des activités opérationnelles du Centre de la sécurité des télécommunications, connu sous l'acronyme CST.

Je considère cette occasion particulièrement importante en cette période où le gouvernement examine la possibilité d'apporter des changements ou des mesures d'examen et de surveillance des activités de renseignement de sécurité, et où les universitaires et d'autres membres du public intéressés en discutent.

You have asked me to appear before you to discuss my annual report that was tabled in Parliament on January 28, 2016. I will provide you with highlights from that report and the accompanying statement I issued regarding metadata and non-compliance by the CSE, and then we would be pleased to answer questions.

I have previously given you details about my mandate, so let me just recall what the National Defence Act provides me to carry out my mandate. First, full independence at arm's length from government and a separate budget granted by Parliament; second, full access to all CSE facilities, files, and systems; and, third, full access to CSE personnel, including the power of subpoena to compel individuals to answer questions, specifically under Part II of the Inquiries Act.

[*English*]

My annual report tabled at the end of January summarizes nine classified reports as submitted to the Minister of National Defence, who is the minister responsible for the Communications Security Establishment, or CSE, and this during the fiscal year 2014-15.

First, these reports included a review of the metadata activities relating to CSE's foreign signals intelligence program. I will speak to this in more detail shortly.

Second, it included a review of CSE information technology security activities conducted under ministerial authorization that included a recommendation for an amendment to the legislation to remove an ambiguity, adding to the list of amendments required.

Third, it included a review of foreign signals intelligence activities of the Canadian Armed Forces that are conducted under CSE authorities.

Fourth, it included a review of CSE assistance to the Canadian Security Intelligence Service, or CSIS, relating to foreign intelligence collection activities within Canada, at the end of which I referred information to SIRC that related to CSIS.

Finally, the annual report included three annual reviews relating to privacy: first, an annual review of foreign signals intelligence ministerial authorizations, which included two separate spot-checks of intercepted private communications; second, an annual review of disclosures of Canadian identity information; and, finally, an annual review of CSE's files of privacy incidents and procedural errors.

Vous m'avez demandé de témoigner devant votre comité pour discuter de mon rapport annuel, qui a été déposé devant le Parlement le 28 janvier dernier. Je vous présenterai des faits saillants de ce rapport et de ma déclaration connexe au sujet des métadonnées et de la non-conformité du CST. Je répondrai ensuite à vos questions avec plaisir.

Je vous ai déjà donné des détails au sujet de mon mandat lors d'une comparution précédente. Laissez-moi vous rappeler ce que la Loi sur la défense nationale me confère afin que je puisse m'acquitter de mon mandat. Premièrement, une autonomie complète sans lien de dépendance avec le gouvernement et un budget distinct accordé par le Parlement; deuxièmement, un accès sans entrave à tous les dossiers, systèmes et installations du CST; et, troisièmement, un accès sans entrave au personnel du CST et, notamment, le pouvoir d'assigner des particuliers à comparaître pour les obliger à répondre à des questions, et ce, en vertu de la partie II de la Loi sur les enquêtes.

[*Traduction*]

Mon rapport annuel déposé à la fin janvier récapitule neuf rapports classifiés que j'ai soumis au ministre de la Défense nationale, qui est responsable du Centre de la sécurité des télécommunications, pendant l'exercice 2014-2015.

Premièrement, ce rapport comprend un examen des activités relatives aux métadonnées qui sont associées au programme de renseignement électromagnétique étranger du CST. J'en parlerai plus longuement bientôt.

On y trouve aussi un examen des activités du CST en matière de sécurité des technologies de l'information qui sont réalisées en vertu d'une autorisation ministérielle. Dans cet examen, j'ai recommandé que les mesures législatives soient modifiées afin d'éliminer une ambiguïté, ajoutant à la liste de modifications législatives nécessaires.

Troisièmement, un examen des activités relatives au renseignement électromagnétique étranger des Forces armées canadiennes qui sont menées sous l'autorité du CST.

Quatrièmement, le rapport renferme un examen de l'aide apportée par le CST au Service canadien du renseignement de sécurité, SCRS, en ce qui a trait aux activités de collecte de renseignements étrangers au Canada, après lequel j'ai renvoyé un élément qui concernait le SCRS au Comité de surveillance des activités de renseignement de sécurité.

Enfin mon rapport comporte trois examens annuels relatifs à la protection de la vie privée : un examen annuel des autorisations ministérielles inhérentes au renseignement électromagnétique étranger, y compris deux vérifications ponctuelles distinctes portant sur des communications privées interceptées; un examen annuel de la divulgation des renseignements sur l'identité de Canadiens; et, enfin, un examen annuel des dossiers du CST relatifs aux incidents liés à la vie privée et les erreurs de procédure.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*Translation*]

Why do I conduct these reviews?

By law, CSE is prohibited from directing its foreign signals intelligence collection and information technology security activities at Canadians — wherever they might be in the world — or at any person in Canada.

My review of CSE activities includes determining whether CSE, in its use and retention of collected information, takes satisfactory measures to protect every Canadian's reasonable expectation of privacy. I examine CSE use, disclosure, and retention of private communications. I verify that Canadian identity information is protected and only shared with authorized partners when needed for understanding foreign signals intelligence or IT security information.

I also verify that metadata is used only to understand the global information infrastructure, to obtain foreign intelligence, or to protect cyber systems, but not to obtain information about a Canadian.

In these reports, I made eight recommendations for CSE to promote compliance with the law and strengthen privacy protection. The Minister of National Defence accepted all eight. I will monitor CSE's efforts to implement the recommendations.

With the exception of the one review related to metadata, all of CSE's activities that I reviewed in 2014-15 complied with the law. While a number of important issues were identified by the reviews, I will focus on the review of metadata and on my finding of CSE's non-compliance with the law.

[*English*]

The National Defence Act authorizes the CSE to acquire and use information from the global information infrastructure, which includes metadata, to provide intelligence on foreign entities located outside of Canada, in accordance with priorities set by the government.

Metadata is information associated with a communication that is used to identify, describe, manage or route that communication. It includes, but is not limited to, a telephone number, an email or Internet Protocol address, and network and location information. Metadata does not include the content of a telecommunication.

Metadata is fundamental to CSE's activities. It helps CSE understand the networks it is targeting and helps it avoid targeting a Canadian.

[*Français*]

Pourquoi est-ce que j'effectue ces examens?

Le CST se voit interdire par la loi, dans le cadre de ses activités de collecte de renseignements électromagnétiques, étrangers et de sécurité des technologies de l'information, ce qu'on appelle en français les TI, de cibler des Canadiens où qu'ils se trouvent dans le monde, ou toute personne au Canada.

Dans le cadre de mon examen des activités du CST, je dois notamment déterminer si ce dernier prend des mesures satisfaisantes pour respecter les attentes raisonnables des Canadiens en matière de vie privée concernant l'utilisation et la conservation des communications privées qu'il a recueillies. J'examine l'utilisation, la divulgation et la conservation des communications privées par le CST. Je vérifie que l'information concernant l'identité des Canadiens est protégée et n'est partagée qu'avec les partenaires autorisés pour comprendre les renseignements électromagnétiques étrangers ou pour assurer la protection des TI.

Je vérifie également que les métadonnées sont utilisées pour comprendre l'infrastructure mondiale d'information, pour obtenir du renseignement étranger ou pour protéger les cybersystèmes, mais non pour obtenir de l'information sur un Canadien.

Dans ces rapports, il y avait huit recommandations pour le CST afin de promouvoir la conformité aux lois et à la protection de la vie privée. Le ministre de la Défense nationale a accepté toutes ces recommandations, et je surveillerai les efforts du CST pour les mettre en œuvre.

Hormis un examen relatif aux métadonnées, toutes les activités du CST que j'ai examinées au cours de l'exercice 2014-2015 étaient conformes à la loi. Bien que de nombreuses questions importantes aient été soulevées dans ces examens, je me concentrerai surtout sur l'examen relatif aux métadonnées et ma constatation que le CST n'a pas agi en conformité avec la loi.

[*Traduction*]

La Loi sur la défense nationale autorise le CST à acquérir et à utiliser l'information provenant de l'infrastructure mondiale d'information, y compris les métadonnées, dans le but de fournir des renseignements sur les entités étrangères situées à l'extérieur du Canada, conformément aux priorités établies par le gouvernement.

Les métadonnées comprennent l'information associée à une communication qui est utilisée pour identifier, décrire, gérer ou acheminer cette communication. Elles englobent, sans pour autant s'y limiter, un numéro de téléphone, une adresse de courriel ou une adresse de protocole Internet ainsi que de l'information concernant un réseau et la géolocalisation. Les métadonnées ne comprennent pas le contenu d'une communication.

Les métadonnées jouent un rôle fondamental dans les activités du CST. Elles l'aident à comprendre les réseaux qu'il cible et à éviter de cibler des Canadiens.

Both the National Defence Act and a ministerial directive on metadata require CSE to have in place measures to protect the privacy of Canadians in the conduct of its metadata activities.

One important measure to protect privacy is what we call the minimization of any Canadian identity information contained within the metadata. Minimization is the process by which information that could identify a Canadian is rendered unidentifiable before it is shared. It is this point that became a significant focus of my review.

Following the start of the review on metadata in November 2013, CSE discovered on its own that certain metadata containing Canadian identity information was not being properly minimized prior to sharing with our Five Eyes partners. As a result, CSE shared some metadata that contained Canadian identity information with its Five Eyes partners in the United States, United Kingdom, Australia and New Zealand.

After making this discovery, CSE proactively suspended the sharing of metadata with its partners and subsequently informed me about this incident. I directed my staff to investigate the metadata minimization deficiencies.

CSE cooperated fully with my investigation. The chief of CSE assured me that the suspension will remain in effect until systems are in place to properly minimize any and all Canadian identity information in the metadata. I concluded that CSE's failure to minimize certain Canadian identity information prior to it being shared with its partners did not — and I emphasize that — comply with the National Defence Act and as a consequence did not comply with the Privacy Act.

I therefore exercised my legal duty under the National Defence Act and informed the Attorney General of Canada and the Minister of National Defence of this non-compliance with the law.

While I believe the actions of CSE were not intentional, it did not, however, act with due diligence when it failed to ensure that the Canadian identity information was properly minimized prior to sharing.

In this review of metadata, I made two recommendations to the Minister of National Defence, who accepted them. My first recommendation was that the minister issue an updated directive to CSE to provide greater specificity and clarity to CSE's collection, use and disclosure of metadata in a foreign signals intelligence context.

La Loi sur la défense nationale et une directive ministérielle sur les métadonnées exigent que le CST dispose de mesures en place pour protéger la vie privée des Canadiens dans le cadre de ses activités relatives aux métadonnées.

Une mesure importante pour protéger la vie privée est la minimisation de toute information sur l'identité canadienne que renferment les métadonnées. La minimisation est le processus en vertu duquel des renseignements susceptibles d'établir l'identité de Canadiens sont rendus non identifiables avant d'être communiqués. C'est ce sujet qui est devenu un élément important de mon examen.

Après le début de l'examen sur les métadonnées, en novembre 2013, le CST a découvert de son propre chef que certains types de métadonnées contenant de l'information sur l'identité de Canadiens n'étaient pas minimisés comme ils le devaient avant d'être communiqués à nos partenaires du groupe des cinq yeux. Par conséquent, le CST a communiqué certaines métadonnées comportant de l'information sur l'identité de Canadiens à ses partenaires du Groupe des cinq, soit les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande.

Après cette découverte, le CST a suspendu de façon proactive le partage de métadonnées avec ses partenaires et m'a avisé de l'incident. J'ai demandé à mon personnel d'enquêter sur les lacunes au chapitre de la minimisation des métadonnées.

Le CST a coopéré pleinement dans le cadre de mon enquête. La chef du CST m'a confirmé que la suspension demeurera en vigueur jusqu'à la mise en place de systèmes pour assurer la minimisation adéquate de toutes les informations sur l'identité des Canadiens que renferment les métadonnées. J'ai conclu que le CST, n'ayant pas minimisé certaines informations sur l'identité de Canadiens avant d'être communiquées aux partenaires du CST, n'a pas agi en conformité avec la Loi sur la défense nationale et, par conséquent, n'a pas agi en conformité avec la Loi sur la protection des renseignements personnels.

De ce fait, j'ai exercé l'obligation qui m'incombe en vertu de la Loi sur la défense nationale et j'ai informé le procureur général du Canada et le ministre de la Défense nationale à propos de cette non-conformité à la loi.

Bien que j'estime que les actes du CST n'étaient pas délibérés, l'organisme n'a pas fait preuve de diligence raisonnable en omettant de faire en sorte que l'information sur l'identité de Canadiens soit correctement minimisée avant d'être communiquée.

Dans cet examen des métadonnées, j'ai formulé deux recommandations, lesquelles ont été acceptées par le ministre de la Défense nationale. Premièrement, que le ministre émette une directive mise à jour à l'intention du CST donnant des lignes directrices claires et précises en ce qui concerne la collecte, l'utilisation et la divulgation de métadonnées dans le contexte de renseignements électromagnétiques étrangers.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

My second recommendation was that CSE use its existing records system to ensure decisions and actions taken are recorded regarding updated collection systems and regarding minimization of metadata involving Canadian identity information.

In my letter to the Attorney General and to the Minister of National Defence, I made an additional recommendation: that the National Defence Act be amended to provide a clear framework for CSE's metadata activities. While the National Defence Act provides authority to CSE to conduct metadata activities, an explicit authority for these activities would strengthen overall accountability.

My predecessors and I have repeatedly — and I should add, over the last 10 years or so — stated that important provisions of Part V.1 of the National Defence Act are ambiguous and need to be amended. The last recommendation I made regarding metadata adds to the list of amendments. I sincerely hope that the government will seize the opportunity to act on these long overdue amendments as part of its stated objective of strengthening accountability of intelligence activities by government agencies and departments.

My decision to inform the Attorney General and the minister was a duty under the law and it had the consequence of prompting the minister to issue a statement about the matter, and CSE to take the unprecedented step of holding a briefing for the media. I encourage CSE to continue to provide as much information as possible.

As I stated on the occasion of my last appearance before this committee, I think that transparency is important for CSE if it wants to maintain public trust.

My office has challenged CSE to justify why certain information needs to be considered classified. Indeed, last year, I included statistics related to unintentionally intercepted private communications collected through CSE's foreign signals intelligence activities; this year's report contains more statistics. I see these as important steps in helping to demystify the work of CSE and contributing to better-informed public discussion.

[*Translation*]

My final remarks will touch briefly on some general points that relate to current discussions about intelligence review.

I support ongoing efforts to increase the accountability of security and intelligence activities within government agencies and departments. I welcome the fact that there is more and more

Deuxièmement, que le CST utilise son registre centralisé actuel pour consigner les décisions et les mesures prises concernant les systèmes de collecte mis à jour ainsi que les décisions et les mesures prises concernant la minimisation des métadonnées renfermant de l'information sur l'identité de Canadiens.

Dans la lettre que j'ai écrite au procureur général et au ministre de la Défense nationale, j'ai formulé une recommandation additionnelle, à savoir qu'il faudrait modifier la Loi sur la Défense nationale de façon à définir un cadre précis pour les activités du CST liées aux métadonnées. Bien que la Loi sur la Défense nationale permette déjà au CST d'entreprendre des activités reliées aux métadonnées, un pouvoir explicite renforcerait la reddition de comptes à ce sujet.

Mes prédécesseurs et moi-même avons déclaré maintes fois — depuis au moins 10 ans — que d'importantes dispositions de la Partie V.1 de la Loi sur la défense nationale sont ambiguës et nécessitent des modifications. La dernière recommandation que j'ai faite concernant les métadonnées s'ajoute à cette liste de modifications. Je souhaite sincèrement que le gouvernement profite de l'occasion qui lui est donnée pour prendre les mesures requises et procéder à ces modifications qui auraient dû être apportées depuis longtemps. Ces mesures s'inscriraient bien dans le cadre de son objectif annoncé de renforcer la reddition de comptes concernant les activités du renseignement menées par les agences et les ministères fédéraux.

Ma décision d'informer le procureur général et le ministre était une obligation en vertu de la loi. Elle a eu pour conséquence de convaincre le ministre de la Défense nationale de diffuser une déclaration sur la question et d'inciter le CST à faire une démarche sans précédent, soit de tenir une séance d'information devant les médias. J'encourage le CST à continuer de fournir le plus d'information possible.

Comme je l'ai indiqué lors de mon dernier passage devant ce comité, je pense que le CST doit faire preuve de transparence s'il veut conserver la confiance du public.

Mon bureau a demandé au CST de justifier pourquoi certains renseignements doivent être considérés comme classifiés. À vrai dire, j'ai inclus l'an dernier des statistiques se rapportant à des communications privées interceptées de façon non intentionnelle et recueillies dans le cadre des activités de collecte de renseignements électromagnétiques étrangers du CST. Le rapport de cette année renferme encore davantage de statistiques. Je vois ces initiatives comme des mesures importantes pour contribuer à démystifier le travail du CST et mieux éclairer le débat public.

[*Français*]

En concluant ces remarques, j'aimerais aborder brièvement certains points généraux qui touchent les discussions actuelles au sujet de l'examen du renseignement.

Je suis en faveur des efforts en vigueur à l'heure actuelle visant à accroître la reddition de comptes relative aux activités de sécurité et du renseignement qui sont menées par les agences et les

interest in the work of my office, which was not the case for my predecessors. I also welcome the opportunity to engage more closely with parliamentarians.

The work of my office forms an integral part of Canada's system of expert, independent review. I believe that expert review is effective, that is, that a single review body focusses on one intelligence agency. This allows for depth of review and investigation and for the accumulation of in-depth knowledge about the intelligence agency by those conducting the review.

This is not to say that there are no gaps. The intelligence functions of certain government departments and agencies are not currently subject to independent, external review. I believe that efforts to enhance intelligence review should build on the strengths of the existing system. Expert review could, for example, help inform a committee of parliamentarians or of Parliament that is cleared to receive classified information.

I also believe it would be preferable to have an explicit authority for co-operation among review bodies — SIRC and CSE, for example — in support of joint reviews of integrated operations by security and intelligence agencies. I have noted, as did my predecessor, that much can be done under the existing laws.

Pierre Blais, who is sitting to my right, and I have discussed ways to enhance co-operation of our two agencies. For example, we can refer to each other questions or basic information regarding a matter that involves the agency under the other's mandate. My office and SIRC have consulted each other on a review of activities in a sector involving co-operation between CSE and CSIS. My officials completed our review and briefed SIRC officials on the conclusions that concerned CSIS, to inform SIRC's review.

Last of all, I would like to reiterate the offer made in my letter to you last April to provide an information session to the committee about the work of my office, how I select activities to review, how I conduct my reviews and the expertise in my office.

Thank you for this opportunity to appear again before you today. My executive director, Mr. Galbraith, and I would be pleased to answer your questions.

[*English*]

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

ministères du gouvernement. Je vois d'un œil positif l'intérêt de plus en plus grand à l'égard du travail accompli par mon bureau, ce qui n'était pas le cas du temps de mes prédécesseurs, et je suis tout à fait disposé à m'engager plus étroitement avec les parlementaires.

Le travail accompli par mon bureau fait partie intégrante du système canadien d'examen indépendant et spécialisé. Je suis d'avis que l'examen mené par des spécialistes est efficace, c'est-à-dire qu'un seul organisme d'examen axe ses efforts sur une agence de renseignement. Cela permet que les examens et les enquêtes se fassent en profondeur et donnent aux enquêteurs des connaissances poussées sur l'agence du renseignement visée.

Je suis conscient, d'autre part, que des lacunes subsistent. Les fonctions du renseignement de certains ministères ou de certaines agences ne font pas, à l'heure actuelle, l'objet d'examens externes indépendants. Je crois que les efforts menés pour améliorer la fonction d'examen des activités du renseignement devraient se fonder sur les points forts du système actuel. L'examen spécialisé pourrait, par exemple, aider à transmettre de l'information à un comité de parlementaires ou du Parlement, dont les membres posséderaient le niveau de sécurité nécessaire pour prendre connaissance de l'information classifiée.

Je crois qu'il serait également préférable de disposer d'un pouvoir explicite afin que les agences d'examen — le CSARS et nous, par exemple —, puissent coopérer en faisant des examens ensemble sur les opérations intégrées des agences de sécurité et du renseignement. J'ai remarqué, tout comme l'a fait mon prédécesseur, que beaucoup de choses peuvent être réalisées en vertu des lois existantes.

Mon voisin de droite, l'honorable Pierre Blais, et moi avons discuté de façons d'améliorer la coopération entre nos deux organismes. Par exemple, nous pouvons nous transmettre des questions ou de l'information de base dans le cadre d'une affaire qui implique les agences sous l'égide du mandat de l'autre. Mon bureau et le CSARS se sont consultés sur l'examen des activités menées dans un secteur mettant en jeu la coopération entre le CST et le SCRS. Mes fonctionnaires ont complété l'examen et ont informé les fonctionnaires du CSARS quant aux conclusions qui concernaient le SCRS, et ceci afin d'éclairer l'examen du CSARS.

En terminant, je voudrais réitérer l'offre d'avril dernier, contenue dans la lettre que je vous avais adressée, d'offrir une séance d'information au comité. Lors de cette séance, je pourrais expliquer le travail effectué par notre bureau, expliquer comment je sélectionne les activités qui font l'objet d'un examen et comment j'effectue ces examens. Je pourrais aussi parler de l'expertise dont nous disposons à nos bureaux.

Je vous remercie de m'avoir donné, encore une fois, l'occasion de vous adresser la parole aujourd'hui. Le directeur exécutif, M. Galbraith, ainsi que moi-même serons heureux de répondre à vos questions.

[*Traduction*]

Le vice-président : Merci beaucoup, monsieur Plouffe.

Colleagues, we have 20 minutes left, but these were both long presentations and very worthwhile. I would propose that we go for half an hour on questions. If that's agreeable, we'll start right away with the questions.

Mr. Plouffe, we made note of your offer, and we had not forgotten. We had an election intervene that might have delayed some of us taking up the offers, but we do appreciate that very much and haven't forgotten it.

I will begin with Senator Kenny, former chair of this committee and senator from Ontario.

Senator Kenny: I'm going to focus my questions, at least in the first round, on SIRC.

I'm concerned about your capacity, Mr. Blais, not individually but as an organization. I start with the understanding that your review is of CSIS, which has relations with 265 foreign agencies in 144 countries. It manages 2,500 employees in 14 regional offices and has a number of offices overseas or individuals overseas and an annual budget in excess of $500 million. In contrast, you have an executive director, a staff of 17, at my last count, five part-time committee members, when all the positions are filled, which hasn't been the case for a number of years, and you only met nine times in 2013-14.

Perhaps you could start by telling us how often you met last year and how you managed to deal with an agency the size of SIRC. You refer to yourself, or the agency has referred to itself, as a micro-agency and said that there are many inherent risks of being a micro-agency. Perhaps if you could comment on those risks, that would be very helpful.

I ask you this all in the context of the reality that SIRC does not review the intelligence agency for effectiveness or value for money. You simply review them to see if they're in conformity with the legislation. I'd like to know your views on whether your organization should be looking at effectiveness and value for money.

Mr. Blais: Well, on the number of meetings we have, usually we meet every two months and we receive reports from our staff. Our staff is very dedicated and spends most of its time on the CSIS site, working with them.

I would say that we will move shortly to new premises here in Ottawa, and we will probably be electronically linked to CSIS, which will be helpful for our staff to have better access to the whole of the information driven by CSIS.

The first point that you should remember, one you didn't mention but that is probably a very important one, is that, around the world, only SIRC has access to everything in CSIS. You will not find any other country — well, maybe some other countries where there is no real democratic government — where an

Chers collègues, il nous reste 20 minutes après ces deux exposés plutôt longs, mais très intéressants. Je propose que nous posions des questions pendant une demi-heure, et si cela vous convient, nous commencerons tout de suite.

Monsieur Plouffe, nous avions pris note de votre offre et nous ne l'avons pas oubliée. À cause des élections survenues après votre dernier passage ici, certains d'entre nous n'ont peut-être pas pu se prévaloir de votre offre, mais nous l'avons beaucoup appréciée et ne l'avons pas oubliée.

Je commencerai par le sénateur Kenny, ancien président du comité et sénateur de l'Ontario.

Le sénateur Kenny : Je vais poser l'essentiel des questions de cette première série sur le SCRS.

Je m'inquiète de votre capacité, monsieur Blais, non pas la vôtre à titre personnel, mais celle de votre organisation. Si je comprends bien, votre examen a concerné le SCRS qui entretient des relations avec 265 agences étrangères réparties dans 144 pays. Le SCRS gère 2 500 employés répartis dans 14 bureaux régionaux et un certain nombre de bureaux ou de particuliers à l'étranger, tout cela avec un budget annuel dépassant les 500 millions de dollars. En revanche, vous disposez d'un directeur général, d'un personnel de 17 employés, d'après mon dernier décompte, de cinq membres du comité à temps partiel, quand tous les postes sont comblés, ce qui n'est pas le cas depuis plusieurs années et vous vous êtes rencontrés neuf fois seulement en 2013-2014.

Vous pourriez peut-être commencer par me dire à combien de reprises vous vous êtes rencontrés l'année dernière et comment vous faites compte tenu de la petite taille de cet organisme qu'est le CSARS. Vous vous êtes vous-même, à moins que ce ne soit l'organisme qui l'ait fait, décrit comme une micro-agence, précisant que cette petite taille entraîne certains risques. Vous pourriez commencer par nous expliquer ce que sont ces risques.

Je vous pose évidemment ces questions en étant conscient que le CSARS n'examine ni l'efficacité ni le rendement du SCRS. Vous vous cantonnez à déterminer si le SCRS se conforme à la loi. Selon vous, est-ce que votre organisation devrait également examiner les dimensions efficacité et rentabilité?

M. Blais : Pour ce qui est de la fréquence de nos réunions, nous nous rencontrons ordinairement aux deux mois et nous recevons des rapports de notre personnel, qui est très dévoué et qui passe la plus grande partie de son temps dans les locaux du SCRS, travaillant avec ses gens.

Je mentionne que nous aménagerons prochainement dans des nouveaux locaux, ici à Ottawa, et que nous serons sans doute liés électroniquement avec le SCRS, ce qui facilitera l'accès de notre personnel à l'ensemble de l'information concernant le SCRS.

Le premier point qu'il faut garder présent à l'esprit, que vous n'avez pas mentionné, mais qui est probablement très important, c'est que le CSARS a accès à tout ce qui se trouve au SCRS, situation propre au Canada. Il n'y a pas d'autres pays — sauf peut-être quelques pays sans réelle démocratie — où l'organe de

oversight body has access to everything. Our people could enter there I wouldn't say any time, but they could have access to everything. You will not find that anywhere else in the world, even with our allies. We have access to that, and we do use it.

We cannot look into the work of each and every employee of CSIS. It's not possible. You can understand that. I don't think that's the objective. The objective is to conduct a review of what they're doing.

We are going to have a meeting in a couple of weeks where we will receive the reports prepared by our employees on what they were doing that we provided a year before. We're working on the plan for next year; that will start in a month or so.

We have to prepare what we are going to look for next year. At every meeting, we're looking at reports about what they found and whether there is something wrong or something that has to be addressed.

It will not be possible. What you're asking for, if I understand your question, is the basics of reviewing everything, every day, of every employee around the world. It's impossible.

What is possible and what we should address is to put our energy into identifying where to look at, which we have done over the last year, and just review and get CSIS's direction. A month ago or so we met with the executive board of CSIS. We discussed many issues. We discussed those recommendations, even though, when they say, "We go with your recommendations, or we decide not to go with them," it's okay. We cannot force them, but we'll put that in our report. You could have access to it. The public has.

At the end of the day, we report to you, to Parliament and to the minister. We did that twice last year, directly pursuant to section 54.

We could probably do more with more means, more money, but what we try to do is to use our money. It will be up to you probably; you're involved somehow with this situation, when decisions are made by the government to provide more money. We were allowed more money in the last budget. Unfortunately, with the electoral period and all of that, we were not in the front-line of priorities, and we got access to the money just at the end of January. We were close to cancelling a meeting just because of the access to the money. It's important to have some money.

We're part time, as you mentioned. I will speak for myself, but if you look at the resumé, the people who were appointed to our committee I think have great experience, are very good and are dedicated. They are spending time not only on the meetings we have every two months to review the report by our employees, but we also act as a tribunal, as you know. We have hearings for complaints. We didn't address that in our report today, but you

surveillance a accès à tout. Nos gens peuvent se rendre au SCRS, je ne dirais pas à tout moment, mais ils auraient accès à tout. Une telle situation ne se trouve nulle part ailleurs au monde, même chez nos alliés. Nous avons un accès illimité et nous en usons.

Nous ne pouvons nous pencher sur le travail de chacun des employés du SCRS. Cela n'est pas possible, vous le comprendrez. Je ne crois pas, d'ailleurs, que c'est l'objectif visé. Notre objectif est de mener un examen des activités du SCRS.

Nous aurons une réunion dans quelques semaines afin de recevoir les rapports de nos employés sur ce qu'ils ont fait pour donner suite à ce que nous avions recommandé l'année précédente. Nous sommes en train de préparer le plan pour la prochaine année, qui débutera dans environ un mois.

Nous devons prévoir ce que nous allons examiner l'année prochaine. À chacune de nos réunions, nous nous penchons sur des rapports décrivant ce qu'ils ont trouvé et relevant s'il y a quelque chose qui fonctionne mal ou qui doit être réglé.

Il ne serait pas possible, si j'ai bien compris votre question, de faire ce que vous suggérez, de vérifier tout ce qui se fait, chaque jour, par chaque employé, partout au monde. C'est impossible.

Ce qui est possible et ce que nous devons faire, c'est de bien cibler les questions à examiner, ce que nous avons fait au cours de la dernière année, d'en faire l'examen et de saisir l'orientation du SCRS. Il y a un mois environ, nous avons rencontré le conseil d'administration du SCRS. Nous avons discuté de nombreux problèmes. Nous avons discuté de ces recommandations, même si, qu'ils soient en accord ou en désaccord avec nos recommandations, nous acceptons la situation. Nous ne pouvons pas les forcer, mais nous l'indiquerons dans notre rapport. Vous y avez accès, et le public également.

En fin de compte, c'est à vous, au Parlement et au ministre que nous faisons rapport. Nous l'avons fait deux fois l'an dernier, conformément à l'article 54.

Nous pourrions probablement faire davantage si nous avions plus de moyens, plus d'argent, mais ce que nous tentons de faire, c'est d'utiliser l'argent qui nous est accordé. Ce sera à vous probablement, puisque vous êtes mêlés de quelque façon à cette situation, lorsque les décisions seront prises par le gouvernement, d'accorder plus d'argent. Nous avons bénéficié d'une augmentation dans le dernier budget. Malheureusement, avec la campagne électorale et tout ce qui l'entourait, nous n'étions pas en première ligne des priorités, et ce n'est qu'en janvier que les ressources financières voulues nous ont été accordées. Nous sommes passés près d'annuler une réunion pour cette raison. Il est important d'avoir des moyens financiers suffisants.

Comme vous l'avez mentionné, nous travaillons à temps partiel. Je parlerai pour moi-même, mais si vous regardez les curriculum vitae, vous verrez que les personnes qui siègent au comité ont, je crois, une solide expérience, et elles sont très compétentes et dévouées. Elles donnent de leur temps non seulement pour assister aux réunions bimestrielles afin d'étudier le rapport de nos employés, mais également pour siéger en tant

have it in our report. We work very hard on that. Our people are meeting as a judge, in a sense, hearing cases and rendering decisions. It's another part of our job.

In a nutshell, we cannot say that we're useless. We're very useful, I think, for the government. We could be more. The more we are asked to come here to help, providing reports, providing information, we will do that.

I could come back here next week, if necessary, but I don't think the number of meetings or the number of individuals will decide the work we do and the return for money spent. As you mentioned, senator, although I don't remember the words, we cannot appreciate if we get enough in return for the money we spend. For the committee, at least for the millions we spend, you get a good return for your money. As far as I'm concerned, we provide a report that makes sense.

The Deputy Chair: Mr. Blais, unfortunately we could spend all day talking just about your group and your organization. We had hoped that this meeting with the two of you here would be focused on the two reports that came out on January 28. It may turn out that we'll have to have you back to talk in more detail about your organization.

We will now move on to Senator White from Ontario.

Senator White: Mr. Blais, high-risk activities are things that I expect you're looking at, such as search warrants. I think I read that 104 federal court orders or warrants were issued. Did you also review the warrants that were refused by the courts to see if those errors were of concern? If so, what concerns did you identify?

Mr. Blais: As far as I'm concerned, our people have access to all of those warrants. As you know, in another life I was part of that, so I know very well this strict process. We also have dedicated judges addressing those warrants, which is very important.

We have access to all of them. Sometimes if a warrant is asked for and refused, which does not happen often, CSIS is allowed to come back. There is no jurisprudence against that. Before going to a judge, as you know, the minister has to approve the warrant. It has to go through the process. When the judge has the application for a warrant, he has access to the persons who sign the affidavits. I have to be careful with the details as I don't want to cross the line of confidentiality, but I want to be sure. The judge should be satisfied that the warrant is really needed, that what they're asking for in the warrant is really needed, and that the evidence is provided. If he is satisfied, he will sign the warrant. If he is not satisfied, he will just refuse. It could go back and forth if there is a problem with the details of the request.

que tribunal, comme vous le savez. Nous tenons des audiences relatives aux plaintes. Nous n'avons pas abordé ce sujet dans notre exposé aujourd'hui, mais c'est dans notre rapport. Nous consacrons beaucoup d'énergie à cette fonction. Nos gens constituent, pour ainsi dire, un tribunal, entendent les plaintes et rendent des décisions. C'est une partie de notre travail.

En deux mots, nous ne pouvons pas dire que nous sommes inutiles. Je pense que nous sommes très utiles au gouvernement. Nous pourrions en faire davantage. Si nous devions être convoqués plus souvent ici pour aider, présenter des rapports, produire de l'information, nous y serions sans faute.

Je pourrais revenir ici la semaine prochaine s'il le faut, mais je ne pense pas que c'est le nombre de réunions ou de personnes qui décidera du travail que nous accomplissons ou du rendement de l'argent investi. Comme vous le disiez, monsieur le sénateur, bien que je ne me souvienne pas exactement des termes que vous avez employés, nous ne pouvons pas déterminer si le rendement des sommes allouées est suffisant. Pour le comité, à tout le moins en ce qui concerne les millions dépensés, le rendement est bon. À mes yeux, nous produisons un rapport qui se tient.

Le vice-président : Monsieur Blais, malheureusement, nous pourrions passer la journée entière à discuter de votre groupe et de votre organisme. Nous espérions que cette rencontre avec vous deux porterait essentiellement sur les deux rapports parus le 28 janvier. Il se pourrait que nous ayons à vous convoquer de nouveau pour discuter de votre organisme de façon plus détaillée.

Je cède maintenant la parole au sénateur White, de l'Ontario.

Le sénateur White : Monsieur Blais, les activités à haut risque sont celles, je suppose, que vous examinez, les mandats de perquisition, par exemple. Je pense avoir lu que 104 ordonnances ou mandats ont été délivrés par la Cour fédérale. Avez-vous également étudié les mandats qui ont été refusés pour vérifier si les erreurs soulevaient des préoccupations? Si oui, quelles préoccupations avez-vous relevées?

M. Blais : Pour ma part, je sais que nos gens ont accès à tous ces mandats. Comme vous le savez, je faisais jadis partie de cet appareil et je connais donc très bien la rigueur de ce processus. Nous avons également des juges spécialisés qui s'occupent de ces mandats, ce qui est très important.

Nous avons accès à tous les mandats. Parfois, si un mandat demandé est refusé, ce qui n'arrive pas souvent, le SCRS peut rappliquer. Rien dans la jurisprudence ne l'empêche. Comme vous le savez, avant qu'une demande de mandat soit présentée au juge, elle doit être approuvée par le ministre. Elle doit passer par le crible du processus. Le juge qui reçoit une demande de mandat a accès aux personnes qui ont signé les affidavits. Il faut porter attention aux détails pour s'assurer de ne pas manquer à la confidentialité, mais il faut néanmoins être certain de son coup. Il faut convaincre le juge que ce qui est demandé dans le mandat est vraiment nécessaire et que des éléments probants lui sont fournis. S'il est convaincu, il signera le mandat. Sinon, il refusera simplement de le signer. Il est possible de revenir à la charge si les détails de la demande posent problème.

I'm sorry, Mr. Chair, I have to be careful with the technical details. I don't think I can enter into too many details.

The Deputy Chair: You don't want to breach confidentiality.

Mr. Blais: We're in public, so I have to be careful with that.

I can assure you that we have access to all of that, if that's your question. I wouldn't say that many are refused because it is possible to refine the material.

[*Translation*]

Senator Dagenais: I would like to thank our witnesses. Mr. Plouffe, you mentioned that an intelligence officer obtained taxpayer information from the Canada Revenue Agency. I believe the information was obtained without a Federal Court warrant at that time. Do we know the scope of the problem? I understand that action was taken and that this did not happen again. I think the question should be for Mr. Blais instead.

Mr. Blais: Your question is very important, and you will understand why. Our executive director asked for a review of this issue, which was diligently carried out by our staff. We found that the problem was more widespread than it seemed to be at first glance. There was not just one offence, but many. That forced us to broaden our recommendations.

An important point, and I believe this is the right time to talk about it, is that we review the secret services, but we do not have access to the CRA. We cannot review it. My colleague, Mr. Plouffe, spoke about this earlier. We communicate with one another on the issue, and we can exchange a certain amount of information. However, in the case of the CRA, neither I nor CSIS have that ability. We were limited in our ability to examine the details of this issue.

I can tell you that we were very concerned, as were you, senator. It is unsettling to know that our tax records can be examined without justification. The issue raised was extremely serious. Unfortunately this underscores the need for a review of the CRA's activities — I have reason to believe that the government is considering this — because it has become quite involved in intelligence activities in recent years as a result of its role at the border and in the area of security.

Unfortunately, neither my colleague nor I can review the activities of another agency. We mentioned in our report that we had limitations, but we did nevertheless include some provisions. I believe that the service took this seriously. We cannot guarantee

Je regrette, monsieur le président, mais je dois me montrer circonspect quant aux détails techniques. Je ne pense pas pouvoir donner beaucoup de renseignements détaillés.

Le vice-président : Vous n'avez pas à manquer à votre devoir de confidentialité.

M. Blais : Nous sommes en public et je dois donc faire attention.

Je peux vous assurer que nous avons accès à tous ces documents, si telle est le sens de votre question. Je ne dirais pas que beaucoup de mandats sont refusés parce qu'il est possible d'apporter des précisions quand il y a problème.

[*Français*]

Le sénateur Dagenais : Merci à nos témoins. Monsieur Plouffe, vous avez mentionné qu'il y avait un agent du renseignement du service qui avait obtenu de l'information sur les contribuables concernant l'Agence du revenu du Canada. Je pense qu'il l'avait obtenue sans mandat de la Cour fédérale à ce moment-là. Est-ce qu'on connaît l'étendue du problème? Je comprends que des mesures ont été prises et que l'incident ne s'est pas répété. Je pense que la question s'adresse plutôt à M. Blais.

M. Blais : Votre question est très importante, vous allez comprendre pourquoi. On nous a demandé de revoir cette question, ce qu'ont fait diligemment nos gens, et c'était à la demande du directeur. Nous avons trouvé que le problème était plus étendu qu'il ne le paraissait à première vue. Il ne s'agissait pas seulement d'une infraction, mais de plusieurs. Cela nous a obligés à élargir nos recommandations.

Un point important, et je pense que c'est le bon moment pour en parler, c'est que nous examinons les services secrets, mais que nous n'avons pas accès à l'ARC; nous ne pouvons pas l'examiner. Mon collègue, M. Plouffe, en a parlé plus tôt, nous communiquons entre nous sur la question, nous pouvons échanger un certain nombre de renseignements, mais dans cas de l'ARC, je n'en ai pas la capacité, et le SCRS non plus. Nous étions donc limités dans notre capacité d'examiner les détails de cette question.

Je peux vous dire que nous étions très préoccupés, comme vous l'êtes, sénateur. Il n'est pas drôle de savoir que nos comptes d'impôts peuvent être examinés sans raison. Il s'agissait d'une question extrêmement sérieuse qui a été soulevée. Malheureusement, cela souligne la nécessité — je pense, sans vouloir parler à travers mon chapeau, que le gouvernement est en train d'en examiner la possibilité — de mener un examen quelconque des activités de l'ARC, car celle-ci a pris beaucoup de place dans le domaine du renseignement au cours des dernières années, en raison du rôle qu'elle joue à la frontière et en matière de sécurité.

Malheureusement, ni mon collègue ni moi ne pouvons vérifier les activités d'une autre agence. Nous avons d'ailleurs mentionné dans notre rapport que nous étions limités, mais nous avons tout de même pris des dispositions. Je crois que le service a pris cela

that the problem will not occur again, but I can tell you that if it does there will a number of us who will stay on it. That was unacceptable.

Senator Dagenais: That situation is similar to the one police find themselves in. Their powers are sometimes limited as well, but we will talk about that another time.

Mr. Plouffe, with respect to the Security of Canada Information Sharing Act, under the famous Bill C-51, could CSIS obtain information from the CRA without a warrant if it said there was a national security issue?

Mr. Plouffe: I believe that is a question for Mr. Blais as it falls outside my mandate. It is not that I do not wish to answer.

Mr. Blais: You were wondering whether the services could obtain a warrant?

Senator Dagenais: Yes, under the famous Bill C-51, could the service decide that with the security of Canada legislation it could seek information without a warrant? Could it do that?

Mr. Blais: I want to be sure that I remain on the right path. We had to examine the fact that documents were consulted without a warrant. We did not examine a warrant because there were none. I believe that if a proper request is made, a warrant could be granted. That is a question that could be examined in another context because you are asking a hypothetical question. However, in this case, what happened was that the service realized that some of its employees obtained information without a warrant. We were not asked if there could be a warrant. It was more about the fact that the damage had been done.

You will have the opportunity to meet the directors of the services and you can ask them the question. However, at first glance, I believe that it is legitimate if it can be justified.

Mr. Plouffe: I can add one thing, if I may. At this point, it is difficult for us to determine the implications that Bill C-51 could have for the CSE. You must understand that the CSE works with CSIS only when it is providing assistance. That is Part C of our mandate. It will be in day-to-day situations that we will see the extent to which CSE will participate.

Senator Carignan: Mr. Plouffe, I have a fairly specific question. You found that the CSE did not adequately minimize Canadian identity information in the metadata. That is something that came out of your report.

Can you tell us why the public was not informed of this situation until 2016? In your estimation, how many Canadians were affected by this error?

très à cœur. On ne peut pas garantir que le problème ne se reproduira pas, mais je peux vous dire que s'il se reproduit, nous serons plusieurs à taper sur le clou. C'est inacceptable.

Le sénateur Dagenais : C'est une situation semblable à celle de la police, dont les pouvoirs sont parfois limités également, mais nous en reparlerons une autre fois.

Monsieur Plouffe, en ce qui concerne la Loi sur la communication d'information ayant trait à la sécurité du Canada, dans le cadre du fameux projet de loi C-51, est-ce que le SCRS pourrait obtenir des renseignements auprès de l'ARC sans mandat, s'il évoquait la sécurité nationale?

M. Plouffe : Je pense que la question s'adresse encore à M. Blais. C'est un sujet qui est hors de mon mandat, en fait. Ce n'est pas que je ne veuille pas répondre.

M. Blais : Vous demandez si les services pourraient avoir un mandat?

Le sénateur Dagenais : Oui, dans le cadre du fameux projet de loi C-51, est-ce que le service pourrait décider que, grâce à une loi sur la sécurité du Canada, il pourrait aller chercher des renseignements sans mandat? Est-ce qu'il pourrait le faire?

M. Blais : Je veux être sûr que je ne sors pas du droit chemin, mais nous avons eu à examiner le fait que des documents ont été consultés sans mandat. Nous n'avons pas examiné de mandat, parce qu'il n'y en avait pas dans ce cas-là. Je pense que si des mandats sont proprement demandés, à première vue, ils pourraient être accordés. C'est une question qui pourrait être examinée dans un autre cadre, parce que c'est une question hypothétique que vous posez. Cependant, dans le cas présent, ce qui s'est passé, c'est que le service s'est rendu compte que des gens parmi ses employés ont obtenu une information sans obtenir de mandat. On ne nous a pas demandé s'il pouvait y avoir un mandat; la question était plutôt que le mal était fait.

Vous aurez l'occasion de rencontrer les directions du service, et vous pourrez leur poser la question, mais, à première vue, je crois que c'est tout à fait légitime si on le justifie.

M. Plouffe : Je peux ajouter une chose, avec votre permission. En ce qui a trait au CST, il est difficile pour nous, à ce stade-ci, de déterminer l'implication que la loi C-51 pourrait avoir sur le CST. Il faut comprendre que le CST collabore avec le SCRS uniquement lorsqu'il lui vient en aide. Il s'agit du mandat C. Alors, c'est dans la pratique que nous pourrons constater, chez nous, jusqu'à quel point le CST y participera.

Le sénateur Carignan : Monsieur Plouffe, j'ai une question assez précise. Vous avez noté que le CST n'a pas minimisé de manière adéquate l'information sur l'identité des Canadiens dans les métadonnées. C'est une partie qui sort de votre rapport.

Pouvez-vous nous expliquer pourquoi le public a été informé de cette situation seulement en 2016? D'après ce que vous avez noté, combien de Canadiens ont été touchés par cette erreur?

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Mr. Plouffe: If I were to be succinct, I would say that you should put the question to the CSE. Nevertheless, I will try to answer your question.

Senator Carignan: Yes, what were your findings, your observations?

Mr. Plouffe: We found that our office has studied or investigated metadata issues since 2006. When we were notified in early 2014, it was part of this ongoing review that we were doing of metadata.

It should be understood that when an intelligence agency knows that the oversight agency is going to conduct an investigation, it is going to go looking around and, at some point . . . In this case I don't know if it was by chance or the result of our investigation, but, in any event, it was the CSE that informed us voluntarily.

Senator Carignan: The review was the reason to some extent.

Mr. Plouffe: I presume that it was a factor. I cannot prove it.

Senator Carignan: What about the number of Canadians?

Mr. Plouffe: It is very difficult to determine how many Canadians were affected. Once again, that is a question for the CSE. To the best of my knowledge — the Minister of Defence also issued a statement in that regard — because of the number of years over which this happened and the fact that the issue is related to the machine systems, it is very difficult to determine the volume and the amount of information — this is known as Canadian Identity Information — that could concern Canadians.

Senator Carignan: Are we talking about hundreds of thousands?

Mr. Plouffe: It is impossible to determine. I have to say that, after a certain period of time, the data disappears from the CSE system. If people want to investigate after the fact, it is very difficult because the data has already been erased. There is a time limit, and after that the data is erased from the system. In light of the volume, if you intercept millions of metadata pieces over the course of a year, the machine can store a certain amount, but after a certain period the data is automatically erased.

Senator Carignan: My next question is for Mr. Blais and concerns insider threats at CSIS.

CSIS has an internal security group that does the work. What are the responsibilities of this internal security group? Why did you recommend to that an outside group investigate insider threats? Can you explain the reasons for this recommendation? What was CSIS's response?

Mr. Blais: I believe that CSIS did not accept it. This will not happen because it rejected the recommendation.

M. Plouffe : Si j'étais lapidaire, je dirais que vous devriez adresser votre question au CST, mais je tenterai tout de même de répondre à votre question.

Le sénateur Carignan : Oui, ce que vous avez noté, votre constat.

M. Plouffe : Nous avons noté que, depuis 2006, notre bureau fait des examens ou des enquêtes sur la question des métadonnées. Lorsque nous avons été avertis, au début de 2014, cela faisait partie de cet examen continu que nous faisons sur les métadonnées.

Il faut comprendre que, lorsqu'une agence de renseignement sait que le surveillant procède à une enquête, elle va gratter un peu partout et, à un moment donné... dans ce cas-ci, je ne sais pas s'il s'agissait d'un hasard ou si c'était à la suite de notre enquête, mais de toute façon, c'est le CST qui, de lui-même, volontairement, nous a informés.

Le sénateur Carignan : L'examen l'a incité un peu.

M. Plouffe : Je présume que cela a eu un impact. Je ne peux pas le prouver.

Le sénateur Carignan : Et quant au nombre de Canadiens?

M. Plouffe : Il est très difficile de déterminer le nombre de Canadiens actuellement. Encore une fois, c'est une question pour le CST. Selon ce que j'en sais, et le ministre de la Défense a également émis une déclaration à cet égard, c'est que, étant donné le nombre d'années pendant lesquelles cela s'est passé, et que c'est une question lié au système des machines, il est très difficile d'établir le volume et le nombre — ce qu'on appelle en anglais le CII (*Canadian Identity Information*) — de renseignements qui pourraient concerner des Canadiens.

Le sénateur Carignan : Parle-t-on de centaines de milliers?

M. Plouffe : Il est impossible de déterminer quoi que ce soit. Il faut dire qu'après un certain temps, dans le système du CST, ces données disparaissent. Si, après coup, on veut faire une enquête à ce sujet, c'est très difficile, parce que les données sont déjà effacées. Elles ont un délai limite et, après, elles sont effacées du système. Compte tenu du volume, si vous interceptez des millions de métadonnées au cours d'une année, la machine peut en prendre un certain nombre de millions, mais après un certain temps, les données sont automatiquement effacées.

Le sénateur Carignan : Ma prochaine question s'adresse à M. Blais et concerne les menaces internes au SCRS.

Il y a un groupe de sécurité interne au SCRS qui fait le travail. Quelles sont les fonctions de ce service de sécurité interne? Pourquoi recommander de faire appel à un groupe externe pour faire l'enquête sur les menaces internes? Pouvez-vous nous expliquer la justification de cette recommandation? Comment a-t-elle été accueillie par le SCRS?

M. Blais : Je pense que le SCRS ne l'a pas accueillie. La question ne se posera pas pour lui, parce qu'il a rejeté cette recommandation.

Senator Carignan: Why?

The Deputy Chair: The government rejected it?

Senator Carignan: No, I believe it was CSIS.

Mr. Blais: It was CSIS that rejected this recommendation.

Senator Carignan: Why?

Mr. Blais: I do not remember the exact reason it gave. It looked at confidentiality and did not want this to be shared with people from outside.

I have to say that this may be the easy answer. We understand our role, we make recommendations, we believe they may be good recommendations. However, they can be rejected. In some cases, we balk and insist because we believe that the recommendation should at least be considered. In this case, it was set aside.

I have to say that everyone is aware of the insider threat and the risk it represents. Our recommendations came out of the work done by our employees and highlighted the fact that it would have been advisable, perhaps more transparent, to entrust the review to an outside group. That was rejected. We are not going to flog this to death. We will move on to something else and see what happens.

A little earlier in our report we mentioned that this became an important element. We noted the harm caused to people. I am not going to comment on the actions of Edward Snowden or other individuals, which had elements of sensationalism. Fundamentally, people's lives are at stake when internal information is disclosed. It poses a threat to Canada, the people and the sources. People's lives are in danger. We are still somewhat concerned, and I believe that you are just as concerned as we are.

National security is a serious issue. Naturally, everyone wants to have access to information. Everyone would like internal information to be public. It is glamorous or sexy to have all the information. We cannot disclose the information because it would put people's lives at risk. That is the danger, even at a parliamentary committee.

[*English*]

Senator Beyak: Thank you, gentlemen.

From your comments I expect you know that many Canadians are interested in national security and watch these programs. The domestic terror threat is always uppermost in their minds. There was a concern about the few charges that are laid against radicalized Canadians who go overseas to fight. Could you elaborate on what you found in your report and do you have recommendations to remedy it?

Le sénateur Carignan : Pourquoi?

Le vice-président : Le gouvernement l'a rejetée?

Le sénateur Carignan : Non, c'est le SCRS, je crois.

M. Blais : C'est le SCRS qui a rejeté cette recommandation.

Le sénateur Carignan : Pourquoi?

M. Blais : Je ne me souviens pas exactement ce qu'il a donné comme raison. Il a examiné l'aspect confidentiel et il ne voulait pas que ce soit partagé avec quelqu'un de l'extérieur.

Il faut dire que c'est peut-être une réponse facile. Vous savez, nous comprenons notre rôle, nous formulons des recommandations, nous pensons qu'elles peuvent être bonnes. Or, elles peuvent être rejetées. Dans certains cas, nous regimbons et nous revenons à la charge, parce que nous croyons que la recommandation devrait au moins être examinée. Dans ce cas, elle a été mise de côté.

Je dois dire que tout le monde est conscient de la menace interne et du risque que cela représente. Nos recommandations, qui émanaient du travail accompli par nos employés, visaient à souligner le fait qu'il aurait été bon, peut-être plus transparent, de confier l'examen à un groupe de l'extérieur. Cela a été rejeté. Nous ne nous battrons pas au sang pour ce genre de chose. Nous allons passer à autre chose, et nous verrons ce que tout cela va donner.

Nous avons mentionné un peu plus tôt, dans notre rapport, que cet aspect est devenu un élément important. Nous avons constaté les dommages pour les gens. Je ne qualifierai pas les gestes d'Edward Snowden ou d'autres personnes — il y a un peu de spectacle dans tout cela —, mais, à la base, des vies humaines sont en danger lorsque des renseignements à l'interne sont divulgués. Il y a une menace pour le Canada, pour les personnes et les sources. Des vies humaines sont en danger. Nous sommes toujours un peu préoccupés, et je pense que vous l'êtes autant que nous.

La sécurité nationale est quelque chose de sérieux. Évidemment, tout le monde a envie d'avoir accès à l'information. Tout le monde voudrait que ce qui est interne soit connu. C'est *glamour*, c'est sexy d'avoir toute l'information. Or, nous ne pouvons pas divulguer l'information, parce que nous mettrions des vies en danger. C'est le danger, même au sein d'un comité parlementaire.

[*Traduction*]

La sénatrice Beyak : Je vous remercie, messieurs.

D'après vos observations, je suppose que vous savez que beaucoup de Canadiens s'intéressent à la sécurité nationale et suivent l'application de ces programmes. La menace terroriste intérieure demeure à l'avant-plan de leurs préoccupations. Le fait que peu d'accusations aient été portées contre les Canadiens radicalisés qui vont combattre à l'étranger a suscité des inquiétudes. Pourriez-vous expliciter les constats que vous faites dans votre rapport et nous dire quelles recommandations vous formulez pour y remédier?

Mr. Blais: One thing is that we all agree it is now a new reality that we have to live with and be concerned with. This is a reality.

We should know that CSIS has always dedicated many resources to this particular point. We're not far yet in the process. In a sense, it is a day-to-day operation dealing with that because what we have seen recently in Canada and abroad tells us that it's not something that hasn't happened in the past. It is happening every day.

We review after the fact, as you know. We cannot properly identify on a daily operation what they should do. We review what they have done and whether they comply with the reality, and we make recommendations. This is what we did.

We agreed that CSIS is exposed to an internal threat here in Canada. You started with the radicalization question with a Canadian, which is something that is an internal threat in a sense that it is internal in Canada but also abroad.

The best we can say is that everybody has an eye on that right now. We will follow up and probably, as I mentioned, we will have a report. As you know, this report finished last year. So we have another 11 months now done. We know what is going on right now. I cannot report right now on that. I can tell you that shortly, with our next report, we will have a little more to say about it.

You see my point? I cannot go too far because we're not yet there, but we will be shortly.

Senator Mitchell: In one sense I was glad to see that both organizations are focused on metadata. Both of your reports refer to problems. I will say, in the case of CSE, at least it was contrite enough to admit it had made a mistake and began to take steps to fix it.

But that can't be said in the case of CSIS, where your recommendation was that CSIS should advise the Federal Court of activities relating to metadata collected. They just thumbed their nose at you and said they didn't agree.

Clearly, it is an issue. It is a privacy issue and a rights issue. It is of grave consequence to Canadians and to the fundamental liberties we have enjoyed in this country.

What steps could you take? Could you recommend that the legislation that they say gives them the out should be changed, that the government needs to strengthen the CSIS Act?

M. Blais : Il y a désormais une nouvelle réalité — c'est un point sur lequel tous sont d'accord — avec laquelle nous devons composer et dont nous devons nous préoccuper. Il s'agit bien d'une réalité.

Il importe de savoir que le SCRS a toujours consacré beaucoup de ressources à ce problème particulier. Le processus n'est pas encore très avancé. S'attaquer à ce problème constitue, dans un certain sens, une opération se déroulant au jour le jour parce ce que ce qui s'est passé récemment au Canada et à l'étranger nous montre que ce n'est pas un phénomène qui ne s'est jamais produit dans le passé. Il se produit tous les jours.

Notre examen est, comme vous le savez, postérieur aux faits. Comme il s'agit d'une opération au jour le jour, nous ne pouvons pas déterminer correctement ce qu'ils devraient faire. Nous passons en revue ce qu'ils ont fait, nous voyons si leur action répondait à la réalité, puis nous formulons des recommandations. C'est ce que nous avons fait.

Nous avons convenu que le SCRS est aux prises avec une menace intérieure, ici au Canada. Vous avez d'abord posé la question de la radicalisation d'un Canadien, ce qui représente une menace intérieure en ce sens qu'elle pèse sur le Canada, mais aussi à l'étranger.

Ce que nous pouvons dire de positif, c'est qu'en ce moment tout le monde est aux aguets. Nous ferons un suivi et, comme je l'ai dit, nous produirons sans doute un rapport. Comme vous le savez, le rapport présenté porte sur l'année dernière. Nous en présenterons donc un autre dans 11 mois. Nous savons ce qui se passe à l'heure actuelle, mais je ne peux pas produire un rapport pour le moment. Je peux vous assurer que bientôt, dans notre prochain rapport, nous en aurons plus à dire sur le sujet.

Vous comprenez ma position? Je ne peux pas m'avancer trop loin parce que nous ne sommes pas encore au fil d'arrivée, mais nous y serons prochainement.

Le sénateur Mitchell : Dans un certain sens, j'ai été heureux de voir que les deux organismes se concentrent sur les métadonnées. Vos deux rapports font état de problèmes. Je dirai, en ce qui concerne le CST, qu'au moins il a été assez contrit pour reconnaître son erreur et entreprendre de la réparer.

Mais on ne peut pas en dire autant du SCRS, à qui vous aviez recommandé d'informer la Cour fédérale des activités liées aux métadonnées recueillies. Il vous a simplement envoyés paître en disant qu'il n'était pas d'accord.

Manifestement, un problème existe. Il s'agit d'un problème de protection de la vie privée et de droits de la personne. Il n'est pas sans avoir des répercussions graves pour les Canadiens et sur les libertés fondamentales dont nous jouissons dans ce pays.

Quelles mesures pouvez-vous prendre? Pouvez-vous recommander que la loi qui lui donne cette latitude soit modifiée, que le gouvernement renforce la Loi sur le SCRS?

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Mr. Blais: If you remember what we put in our report, our recommendation was to be more transparent, that CSIS should be more transparent with the judges, when they brought the metadata to the attention of the judges. To make a long story short, it is in our report, so everybody can read that, including judges.

Senator Mitchell: Right.

Mr. Blais: In my view, I think we're probably close to seeing that the judges will have discussions with CSIS. They could have discussions on this particular suggestion we made. Even though our recommendation is there, we could expect that the judges will have more transparent access in the near future.

Is it clear enough?

Senator Mitchell: Yes. I think you are sending a message to the judges, who should be watching this.

Mr. Plouffe: In our case, we are not in the same predicament that my friend is. Most of the recommendations are being accepted by the minister who is responsible for the CSE. In my mind, if a recommendation that I make to CSE is not respected, I go to the minister and I say, "Sir, I made this recommendation. I had reason to make this recommendation, and I would suggest that you speak to your employee, CSE."

We have done that in the past with success. In our case, 93 per cent of our recommendations have been accepted by both the minister and CSE. There is a way to put pressure on the agency with regard to recommendations they don't accept.

Senator Mitchell: Last year, legislation — I think it was Bill C-44 — gave CSIS special warranting authority to break laws in foreign lands. You can write your response. I want to know whether you are taking steps to monitor that, to see how it is being set up, and to give us some assessment on how that is operating.

The Deputy Chair: Can you answer briefly?

Mr. Blais: It would be a good question for our future presentation before you because, as I mentioned, we report about last year, so everything that happened over the last few months.

Senator Mitchell: Just encouraging —

Mr. Blais: It is not because I don't want to answer; I'm not in a position to answer.

The Deputy Chair: The work that each of your organizations is doing is extremely important to parliamentarians and to the public at large. You can see from the questions that every senator could have gone on at some length.

M. Blais : Vous vous rappellerez ce que nous avons dit dans notre rapport, que nous recommandions une plus grande transparence, que le SCRS devait être plus transparent vis-à-vis des juges lorsqu'il portait les métadonnées à leur attention. Sans vouloir reprendre toute l'histoire, disons que c'est dans notre rapport, que tous peuvent lire, y compris les juges.

Le sénateur Mitchell : D'accord.

M. Blais : À mes yeux, nous sommes probablement près de voir les juges tenir des discussions avec le SCRS. Ils pourraient discuter de cette suggestion particulière que nous avons faite. Notre recommandation étant formulée, on pourrait s'attendre à ce que les juges bénéficient bientôt d'un accès plus transparent.

Est-ce suffisamment clair?

Le sénateur Mitchell : Oui. Je pense que vous envoyez un message aux juges, qui devraient être à l'écoute.

M. Plouffe : Pour notre part, nous ne sommes pas dans le même embarras que mon ami. La plupart de nos recommandations ont été acceptées par le ministre responsable du CST. Dans mon esprit, si je fais une recommandation que le CST n'applique pas, je n'ai qu'à aller voir le ministre et lui dire : « Monsieur le ministre, j'ai fait telle recommandation, j'avais de bonnes raisons de la faire et je vous suggère d'en parler à votre employé, le CST. »

Nous avons fonctionné ainsi avec succès dans le passé. Dans notre cas, 93 p. 100 de nos recommandations ont été acceptées à la fois par le ministre et le CST. Il y a moyen de mettre de la pression sur l'organisme pour ce qui est des recommandations qu'il n'accepte pas.

Le sénateur Mitchell : L'an dernier, un texte législatif — le projet de loi C-44, je crois — donnait au SCRS un pouvoir spécial l'autorisant à enfreindre la loi dans des pays étrangers. Vous pouvez rédiger votre réponse. Je voudrais savoir si vous prenez des mesures pour contrôler l'exercice de ce pouvoir, pour connaître ses modalités d'implantation et pour nous donner une évaluation de son fonctionnement.

Le vice-président : Pouvez-vous répondre brièvement?

M. Blais : Ce serait une bonne question à poser à notre prochaine comparution pour la simple raison que, comme je l'ai mentionné, notre rapport porte toujours sur l'année précédente, si bien que tout ce qui s'est produit au cours des derniers mois...

Le sénateur Mitchell : Je cherche simplement à encourager...

M. Blais : Ce n'est pas que je ne veuille pas répondre, c'est que je ne suis pas en position de le faire.

Le vice-président : Le travail qu'accomplit chacun de vos deux organismes revêt une importance extrême pour les parlementaires et le grand public. Vous aurez constaté d'après les questions qui vous ont été adressées que chacun des sénateurs aurait pu poursuivre longtemps.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Mr. Blais, I was going to ask if we could arrange through our clerk and your office for a reappearance to continue this discussion. Many senators have indicated an interest in continuing the discussion, but unfortunately we have scheduled another panel that should be starting any time now. Would that be possible?

Mr. Blais: Yes, and I'm sure I'm also speaking for Mr. Plouffe. We're open to that. It is important. So far, you are the only committee that we could —

The Deputy Chair: We will have you back soon.

Mr. Blais: I wasn't here before, but I will be more than happy to come back.

The Deputy Chair: Mr. Doucet has represented you well in the past before Senate committees, and it is good to see him back.

Mr. Plouffe, is that all right?

Mr. Plouffe: By all means.

The Deputy Chair: I thank the four of you very much for being here.

We will now hear from the final panel of the afternoon.

The Office of the Auditor General of Canada tabled its 2015 Fall Reports in Parliament on February 2, 2016, not long ago. The Standing Senate Committee on National Security and Defence, our committee, is authorized through its general orders of reference to examine and report on Canada's national security and defence policies, practices, circumstances and capabilities.

The Office of the Auditor General has been invited to appear before the committee to discuss Report 2, *Controlling Exports at the Border*, and Report 5, *Canadian Armed Forces Housing*, which both can be found in the 2015 Fall Reports of the Auditor General.

We are pleased to welcome Nancy Cheng, Assistant Auditor General. She is accompanied by Gordon Stock, Principal. Some of us would have met him in another incarnation a while back that we're trying to forget now. Nicholas Swales, Principal, is also present.

Thank you very much for being here. We appreciate it and look forward to your discussion.

Ms. Cheng, the floor is yours.

Monsieur Blais, j'allais vous demander si nous pouvions demander à notre greffier de prendre des arrangements avec votre bureau pour vous faire comparaître de nouveau, afin de poursuivre cette discussion. Bon nombre de sénateurs se sont montrés intéressés à la poursuivre, mais malheureusement nous avons une autre table ronde qui est sur le point de commencer. Serait-ce possible?

M. Blais : Oui, et je suis certain que M. Plouffe acceptera également. Nous y sommes tout à fait disposés. C'est important. Jusqu'à présent, vous êtes le seul comité auquel...

Le vice-président : Nous vous reviendrons sous peu à ce sujet.

M. Blais : Je n'étais pas ici auparavant, mais je serais plus qu'heureux de revenir.

Le vice-président : M. Doucet vous a bien représenté dans le passé devant les comités du Sénat, et c'est toujours un plaisir de le revoir.

Monsieur Plouffe, cela vous va?

M. Plouffe : Tout à fait.

Le vice-président : Je vous remercie tous les quatre de vous être présentés devant nous.

Nous passons maintenant à la dernière table ronde de cet après-midi.

Le Bureau du vérificateur général du Canada a déposé ses rapports de l'automne 2015 au Parlement le 2 février 2016, il n'y a pas longtemps. Le Comité sénatorial permanent de la sécurité nationale et de la défense, notre comité, est autorisé, par un ordre de renvoi général, à étudier afin d'en faire rapport les politiques, les pratiques, les circonstances et les capacités du Canada en matière de sécurité nationale et de défense.

Le Bureau du vérificateur général a été invité à comparaître devant le comité pour discuter du *Rapport 2 — Le contrôle des exportations à la frontière*, et du *Rapport 5 — Les logements des Forces armées canadiennes*, lesquels sont parmi les rapports du vérificateur général du Canada de l'automne 2015.

Nous sommes heureux d'accueillir Nancy Cheng, vérificatrice générale adjointe, qui est accompagnée de Gordon Stock, directeur principal. Certains d'entre nous l'ont rencontré naguère dans une autre incarnation que nous tâchons d'oublier. Nicholas Swales, directeur principal, est aussi présent.

Je vous remercie tous d'être ici aujourd'hui. Nous l'apprécions hautement et nous sommes impatients de vous entendre.

Madame Cheng, la parole est à vous.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*Translation*]

Nancy Cheng, Assistant Auditor General, Office of the Auditor General of Canada: Thank you for this opportunity to discuss two reports that were recently presented to Parliament. I am accompanied by Nicholas Swales, principal responsible for Report 2 — Controlling Exports at the Border and by Gordon Stock, principal responsible for Report 5 — Canadian Armed Forces Housing.

Let me begin with our report on controlling exports at the border. Exports are vital to Canada's economy, but are controlled to achieve a range of strategic objectives including national security. Several federal entities play a role in controlling exports, but the Canada Border Services Agency is the last line of defence in preventing goods that contravene Canada's export laws from leaving the country.

Our audit focused on whether the agency had what it needed to implement its export control enforcement priorities, prevent the export of goods that contravene Canada's export laws, and facilitate legitimate trade.

We found weaknesses in the authorities, information, and practices the agency applied to assess export risks, assign its resources, and act on its priorities. As a result, the agency missed opportunities to stop some goods that did not comply with Canada's export control laws from leaving the country.

[*English*]

For example, the Canada Border Services Agency relied on export declarations to identify and examine high-risk shipments but was unable to review all the declarations it received. We noted that it was not able to review export declarations received on paper as rigorously as those received electronically. Even when the agency flagged shipments as high risk, it did not examine about one in five.

We also noted some systematic gaps in coverage. For example, as a result of staffing challenges, the agency did not conduct any examinations of parcels leaving Canada at one large processing centre.

We also looked at the impact that the agency's export control activities had on legitimate trade. We found that the number of legitimate export shipments that were delayed by the agency to carry out its control activities was very small compared to total exports. However, the agency did not process 11 per cent of temporarily detained shipments in a timely manner.

[*Français*]

Nancy Cheng, vérificatrice générale adjointe, Bureau du vérificateur général du Canada : Je vous remercie de me donner l'occasion de discuter de deux rapports qui ont été déposés récemment au Parlement. Je suis accompagnée de Nicholas Swales, directeur principal chargé du *Rapport 2 — Le contrôle des exportations à la frontière*, et de Gordon Stock, directeur principal chargé du *Rapport 5 — Les logements des Forces armées canadiennes*.

Permettez-moi de commencer par le rapport sur le contrôle des exportations à la frontière. Les exportations sont essentielles à la vie économique du Canada. Elles sont cependant contrôlées dans le but d'atteindre une série d'objectifs stratégiques, notamment la sécurité nationale. Plusieurs organisations fédérales jouent un rôle à cet égard, mais l'Agence des services frontaliers du Canada est la dernière ligne de défense du Canada pour ce qui est de l'envoi hors du pays de marchandises qui contreviennent aux lois canadiennes en matière d'exportation.

Notre audit visait à déterminer si l'agence disposait de ce qu'il fallait pour mettre en œuvre ses priorités en matière d'exécution de la loi et de contrôle des exportations, prévenir l'exportation de marchandises qui contreviennent aux lois canadiennes et faciliter le commerce légitime.

Nous avons constaté qu'il y avait des faiblesses dans les pouvoirs, l'information et les méthodes sur lesquels se fonde l'agence pour évaluer les risques d'exportation, allouer ses ressources et donner suite à ses priorités. Par conséquent, l'agence a manqué des occasions d'empêcher des marchandises non conformes aux lois de contrôle des exportations du Canada de quitter le pays.

[*Traduction*]

Par exemple, l'Agence des services frontaliers du Canada s'est fondée sur les déclarations d'exportation pour repérer et examiner les expéditions à haut risque, mais n'a pas été en mesure d'examiner toutes les déclarations qu'elle a reçues. Nous avons constaté qu'elle n'a pas pu examiner les déclarations d'exportation sur papier de façon aussi rigoureuse que les déclarations électroniques. Même parmi les envois signalés comme à haut risque par ses services, un sur cinq environ n'était pas examiné.

Nous avons également constaté des lacunes systématiques dans la couverture. Par exemple, en raison du manque d'effectifs, l'agence n'a examiné aucun des colis expédiés hors du Canada dans un grand centre de traitement.

Nous avons examiné également l'incidence des activités de surveillance des exportations de l'agence sur les échanges légitimes. Il nous est apparu que le nombre d'envois destinés à l'exportation retardés par l'agence pour mener à bien ses activités de contrôle était très faible par rapport au volume total des exportations. Cependant, 11 p. 100 des envois retardés temporairement n'ont pu être traités dans les délais voulus.

Mr. Chair, we are pleased that the Canada Border Services Agency has agreed with our recommendations.

[*Translation*]

Let me now draw your attention to the second report of interest today on Canadian Armed Forces housing. This audit focused on whether National Defence and its Canadian Forces Housing Agency had managed military housing in a manner that was supported housing requirements, was cost effective and was consistent with government regulations and policies.

We found that National Defence did not comply with key aspects of its housing policy, which states that it can provide housing only in locations where there is an operational requirement, or where the private housing market cannot meet Canadian Armed Forces members' needs. We found the Department had not determined which members should be receiving housing, what form this housing should take, or where it should be located.

We also found that National Defence did not consider whether the private market could meet members' housing needs in some locations, although it had market analyses that showed they could be met in some urban locations like Halifax and Valcartier by the private sector.

[*English*]

We noted that National Defence policy requires that rental rates for its housing units be in line with market rates. We noted that the department had market analyses that showed that rental rates for military housing were below market in some locations. In the past, the department used appraisal values set by the Canada Mortgage and Housing Corporation until it stopped providing this service in 2013.

Most of National Defence's housing portfolio was built between 1948 and 1960 and needed renovation and updating. We found that the department had set a goal to modernize its portfolio but had not developed plans that set out the work, time and resources required to meet this goal. It also lacked up-to-date information about the condition of housing units.

About $380 million was spent on military housing between the 2012-13 and 2014-15 fiscal years. Without a plan to guide its spending and accurate information about the condition of units, National Defence cannot ensure these funds were used effectively on the highest priorities.

Monsieur le président, nous sommes heureux que l'Agence des services frontaliers du Canada ait accepté nos recommandations.

[*Français*]

J'aimerais maintenant attirer votre attention sur le deuxième rapport, soit celui sur les logements des Forces armées canadiennes. Cet audit visait à déterminer si la Défense nationale et son agence de logement des Forces armées canadiennes avaient géré le logement militaire de façon à répondre aux besoins en la matière, de manière économique et conforme aux règlements et aux politiques du gouvernement.

Nous avons constaté que la Défense nationale n'avait pas respecté des aspects importants de sa politique sur le logement militaire, laquelle prévoit que le ministère peut offrir des logements seulement dans les endroits où il y a un besoin opérationnel à satisfaire ou dans les endroits où le marché du secteur privé ne peut répondre aux besoins des membres des Forces armées canadiennes. Nous avons constaté que le ministère n'avait pas déterminé qui, parmi les membres des Forces armées canadiennes, devrait bénéficier de logement, ni sous quelle forme ni à quel endroit.

Nous avons aussi constaté que le ministère ne s'était pas demandé si le secteur privé pouvait répondre aux besoins en logement de ses membres dans certains endroits, même si ses analyses de marché démontraient que le secteur privé aurait pu le faire dans certaines régions urbaines, comme celles d'Halifax et de Valcartier.

[*Traduction*]

Nous avons relevé que la politique de la Défense nationale exige que les loyers de ses logements soient alignés sur les taux du marché. Nous avons noté que le ministère dispose d'analyses de marché montrant que les taux des loyers pour les logements militaires sont inférieurs aux taux du marché dans certains endroits. Par le passé, le ministère utilisait les barèmes d'évaluation établis par la Société canadienne d'hypothèques et de logement, et ce, jusqu'en 2013, date à laquelle elle a cessé de fournir ce service.

L'essentiel du parc immobilier du ministère de la Défense nationale avait été constitué entre 1948 et 1960 et avait besoin d'être rénové et réactualisé. Nous avons constaté que le ministère s'était donné pour objectif de moderniser son patrimoine, mais n'avait pas élaboré de plan prévoyant les travaux à accomplir, le calendrier à respecter et les moyens nécessaires pour réaliser cet objectif. Il ne disposait pas non plus d'un état des lieux actualisé de son parc immobilier résidentiel.

Au cours des exercices 2012-2013 et 2014-2015, les dépenses en matière de logements militaires se sont chiffrées à quelque 380 millions de dollars. Faute d'un plan pour orienter ses dépenses et d'une information précise sur l'état des logements, le ministère ne peut garantir que ces fonds ont été employés de manière efficace dans le respect de l'ordre des priorités.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

The timing of receipts of capital funding for major renovations from National Defence did not always match the construction cycle. For example, the agency received $6 million in January 2015 and did not have enough time to allocate funds to significant and highest priority work.

We are pleased to report that National Defence agreed with our recommendations and committed to take corrective action.

Mr. Chair, this concludes my opening remarks. We would be pleased to answer any questions the committee may have.

The Deputy Chair: Thank you very much, Ms. Cheng. I see you have with you the two principals responsible for each of the studies, which is very good.

Senator White: It is good to see the Auditor General's office here. I'm not sure I would have been saying that a year ago, but I do appreciate it.

My question surrounds the housing. I look at 1,500 empty units. It may not sound like a lot to National Defence, but certainly for the folks out there looking for PMQs, it would have had a real impact, I think, on the military and their ability to provide housing. You briefly talked about renovations, which may explain the 1,500.

Have you seen a document that may have given advantages or disadvantages to Crown versus renting from the public market? If so, could you share the results as to whether or not you made recommendations to them?

Ms. Cheng: I will ask Mr. Gordon Stock to answer that question.

Gordon Stock, Principal, Office of the Auditor General of Canada: We did not see a specific document that you are speaking of, if one exists. What we did look at was the percentage, and we thought it was a significant percentage that was still open. That's why we included it in the report.

From our work, it is far above what would be expected of someone providing the service for the private sector. It allows them to do that renovation work, but from our perspective it is a very high number.

Senator White: Thank you for that.

I know in the past that PWGSC has provided the renovation work in large centres. Having been in the RCMP and in communities where the military were, there have been complaints about how long it took PWGSC, because housing wasn't always a priority but offices were.

Le moment où la Défense nationale perçoit les fonds d'investissement destinés aux rénovations majeures ne coïncide pas toujours avec le cycle de la construction. À titre d'exemple, le ministère a reçu 6 millions de dollars en janvier 2015 et n'a pas disposé d'assez de temps pour allouer les fonds aux travaux les plus importants et les plus prioritaires.

Nous sommes heureux de consigner dans notre rapport que le ministère de la Défense nationale a accepté nos recommandations et s'est engagé à prendre les mesures nécessaires.

Monsieur le président, cela conclut ma déclaration préliminaire. Nous nous ferons un plaisir de répondre aux questions du comité.

Le vice-président : Merci beaucoup, madame Cheng. Je me réjouis de voir à vos côtés les deux directeurs principaux responsables de chaque étude.

Le sénateur White : Je suis heureux de recevoir ici le Bureau du vérificateur général. Je n'en aurais peut-être pas dit autant l'année dernière, mais j'apprécie vivement.

Ma question porte sur le logement. Je vois que 1 500 logements sont vides. Ça n'a peut-être pas l'air de grand-chose pour la Défense nationale, mais pour les intéressés sur le terrain, à la recherche d'un logement familial, cela aurait eu un fort impact, je crois, sur la capacité de l'administration militaire de fournir des logements. Vous avez fait allusion à des rénovations, cela pourrait expliquer ce chiffre de 1 500 logements vides.

Disposez-vous d'études montrant quels sont les avantages ou les désavantages de louer à la Couronne plutôt que s'adresser au marché? Si c'est le cas, pourriez-vous nous faire part des recommandations que vous auriez faites au ministère sur cette base?

Mme Cheng : Je demanderai à M. Gordon Stock de répondre à cette question.

Gordon Stock, directeur principal, Bureau du vérificateur général du Canada : Nous n'avons pas pris connaissance d'un document spécifique dont vous parlez, si tant est qu'il en existe un. Mais nous avons examiné le pourcentage et il nous a semblé que c'était un pourcentage important de logements qui restaient disponibles. C'est pourquoi nous l'avons consigné dans le rapport.

D'après nos travaux, il est très supérieur à ce que l'on attendrait de quelqu'un offrant ce service dans le secteur privé. Cela leur permet de procéder aux rénovations, mais à notre point de vue, c'est un chiffre très élevé.

Le sénateur White : Je vous remercie de votre réponse.

Je sais que, par le passé, c'est TPSGC qui s'est chargé des travaux de rénovation dans les grands centres. À l'époque où j'étais à la GRC, dans des collectivités où il y avait des militaires, j'ai entendu des plaintes sur les lenteurs de TPSGC, parce que le logement n'était pas toujours une priorité, contrairement aux bureaux.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Was there any consideration or anything in there indicating that concerns raised about the 10 per cent was as a result of a lack of support from PWGSC?

Mr. Stock: No, we did not have evidence of that. There is some work done by Defence Construction Canada as well for some of the construction contracts. They report through the similar minister.

Senator White: Yes.

Mr. Stock: I don't think that would be the same issue.

The main thing we noted was that the timing of when the funding was provided was very late in the year.

Senator White: March madness.

Mr. Stock: Because of that delay and the timing of the construction season and winter, it prevented some of the work from being done.

Senator Kenny: Mr. Stock, I wanted to ask about housing. This committee visited Gagetown about 10 years ago, and we were interested in their housing facilities there that were referred as their "shacks." I think that's the colloquial phrase for them in the military. We were told that they set aside 2 per cent of the value of the housing for maintenance on an annual basis and that amount was sufficient to keep the houses habitable and in good shape.

Did you encounter that percentage anywhere, and is that percentage sufficient to do the job?

Mr. Stock: We did not encounter that percentage. The percentage that we had was closer to the 15 per cent previously mentioned in terms of keeping houses open. Of that, approximately 10 per cent was for the renovations.

Part of the other need that was expressed to us was the period of time, especially in the summer, when there are a lot of transfers and trying to organize the work and renovations so that it fit in with the transfers.

In terms of the 2 per cent, no, we did not encounter that.

Senator Kenny: Frankly, 15 per cent of the market value of a house seems extraordinarily high. Do people spend that percentage on maintenance and upkeep in civilian life?

Mr. Stock: I'm sorry; I may have misunderstood your question. I was looking at the 15 per cent of units that were vacant.

Senator Kenny: I'm talking about 2 per cent of the market value.

Mr. Stock: That may have been an average of the amount, but given the age of the facilities that we're talking about — most of them were built between 1948 and 1960 — it would require a significant amount of money to keep them up, especially the older facilities.

Avez-vous quelque raison de penser que ce problème des 10 p. 100 était imputable au manque de soutien de TPSGC?

M. Stock : Non, rien ne nous l'indiquait. Construction de Défense Canada se charge également de certains contrats de construction. Ils relèvent du même ministère.

Le sénateur White : Oui.

M. Stock : Ce ne serait pas le même problème, je crois.

Ce qui nous a surtout frappés, c'est que les fonds n'arrivaient que très tard dans l'année.

Le sénateur White : La folie de mars.

M. Stock : Du fait de ce retard, du calendrier de la construction et de l'hiver, certains travaux n'ont pu être réalisés.

Le sénateur Kenny : Monsieur Stock, c'est du logement dont je voulais vous parler. Notre comité s'est rendu en visite à Gagetown, il y a environ 10 ans, et nous nous sommes intéressés aux installations de logement là-bas, qu'on appelle « cabanes ». C'est ainsi, je crois, qu'on les désigne en argot militaire. On nous avait dit que l'armée met chaque année 2 p. 100 de la valeur des logements de côté pour l'entretien et que ce montant suffisait pour maintenir les logements habitables et en bon état.

Avez-vous trouvé ce pourcentage quelque part, et est-ce qu'il est suffisant pour les besoins de la tâche?

M. Stock : Nous n'avons pas entendu parler de ce pourcentage. Celui qu'on avait se rapprochait des 15 p. 100 mentionnés plus tôt en termes de logements disponibles. Dont 10 p. 100 environ étaient destinés aux rénovations.

Un autre problème qui nous a été signalé concerne la période de l'année, l'été en particulier, où les mutations sont nombreuses et il faut s'efforcer d'organiser les travaux et les rénovations en tenant compte de ce phénomène.

Pour ce qui est des 2 p. 100, non, nous n'en avons pas entendu parler.

Le sénateur Kenny : Franchement, 15 p. 100 de la valeur de marché d'une maison semble extraordinairement élevés. Est-ce que dans le civil, on dépense un tel pourcentage pour l'entretien?

M. Stock : Je suis désolé; j'ai peut-être mal compris votre question. Je parlais des 15 p. 100 de logements qui sont vacants.

Le sénateur Kenny : Je parle des 2 p. 100 de la valeur du marché.

M. Stock : C'était peut-être le montant moyen, mais étant donné l'âge des installations dont on parle — bâties pour la plupart entre 1948 et 1960 —, les montants exigés pour leur entretien, surtout les installations les plus vieilles, doivent être non négligeables.

Senator Kenny: Mr. Swales, my understanding is that two hours are permitted for CBSA to take a look at goods leaving the country on aircraft and 48 hours on ships. Those two figures seem to be very short periods of time in which to do anything reasonable. I'm also concerned about trains in as much as CBSA doesn't inspect any freight trains coming into the country. It would seem strange if they were inspecting any leaving.

Nicholas Swales, Principal, Office of the Auditor General of Canada: With regard to trains, we didn't look at exports to the United States because the process of control for them is very different.

With regard to ships and aircraft, those time frames that you provided are correct. We do make a comment in the report about some work that the agencies had done on random examinations, and they certainly found those time frames challenging to try to look at goods through those exercises.

Senator Kenny: I don't want to put words in your mouth, but challenging verging on impossible?

Mr. Swales: These time frames are established in regulation, so they are established by policy.

They certainly find it challenging. It's not always impossible. They clearly get to many of the shipments that they've identified for examination. Eighty per cent were looked at in a timely manner; 20 per cent were not.

Ms. Cheng: Often when you look at what CBSA is trying to do, they're trying to balance enforcement with facilitation. A longer period might have an impact on calmness as well. That's probably the underlying reason for the policy to be made like that.

Having said that and as Nick has pointed out, there were able to show results. Even with the short turnaround, they were able to intercept a number of activities whereby they were able to stop certain goods that shouldn't go without permit or the necessary paperwork.

The Deputy Chair: If I understood Senator Kenny's question and your response, you say the time limits are established by regulation. I read in your report that the agency has accepted all your recommendations. Have they accepted the recommendation that the regulation should be changed?

Ms. Cheng: The recommendations did not specifically suggest that regulations be changed. This would be a policy call on the part of CBSA to propose to the government to see if the regulations should be modified.

The Deputy Chair: If you felt CBSA wasn't able to properly do the job expected of them because the regulation was too limiting, surely you should make comment on that, shouldn't you?

Le sénateur Kenny : Monsieur Swales, je crois comprendre que l'on donne 2 heures à l'ASFC pour inspecter les marchandises qui quittent le pays par avion et 48 heures pour les bateaux. Ces deux chiffres semblent laisser très peu de temps pour faire quoi que ce soit de raisonnable. Le transport ferroviaire me préoccupe également dans la mesure où l'ASFC n'inspecte pas les trains de marchandises qui entrent au pays. Il semblerait étrange qu'ils inspectent ceux qui en sortent.

Nicholas Swales, directeur principal, Bureau du vérificateur général du Canada : Pour ce qui est des trains, nous n'avons pas surveillé les exportations vers les États-Unis parce que le processus de contrôle dans leur cas est très différent.

Pour ce qui est des navires et des avions, les délais que vous avez mentionnés sont exacts. Notre rapport contient d'ailleurs des remarques sur les contrôles aléatoires réalisés par les services de l'agence, lesquels trouvent que les délais consentis pour les inspections constituent un défi.

Le sénateur Kenny : Je ne veux pas vous faire dire ce que vous ne dites pas, mais c'est un défi qui frise l'impossible?

M. Swales : Ces délais sont ceux que stipule le règlement, dans le cadre des orientations générales de l'agence.

Pour le personnel, ils constituent un défi qu'il n'est pas toujours impossible de relever. Le personnel voit effectivement un grand nombre d'expéditions qu'il a inscrites sur les listes des expéditions à inspecter. Quatre-vingts pour cent ont été examinées dans les délais prévus; 20 p. 100 non.

Mme Cheng : Lorsqu'on examine la façon de travailler de l'ASFC, on voit que, bien souvent, l'agence s'efforce de réconcilier l'obligation de contrôler et le souci de faciliter les échanges. Un délai plus long pourrait avoir une incidence sur la décontraction également. C'est sans doute la raison pour laquelle la réglementation a été conçue de la sorte.

Cela étant posé, et comme le signalait Nick, l'agence a pu faire valoir des résultats. Malgré la brièveté des inspections, le personnel a pu intercepter de nombreuses activités et retenir certaines marchandises qui ne doivent pas circuler sans permis ou sans la documentation nécessaire.

Le vice-président : Si j'ai bien compris la question du sénateur Kenny et votre réponse, vous dites que la durée des exercices d'inspection est établie par le règlement. Je lis dans votre rapport que l'agence a accepté toutes vos recommandations. A-t-elle accepté celle demandant que le règlement soit modifié?

Mme Cheng : Les recommandations ne demandaient pas expressément que le règlement soit modifié. C'est à l'ASFC qu'il appartient, en fonction de ses orientations générales, de proposer au gouvernement de modifier le règlement.

Le vice-président : Si vous estimiez que l'ASFC n'est pas en mesure de s'acquitter des tâches qui lui sont confiées en raison d'une réglementation trop stricte, vous vous sentiriez tenue de le signaler, n'est-ce pas?

Ms. Cheng: We have made comment on the various limiting factors to highlight the problems and issues to the department so it, in turn, can study and decide the proper course of action to move forward. We did not go as far as explicitly asking for regulations to be changed.

The Deputy Chair: You're saying that the CBSA would have to ask for that change, but did you have a discussion with them that that should be done?

Ms. Cheng: We have had discussions about that.

Mr. Swales: The one thing we said in the report is that they weren't, in fact, tracking the reasons for missed targets and that we had to go through a process of trying to collect information on that by primarily asking the people in the ports what was causing some of these challenges. They said to us that the fact that these things were sometimes loaded on the conveyances was already a problem. We ended up saying, "Since you do not have a full understanding of the situation, the first thing to do is to get a full understanding of the situation, which, amongst other things, could include the impact of the time frames on that."

The Deputy Chair: They agreed with all your recommendations?

Mr. Swales: They did.

[*Translation*]

Senator Dagenais: My question is for Ms. Cheng. Do you know how many border services officers are responsible for export control?

[*English*]

Ms. Cheng: We do have comments about the resources that have been allocated to export. I believe it is in paragraph 2.7.

We have not looked at the exact number. The agency itself did not keep track, so in our estimate, we felt that roughly less than 1 per cent of its full-time complement had been dedicated to exports.

[*Translation*]

Senator Dagenais: In your opinion, is that sufficient?

[*English*]

Ms. Cheng: From our perspective, we highlighted a number of problems and challenges that the agency faced. One of them is the resourcing and the staffing levels. Later on in the report we indicated how it manifested itself. There were certain activities such as targeted examination that did not get carried out when people were on leave or on vacation.

Mme Cheng : Nous avons communiqué nos observations sur les différentes contraintes afin de signaler les différents problèmes au ministère, qui, à son tour, peut faire ses propres études et décider des orientations à prendre. Nous ne sommes pas allés jusqu'à demander expressément une modification de la réglementation.

Le vice-président : Vous dites que c'est à l'ASFC d'en faire la demande, mais avez-vous parlé avec ces gens-là de la nécessité de modifier la réglementation?

Mme Cheng : Nous en avons parlé.

M. Swales : Ce que nous avons souligné dans le rapport, c'est qu'en fait, ils ne cherchaient pas à savoir pour quelles raisons les objectifs n'étaient pas atteints, ce qui nous a obligés à aller à la recherche de l'information essentiellement auprès des personnes dans les ports pour savoir ce qui posait problème. On nous a dit que, parfois, ces marchandises étaient chargées sur des véhicules, ce qui était déjà un problème. En fin de compte, nous avons dit « Puisque vous ne comprenez pas parfaitement la situation, la première chose à faire serait de vous assurer de bien comprendre, notamment en menant une étude de l'impact des temps d'exécution des tâches. »

Le vice-président : Ont-ils accepté toutes vos recommandations?

M. Swales : Oui.

[*Français*]

Le sénateur Dagenais : Ma question s'adresse à Mme Cheng. Avez-vous une idée du nombre d'agents à l'Agence des services frontaliers qui sont chargés du contrôle des exportations?

[*Traduction*]

Mme Cheng : Nous avons des commentaires à faire sur les ressources allouées aux exportations. C'est, je crois, le paragraphe 2.7 qui est visé.

Nous n'avons pas eu de montant précis sous les yeux. L'agence elle-même ne les a pas enregistrés alors, d'après nos estimations, c'est un peu moins de 1 p. 100, grosso modo, de son effectif à plein temps qui a été affecté aux exportations.

[*Français*]

Le sénateur Dagenais : Selon vous, est-ce suffisant?

[*Traduction*]

Mme Cheng : Nous avons signalé un certain nombre de problèmes et de défis que l'agence doit, selon nous, affronter. L'un de ces problèmes concerne le niveau des ressources et des effectifs. Nous avons indiqué plus loin dans le rapport comment cela se manifestait. Il y a des activités, comme les examens ciblés, qui ne sont pas menées à bien lorsque des personnes sont en congé ou en vacances.

They are locations whereby the enforcement is very light. One example we quoted was at a processing centre for parcels. Indeed, it wasn't really looked at.

[*Translation*]

Senator Dagenais: In your opinion, does the CBSA have the necessary information, practices and authorities to prevent the export of goods that contravene Canada's laws? In other words, do officers have adequate tools? We realize that there will always be goods that get through, but do they have the tools they need?

I will give you an example. I often go through customs on my way to the United States, and I have noticed that the U.S. customs service is very well equipped in terms of cameras and detection systems. I have the impression that there is a little less equipment on the Canadian side.

[*English*]

Ms. Cheng: We're primarily speaking to the export side of things. When you look at export activities, the audit found that the information is limited. The tools they have aren't exactly adequate either.

We describe a system whereby the declarations could be electronically declared. That system is old, and it was set up to trace statistics; it was not for the purpose of export control.

So, as a result, while the information is there, it's not actually helping the agency to identify or target risk. They have to set up separate resources to look at those declarations to decide whether some shipments are risky and should therefore be detained so they can examine them.

So the information is not very good. They have lots of declarations to deal with. Volume-wise in 2014, we're looking at 780,000 electronic declarations, and they have to go through those.

On top of that, there is the ability for exporters to file paper declarations, which makes it even more challenging. We were just talking about the 2 hours and the 48 hours. It's not so bad that if a local office gets the information, looks at it, the shipment is right there, and they have grounds to say, "We need to inspect this shipment or the other one."

Exporters can file paperwork at port A and export through port B. So if you only have a limited amount of time, by the time you say, "I want to stop to look at this particular shipment," it's quite possible and does happen that the shipment has already left the country. The law does not require the exporter to get release before goods can leave Canada. It's unlike import, where it needs to be accepted before it can be admitted into Canada.

Dans certains endroits, le règlement est appliqué de manière superficielle. Nous avons cité un exemple, celui du centre de traitement des colis. En fait, il n'y avait aucun contrôle du tout.

[*Français*]

Le sénateur Dagenais : Selon vous, est-ce que l'ASFC dispose de toute l'information, des méthodes et des pouvoirs nécessaires afin de prévenir l'exportation de marchandises qui contreviennent aux lois canadiennes? Autrement dit, est-ce que les agents sont suffisamment outillés? On comprend qu'il y aura toujours des marchandises qui passeront, mais est-ce qu'ils disposent de l'équipement nécessaire?

Je vous donne un exemple. Je traverse souvent les douanes pour aller aux États-Unis, et je remarque que les douanes américaines sont très bien outillées en termes de caméras et de systèmes de détection. Du côté canadien, on a l'impression qu'il y a un peu moins d'équipements.

[*Traduction*]

Mme Cheng : On parle surtout des aspects liés à l'exportation. Concernant les activités d'exportation, la vérification a montré que l'information dont on dispose est limitée. Les outils à leur disposition ne sont pas non plus des mieux adaptés.

Nous décrivons un système qui permettrait l'informatisation des déclarations. C'est un vieux système qui visait à permettre de suivre les statistiques; il n'avait pas pour objectif le contrôle des exportations.

Il s'ensuit que, même si l'information est disponible, elle ne sert pas vraiment à cerner ou à cibler le risque. Il faut mettre en œuvre d'autres ressources pour examiner ces déclarations, décider si des expéditions présentent un risque et devraient être retenues pour inspection.

L'information n'est par conséquent pas très bonne. Il faut traiter quantité de déclarations. En 2014, cela représente un volume de 780 000 déclarations électroniques à éplucher.

Qui plus est, les exportateurs peuvent remplir leurs déclarations sur papier, ce qui ajoute encore au défi. Nous avons parlé des 2 heures et des 48 heures. Ce n'est pas si mal qu'un bureau local puisse recevoir l'information et l'examiner, que la marchandise à expédier soit là et que les gens sur place aient des motifs de dire : « Il nous faut inspecter cette expédition ou cette autre. »

Les exportateurs peuvent remplir leur déclaration au port A et exporter du port B. De sorte que si vous n'avez que peu de temps à votre disposition, le temps pour vous de décider : « Je veux m'arrêter pour inspecter cet envoi, », il est bien possible — et ça arrive — que la cargaison ait déjà quitté le pays. La loi n'exige pas de l'exportateur qu'il obtienne une décharge avant que la marchandise ne puisse quitter le pays. À la différence des importations, qui doivent être acceptées avant d'être admises au Canada.

The Deputy Chair: To clarify the record, Ms. Cheng, we're talking about full-time equivalents dedicated to export control activities. Paragraph 2.7 or Report 2 says "fewer than 1 per cent."

Ms. Cheng: Yes, that's correct.

The Deputy Chair: I wanted that on the record.

Senator Mitchell: I'm interested in the fact that your review, which I expect you don't do much more frequently than once every decade — maybe I'm wrong, give or take a few years — caught this serious problem. There is an emerging debate now, at least on the Hill and elsewhere, that we need better oversight. We just had SIRC and the Commissioner for CSE here. CBSA, which is every bit as big as CSIS, has zero oversight except once every couple of decades or the decade you happen to look at it.

Did you make any recommendations about the need for an oversight body to supervise CBSA on an ongoing basis like SIRC does CSIS?

Ms. Cheng: When you look at the government machinery, many departments and agencies are delivering important mandates. Most do not have an oversight body. You have a management board, such as Treasury Board Secretariat, that provides government directives and policies that help guide good conduct and god behaviour, promote probity, transparency and accountability. Also, there are a lot of government policies that require people to do "the right thing" — normal processes that need to be followed in terms of making sure that there is fairness and equity in things we do within the public sector.

It is also incumbent upon those central agencies to oversee and provide management oversight. That's the management oversight that gets provided.

Of course, there would be parliamentary oversight as well. Whenever we do our reports, they are automatically referred to the Standing Committee on Public Accounts. That committee often calls us as witnesses and also calls departments and agencies to appear as witnesses to ask them about what happened with respect to the some of the observations we make and what they plan to do with some of our recommendations.

Senator Mitchell: You have recommended external oversight in other audits that we're aware of.

My next question concerns housing. I happened to have lived in eight military houses because I grew up with a military father. When we went back to Oromocto, not 10 years ago but even more recently, the house where I lived had a small roof over the steps. The post had broken and was hanging down and had been for some time. Clearly, there is a structural problem in many places.

Le vice-président : Je tiens à préciser pour mémoire que nous parlons bien des équivalents temps plein consacrés aux activités de contrôle des exportations, madame Cheng. Il est dit au paragraphe 2.7 du rapport 2 : « moins de 1 p. 100 ».

Mme Cheng : Oui, c'est exact.

Le vice-président : Je voulais que cela figure dans la transcription.

Le sénateur Mitchell : Je suis intéressé par le fait que votre examen a relevé ce problème grave alors qu'à mon avis vous n'en faites pas plus d'un tous les 10 ans — je me trompe peut-être à quelques années près. Il y a un nouveau débat maintenant, au moins au Parlement et ailleurs, qu'il faut suivre de plus près. Nous venons tout juste d'entendre le CSARS et le commissaire du CST. L'ASFC, qui est tout aussi grande que le SCRS, n'est pas surveillée du tout, ou une fois tous les 10 ou 20 ans, où quand le hasard en décide.

Avez-vous fait des recommandations sur la nécessité d'instaurer un organisme de surveillance supervisant l'ASFC en continu comme le fait le CSARS dans le cas du SCRS?

Mme Cheng : Vous pourrez constater que de nombreux ministères et organismes s'acquittent de mandats importants sans surveillance externe. Vous avez un comité de gestion comme le Secrétariat du Conseil du Trésor qui élabore des directives et politiques servant à définir un code de bonne conduite et à promouvoir la probité, la transparence et la responsabilité dans le gouvernement. Il y a aussi beaucoup de politiques du gouvernement qui demandent aux personnes de faire « les choses comme il faut » — en s'en tenant aux processus normaux à suivre pour être certain que nous faisons preuve d'équité dans le secteur public.

Il incombe aussi aux organismes centraux de superviser et de surveiller la gestion. C'est ça la supervision de la gestion qui est prévue.

Bien sûr, le Parlement aussi exerce une fonction de supervision. Quand nous déposons un rapport, le Comité permanent des comptes publics en est automatiquement saisi. Ce comité nous invite fréquemment à témoigner, de même qu'il invite les ministères et les agences pour leur demander ce qu'il en est du respect de certaines des observations que nous faisons et de la suite qu'ils entendent donner à nos recommandations.

Le sénateur Mitchell : Vous avez recommandé une supervision externe dans d'autres vérifications dont nous avons eu connaissance.

Ma prochaine question concerne le logement. Il se trouve que j'ai vécu dans huit logements militaires parce que j'ai été élevé par un père militaire. Lorsque nous sommes retournés à Oromocto, il n'y a pas 10 ans, mais plus récemment encore, la maison où j'ai vécu avait une petite marquise au-dessus des marches d'escalier. Son support était cassé et pendait, depuis pas mal de temps déjà. De toute évidence, il y a des problèmes structurels dans bien des endroits.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

With respect to your point 15 of your presentation, the agency received $6 million in January 2015 to do some work, which as too late to get it done. Whose fault would that be? Why would that happen? How would we structure it so it doesn't happen again?

Ms. Cheng: Perhaps I can give a general answer, and then I will ask Gord to provide more details.

If they were provided funding in January, you only have until the end of the fiscal period to deploy and use that. So if that money gets sent to the agency by the Department of National Defence, then the agency only has two months to try to provide for the work orders to do construction. In January, it would be difficult to try to do that kind of work; it would be difficult to address the urgent needs.

Mr. Stock: This problem is not just within National Defence but also across government, to a certain extent. In this particular case, you've got National Defence providing funds to the agency. It comes from the parliamentary appropriation that is approved much earlier in the year, but the authorization to spend is not with the agency until late in the year for some of that capital funding. So that part is somewhat within the department.

But the part that's more across government, especially on the capital expenditure side, where you have a number of houses and long-term assets, and you're trying to match the actual funding and the replenishment of the long-term assets with allocations made during one year — and it may take more than one year to plan, construct and deliver the assets that you need. It takes considerable organization to be able to do that, and it is not always possible to have the authorization to spend before you spend the money.

So while this could point some in the direction of accrual appropriations, it is a long-standing issue and not just with the agency.

Ms. Cheng: If I may add, basically they were also able to use the rental revenue, but the rental revenue can only be used for operations and maintenance; they couldn't use it for capital construction. So when you have old houses that date back to the 1948 and 1960s period, there is a lot of capital construction work needed. If you don't line up your construction cycle with when the money comes, then every year you only get to do a small part of it and the money doesn't really help you renovate those houses. You only have the rental revenue to help support the ongoing maintenance.

There was a question about why the maintenance cost is so high. When the houses are run down, obviously it costs more to maintain them.

À propos du point 15 de votre présentation, l'agence a reçu 6 millions de dollars en janvier 2015 pour effectuer des travaux, c'est-à-dire trop tard pour qu'ils puissent être réalisés. À qui la faute? Comment cela peut-il se produire? Comment restructurer le processus pour éviter que cela ne se reproduise?

Mme Cheng : Je peux peut-être répondre en termes généraux, puis je demanderai à Gord de donner davantage de détails.

Si vous recevez le financement en janvier, vous n'avez que jusqu'à la fin de l'exercice fiscal pour répartir et employer ces fonds. Par conséquent, si le ministère de la Défense nationale envoie ces fonds à l'agence, celle-ci n'a plus que deux mois pour passer les contrats de construction. En janvier, ce serait difficile de faire ce genre de travaux; il serait difficile de répondre aux besoins urgents.

M. Stock : Le problème ne concerne pas seulement la Défense nationale, mais l'ensemble du gouvernement dans une certaine mesure. Dans le cas qui nous occupe, le ministère de la Défense nationale fournit les fonds à l'agence. Ils proviennent du budget adopté par le Parlement beaucoup plus tôt dans l'année, mais, pour une partie de son budget d'immobilisations, l'agence ne reçoit l'autorisation de dépenser que plus tard dans l'année. Donc pour cette partie, c'est plutôt le ministère qui est concerné.

Mais pour le reste, les responsabilités sont davantage réparties entre les différents ministères, en particulier pour ce qui est des investissements, quand vous avez de nombreux bâtiments et des équipements à long terme, et qu'il vous faut trouver le juste équilibre entre le financement courant et la reconstitution de ces équipements avec les montants alloués durant une année — et qu'il faut parfois plus d'une année pour programmer, construire et livrer les équipements dont vous avez besoin. Il faut une excellente organisation pour y parvenir et il n'est pas toujours possible d'avoir l'autorisation de dépenser avant de dépenser les fonds.

Alors cela amènera peut-être certains à pencher en faveur de l'adoption de la comptabilité d'exercice, mais le débat sur la question dure depuis longtemps et ne concerne pas seulement l'Agence.

Mme Cheng : Permettez-moi d'ajouter que l'agence peut également employer le produit des loyers, mais seulement au titre de l'exploitation et de la maintenance; pas pour les immobilisations. Or, avec de vieilles maisons qui remontent aux années 1948 et 1960, il y a de gros besoins en la matière. Si votre cycle de construction n'est pas en phase avec vos rentrées de fonds, vous ne pouvez en réaliser qu'une petite partie chaque année et cet argent ne vous sert pas réellement à rénover ces maisons. Vous ne disposez que du revenu des loyers pour financer les activités courantes d'entretien.

On a demandé pourquoi le coût de l'entretien est si élevé. Il va de soi que lorsque les maisons sont en piteux état, leur entretien coûte plus cher.

So there are problems with the actual cycle itself to match up with when they get capital funding, but they are also hamstrung with the fact that they can't use the rental money to do capital construction.

I found it: paragraph 5.57, about $270 million in rental revenue and $110 in capital. So of the 380, most of the funding was rental revenue that they would get throughout the year, but they can't use that with capital work.

Senator Mitchell: But that could be changed with a legislative or regulatory change.

Mr. Stock: That is beyond my knowledge in terms of the actual mechanisms as far as how that would be changed.

They do have the special operating agency authority right now, so they have the authority to re-spend the revenue, as Ms. Cheng said. They have not been able to use all of that for the renovations, and so they have used a mechanism whereby they have provided some of that money back to National Defence. National Defence has provided them with the capital. That's part of the delay that is going on within that mechanism.

I don't think it is a good mechanism right now.

Ms. Cheng: If you are looking at departmental spending, then it's actually a change between the capital vote and the operating vote. For that change, it actually has to go to Parliament.

If it's a special operating agency, we are not specifically clear on what the rules are, but if you're interested, I think we should be able to find that and get back to you.

Senator Ngo: My question is related to your audit. You say about one third of the targets were not examined because the agency's local office receives information about the targets too late or after the shipment has already left or had been loaded onto the planes or the ships. How do you explain these delays? And did the targets you mentioned that were examined contain weapons or goods subject to economic sanctions?

Ms. Cheng: Mr. Chair, if I may, I will clarify the context a little bit.

Essentially, what we're saying is that there is a targeting unit that identifies major shipments that might have risk. Then it would be the up to the Border Service officers to stop shipments from leaving Canada, and examine them. Even know the targeting unit has identified a number of these high-risk shipments, 1 in 5 did not get looked at. What you quoted was the reason one in five did not get looked at. One of the reasons is that by the time they get to it, the shipment has already left the

Donc, le problème se pose déjà de la mise en phase du cycle de construction et du cycle de financement, à quoi s'ajoute la contrainte interdisant d'utiliser le revenu des loyers pour la construction de nouveaux logements.

J'ai trouvé : au paragraphe 5.57, le chiffre est d'environ 270 millions de dollars pour les revenus des loyers et 110 millions pour les fonds d'immobilisations. Donc, sur les 380 millions, la plus grosse partie du financement correspondait aux revenus de loyers qui rentrent tout au long de l'année, mais qui ne peuvent pas être utilisés pour des investissements en capital.

Le sénateur Mitchell : Mais cela pourrait changer moyennant une modification de la loi ou de la réglementation.

M. Stock : Ma connaissance des modalités d'un tel changement ne va pas jusque-là.

Son statut d'organisme de service spécial autorise déjà l'agence à dépenser les revenus qu'elle perçoit, comme l'a dit Mme Cheng. Comme elle n'a pas pu employer tous ces fonds pour les rénovations, elle a eu recours à un mécanisme lui permettant de reverser une partie de ces fonds à la Défense nationale qui lui a fourni le capital. Les retards encourus sont en partie imputables à ce mécanisme.

Je ne pense pas que le mécanisme actuellement en place soit bon.

Mme Cheng : Pour ce qui est des dépenses du ministère, il s'agit d'un changement entre le budget d'immobilisations et le budget de fonctionnement. Une telle redistribution ne peut être décidée que par le Parlement.

Dans le cas d'un organisme de service spécial, je ne sais pas exactement quelles sont les règles à suivre, mais si cela vous intéresse, nous pourrons nous informer et vous revenir.

Le sénateur Ngo : Ma question concerne votre vérification. Un tiers des cibles n'ont pas été inspectées, dites-vous, parce que les bureaux locaux de l'agence reçoivent les informations relatives à ces cibles trop tard ou après que les marchandises ont déjà été expédiées ou chargées à bord des avions ou des navires. Comment expliquez-vous ces retards? Et pour ce qui est des envois ciblés qui ont été examinés, est-ce qu'ils contenaient des armes ou des marchandises passibles de sanctions économiques?

Mme Cheng : Monsieur le président, avec votre permission, je voudrais préciser un peu le contexte.

En substance, il y a une unité chargée du ciblage, qui repère les gros chargements présentant un risque. Après quoi, il revient aux agents de l'ASFC d'empêcher que les marchandises ne quittent le Canada et de procéder aux inspections. Mais bien que l'unité du ciblage ait identifié un bon nombre de ces envois à haut risque, un chargement sur cinq n'a pas été inspecté. Vous avez cité une des raisons pour lesquelles il en est ainsi. Une autre de ces raisons, c'est que la marchandise peut avoir quitté le pays avant que les

country. The shipments can leave the country if they are not held and formally detained by the Border Service officers. That is one of the problems that the agency faces.

Senator Ngo: With these missing targets, we do not know if the containers hold weapons?

Ms. Cheng: In one of the exhibits we showed there are three priorities. One is strategic goods, and the priority is essentially to deal with counter-proliferation. For that particular one, about 1 in 5 did not get examined. When they actually are able to examine them, they have results to show. Our audit noted that 29 per cent of them found exceptions. Not all were major exceptions, but some were important.

Senator Ngo: How do you explain the fact that the CBSA has limited authority to review all export declarations, such as the importation of illegal drugs. What would you recommend to address this situation?

Ms. Cheng: There are a number of authority-related issues and challenges that CBSA faces. One of them is a situation where there is no report. Not every export requires declaration, so if they don't declare, the CBSA does not actually have authority to go in and open up and stop a shipment unless they have reasonable grounds. They need to say, "I have reason to think there may be a contravention here," and therefore they can stop the shipment. That is a significant limiting factor when you start to look at non-reported shipments. That's one of the authority issues we're referring to.

Senator Ngo: Thank you.

Senator Beyak: I have two questions, one for Ms. Cheng and Mr. Swales. The number was mind-boggling to me: 780,000 declarations. If they did 2,000 a day, 24 hours a day, 7 days a week — how can they possibly review that many? How many are they not able to review and are slipping out without review?

Ms. Cheng: It is a lot. They do have a central targeting unit. We just talked about the statistics. From our estimate, less than 1 per cent of their full-time strength has been assigned the responsibility to look at the declarations. There they were not able to cover all of the declarations that were received in the system.

With regard to the problem with looking at it in terms of how many a day, I think I'll ask Nick to give more clarification.

Mr. Swales: The way in which it is at least conceptually possible is that these declarations are received electronically. The way they go about is to apply filters to the electronic information so that they are looking for particular things.

inspecteurs n'aient pu se rendre sur place. La marchandise peut quitter le pays à moins qu'elle ne soit formellement retenue par les agents du service des frontières. C'est l'un des problèmes auxquels doit faire face l'ASFC.

Le sénateur Ngo : En l'absence de ces cibles, on ne sait pas s'il y avait des armes dans ces conteneurs?

Mme Cheng : On voit, dans l'une des pièces que nous avons montrées, qu'il y a trois priorités. L'une concerne les marchandises stratégiques et elle vise essentiellement à lutter contre la prolifération. À cet égard, un chargement sur cinq environ n'a pas été inspecté. Quand les inspections peuvent se faire, elles donnent des résultats. Il est signalé dans notre rapport de vérification que des exceptions ont été constatées dans 29 p. 100 des cas. Ce n'était pas toujours des exceptions majeures, mais certaines étaient importantes.

Le sénateur Ngo : Comment expliquez-vous que les pouvoirs de l'Agence de surveiller toutes les déclarations d'exportations soient limités, comme dans le cas de l'importation de drogues? Que recommanderiez-vous pour remédier à la situation?

Mme Cheng : L'ASFC se heurte à de nombreux problèmes en matière de compétence et à de nombreux défis. L'un d'entre eux tient à l'absence de rapports. Toutes les exportations n'exigent pas une déclaration, par conséquent s'il n'y a pas de déclaration, l'agence n'a pas l'autorisation d'ouvrir les conteneurs et d'empêcher l'expédition à moins d'avoir des motifs raisonnables. À moins de pouvoir dire « j'ai de bonnes raisons de penser qu'il y a contravention à la loi dans ce cas, » l'ASFC ne peut pas empêcher l'expédition. C'est une contrainte importante quand on parle d'envois ne faisant pas l'objet d'une déclaration. C'est l'un des problèmes que l'on signalait en matière de compétences.

Le sénateur Ngo : Merci.

La sénatrice Beyak : J'ai deux questions à poser, l'une à Mme Cheng et l'autre à M. Swales. Ce chiffre m'a donné le vertige : 780 000 déclarations. Si l'on en fait 2 000 par jour, 24 heures par jour, 7 jours par semaine — comment peut-on donc en vérifier un si grand nombre? Combien de ces déclarations ne peuvent être vérifiées et échappent à toute vérification?

Mme Cheng : Beaucoup. Il existe une unité centrale de ciblage. Nous venons de parler des statistiques. Selon nos estimations, moins d'un pour cent des effectifs à temps complet de l'ASFC a été affecté à la vérification des déclarations. Il n'était donc pas possible de couvrir toutes les déclarations entrées dans le système.

En ce qui concerne le rythme journalier de vérification des déclarations, je voudrais demander à Nick d'apporter des précisions.

M. Swales : Le fait que les déclarations soient informatisées rend la chose au moins concevable. La méthode consiste à appliquer des filtres aux déclarations informatisées, à la recherche de données particulières.

It's an old example now, but shipments to Iran would be something that, in the past, they would have looked at and tried to identify. You could do that electronically in the system. It's not entirely impossible if you have the right kind of system.

Part of the problem is they don't have a system that can do that part of the work automatically, so they have to do all that filtering manually.

The other issue we saw is that staffing levels are not consistent. There were periods of time when there were fewer people and the declarations were coming through at a fairly consistent rate.

We weren't able to come up with any data on how many they miss or aren't able to look at. Again, the information system doesn't track how they look at them well enough for us to do that. But we did know that there were periods of time when there weren't people working on them.

Ms. Cheng: I will add a little bit of information.

If you look at the report in paragraphs 2.46 to 2.48, you will see comments about the staffing level. One problem is that because they couldn't staff it 24/7 — essentially evenings and weekends — if the information were to come about then, and you only have short turnaround from 2 hours to 48 hours, it would be difficult to spot those high-risk shipments, stop them, inspect them, and the satisfy yourself before you release them.

One of the concerns we have is the patterns. There are times that you talk about controls. They need to be systematic and you need to implement them, but from time to time there are gaps. What we are seeing now is that there are systematic gaps, so it makes it not that difficult for people who want to skirt the system to try to do something.

We are satisfied with the results. That's something the agency needs to look at and have dialogue and discussion with the government. Perhaps if Parliament were to take an interest and ask questions on that, they could decide whether the status quo is sufficient.

Certainly the agency is rather receptive. As we indicated in our opening statement and have confirmed at this hearing, they agree with all our recommendations and are preparing action plans to try to deal with some of the comments we've made. They need to be able to look at the resource balance, the authority question, and the automatic tool.

With regard to the case system we referred to, there have been a number of statements to say how it has been falling short and needs updating, but also because different departments are working with their priority lists. Statistics Canada indicated that's not something they wish to maintain, so even its viability is

Mon exemple est peut-être maintenant désuet, mais il fut un temps où les envois destinés à l'Iran auraient retenu l'attention et donné lieu à des recherches approfondies. Le système informatique permet cela. Avec le système approprié, ce n'est pas entièrement impossible.

Le problème tient en partie au fait que le système ne permet pas un traitement automatique d'une partie de ce travail et que tout le travail de filtrage doit se faire manuellement.

L'autre problème qui nous est apparu est que le niveau des effectifs n'est pas constant. À certaines périodes, il y avait moins de personnel alors que les déclarations continuaient de rentrer à un rythme assez soutenu.

Il ne nous a pas été possible d'obtenir des données sur le nombre de déclarations qui passent au travers des mailles du système et ne font pas l'objet de vérifications. Je répète que le système informatique ne permet pas un suivi suffisant des modalités de vérification pour produire ces données. Mais nous avons pu apprendre qu'à certaines périodes, personne ne vérifiait les déclarations.

Mme Cheng : J'ajouterai quelques éléments d'information.

Si vous vous reportez aux paragraphes 2.46 à 2.48 du rapport, vous trouverez des commentaires portant sur le niveau des effectifs. L'un des problèmes tient au fait que, faute de pouvoir employer du personnel 24 heures sur 24 et 7 jours sur 7 — en particulier la nuit et les week-ends — si les données entrent à ces moments-là, et vous n'avez que deux heures ou 48 heures pour procéder aux inspections, il devient difficile de repérer les chargements à haut risque, de les arrêter, de les contrôler et de vous assurer que vous pouvez les laisser repartir.

L'un de nos sujets de préoccupation concerne les modes opératoires. On parle parfois de contrôles. Ils doivent être systématiques et il faut les mettre en œuvre, mais il y a parfois des lacunes. On constate maintenant qu'il y a des lacunes systématiques, de sorte qu'il n'est pas très difficile pour ceux qui voudraient contourner le système, de s'y essayer.

Nous sommes satisfaits des résultats. L'ASFC doit se pencher sur ces problèmes et engager le dialogue et la discussion avec le gouvernement. Si le Parlement s'intéressait à la chose et posait des questions à ce sujet, peut-être serait-il en mesure de décider si l'on peut se contenter du statu quo.

L'agence, pour sa part, est tout à fait réceptive. Comme nous l'avons dit au tout début et confirmé pendant l'audience, elle a accepté toutes nos recommandations et elle est en train d'élaborer des plans d'action en réponse aux commentaires que nous avons faits. Les questions concernant l'équilibre des ressources, les compétences de l'agence et l'automatisation du système devront être examinées.

Pour ce qui est du système de gestion des cas dont nous avons parlé, de nombreuses interventions ont signalé ses insuffisances et la nécessité de le moderniser, le fait que les différents ministères aient chacun leur liste de priorités constituant un facteur aggravant. Statistique Canada a déclaré ne pas souhaiter

being questioned at the moment. There are a number of issues that the agency faces, and they have to come to an informed decision as to what to do.

Senator Beyak: Your report was excellent.

Mr. Stock, I notice that DND agreed with your report completely and is going to implement your recommendations. What did you take into account from the 2010 report that they did not agree with? It was an external report, not one of yours, and they didn't take into account personal life, finances, divorce, actual proximity to the base.

Mr. Stock: The report you speak about was one that tried to estimate the number of houses that were needed. It was done as an internal report, and there was a different basis on which the information was put together. Underlying that different basis is a difference between government policy and what is being put in place in terms of regulations under the National Defence Act. Some aspects of the regulations allow them to do things. Affordability is one instance. They can provide houses to meet their needs under those regulations that may not be totally in line with the policy. It's because of that that you get a discrepancy coming in between the two, as the regulations take precedence over the policy. Therefore, that's the real answer to the question as to how they can agree with the recommendations.

We were quite happy with the agreement, with the recommendations and the commitment to action.

[*Translation*]

Senator Carignan: I am somewhat troubled by some of your statements. First, with respect to the strategic objective of inspection, particularly national security, you explained that in one centre in particular, no packages were inspected for a long period of time. You also said that there were systematic gaps at certain locations and that an ill-intentioned person could use them to contravene national security rules. Given the importance and seriousness of the situation, did you report individuals to the RCMP?

[*English*]

Ms. Cheng: Certainly, there are significant implications in terms of some of these gaps. The member has highlighted several of them, things like when I indicated earlier that a paper declaration can be filed in port A and export happens in port B. Those things actually happen. The audit tried to find out whether people were filing and shipping goods in different ports. Those things actually came to pass. They happened.

continuer à le gérer, de sorte que sa survie n'est même pas assurée à l'heure actuelle. L'ASFC fait face à de nombreux problèmes et doit décider, en connaissance de cause, des mesures à prendre.

La sénatrice Beyak : Votre rapport était excellent.

Monsieur Stock, je remarque que le ministère de la Défense nationale était entièrement d'accord avec votre rapport et qu'il s'apprête à mettre en œuvre vos recommandations. Y a-t-il des éléments du rapport de 2010 que vous aviez pris en compte, avec lesquels il n'était pas d'accord? Il s'agissait d'un rapport externe, pas de l'un de vos rapports, et il ne tenait pas compte de la vie privée du personnel, des aspects financiers, du divorce, de la proximité avec la base.

M. Stock : Le rapport dont vous parlez cherchait à estimer le nombre de maisons dont on avait besoin. Il s'agissait d'un rapport interne et l'information n'avait pas été structurée de la même façon. La différence tenait à l'écart entre les orientations du gouvernement et la nature de la réglementation mise en place aux termes de la loi sur la Défense nationale. Certains aspects de la réglementation permettent de faire des choses. Le facteur prix entre en ligne de compte. Il est possible de répondre aux besoins en matière de logement en jouant sur les dispositions de cette réglementation qui peut ne pas être exactement alignée sur les orientations générales. C'est ce qui explique qu'une divergence s'instaure entre les deux, la réglementation, prenant le pas sur les orientations générales. Par conséquent, c'est là la véritable réponse que l'on peut donner à la question de savoir comment le ministère peut être d'accord avec les recommandations.

Nous étions contents qu'il soit d'accord, qu'il accepte les recommandations et s'engage à les mettre en œuvre.

[*Français*]

Le sénateur Carignan : Je suis un peu troublé par certaines de vos affirmations. Premièrement, en ce qui concerne l'objectif stratégique de l'inspection, notamment les questions de sécurité nationale, vous avez expliqué que, dans un certain centre en particulier, pendant une longue période de temps, aucune inspection de colis n'a eu lieu. Vous avez également dit qu'il se crée aussi des écarts systématiques à certains endroits et qu'une personne malveillante pourrait les utiliser pour enfreindre les règles de la sécurité nationale. Compte tenu de l'importance et de la gravité de la situation, avez-vous recommandé des gens à la GRC?

[*Traduction*]

Mme Cheng : Ces lacunes ont sans aucun doute des implications importantes. Le membre du comité en a signalé quelques-unes, du genre de celle que j'ai signalées relativement à la possibilité d'introduire une déclaration sur papier dans un port A et d'exporter la marchandise à partir d'un port B. Ces choses se produisent dans la réalité. La vérification a visé à établir si certaines personnes enregistraient la déclaration dans un port et exportaient d'un autre. Cela se produit effectivement. Cela arrive.

In terms of some of the paper returns, we also found that the CBSA has these watch lists for exporters. We also found that paper declarations were filed by exporters that were on the watch list, and they were generally not looked at. So there are a number of concerns of this kind.

That's why we're underscoring that we're somewhat making it a little easy for people who are trying to skirt the system. We need to be less predictable. That, indeed, is one of the recommendations.

Herein lies the problems with non-declared shipments, for example, because for those, the CBSA doesn't have authority to do random checks. Random checks are a good deterrent. I don't actually know what's there, but every so many shipments I'm going to stop one and look at it. It would act as a deterrent to those who try to skirt the system. For non-reported shipments, CBSA does not have the authority to do random checks. That's another constraint they have, in addition to the other constraints that we talk about.

[*Translation*]

Senator Carignan: Perhaps my question was not clear enough. In view of the fact that there are systematic gaps and that there is at least one centre with no controls, an ill-intentioned manager at that location could systematically not staff the position and tell a criminal to use centre X or Y where no controls take place on the weekend, for example.

I am very concerned by what you discovered. I imagine that since the objectives are linked to national security, this also caught your attention when you were conducting your audit.

Therefore, did you go to the RCMP so that it would investigate those people and determine whether this lack of oversight provides the opportunity to commit crimes? Did you refer information to the RCMP?

[*English*]

Ms. Cheng: I thank the member for clarifying his question. His question refers to whether we have referred any information to the RCMP.

The RCMP was an intervenor when we were looking at the audit work, when we were looking at stolen cars and illicit drugs and the like, but I don't believe any of the audit findings, as such, were referred to them for further investigative work. I'll ask for confirmation that Nick might have.

[*Translation*]

Mr. Swales: No, we did not give information specifically to the RCMP. You are wondering whether gaps in oversight were deliberate.

Pour ce qui est des déclarations sur papier, nous avons également découvert que l'ASFC a des listes d'exportateurs à surveiller, mais que les déclarations soumises par ces exportateurs n'étaient généralement pas inspectées. Il y a plusieurs préoccupations de ce genre.

C'est pourquoi nous soulignons le fait que nous facilitons un peu trop la tâche à ceux qui veulent contourner le système. Il nous faut être moins prévisible. C'est en effet une de nos recommandations.

Prenez, entre autres, le problème des envois non déclarés pour lesquels l'ASFC n'a pas le droit d'effectuer de contrôles aléatoires. Les contrôles aléatoires sont un bon moyen de dissuasion. On ne sait pas ce qu'il y a dans une série des chargements, mais on va périodiquement en bloquer aux fins d'inspection pour dissuader ceux qui tentent de passer entre les mailles du filet. Cependant, pour les envois non déclarés, l'ASFC n'est pas autorisée à faire ces contrôles aléatoires. C'est encore une contrainte qui vient s'ajouter à toutes celles dont nous avons parlé.

[*Français*]

Le sénateur Carignan : Peut-être que ma question n'était pas suffisamment claire. Étant donné qu'il y a des écarts systématiques, étant donné qu'il y a un centre, entre autres, où aucun contrôle n'a été fait, une personne malveillante au sein de la direction de ce service pourrait, de façon systématique, ne pas pourvoir le poste et dire à un criminel d'utiliser le centre X ou Y, puisqu'il n'y a pas de contrôle la fin de semaine, par exemple.

Ce que vous avez vu m'inquiète énormément. J'imagine que, dans le cadre de votre vérification, étant donné que les objectifs sont liés à la sécurité nationale, cela a attiré votre attention également.

Donc, vous êtes-vous tournée vers la GRC pour qu'elle fasse enquête sur ces gens afin de déterminer s'il y avait un potentiel d'actes criminels occasionné par ce manque de surveillance? Avez-vous transmis des données à la GRC?

[*Traduction*]

Mme Cheng : Je remercie le sénateur d'avoir précisé sa question. Il demande si nous avons transmis à la GRC les informations que nous avons trouvées.

La GRC est intervenue quand nous avons examiné le travail de vérification et quand nous avions des cas de voitures volées, de drogues illégales ou autres, je ne pense pas que les conclusions des vérifications en tant que telles leur aient jamais été transmises pour complément d'enquête. Je demanderai à Nick s'il est en mesure de confirmer.

[*Français*]

M. Swales : Non, nous n'avons pas transmis des données spécifiquement à la GRC. Vous vous demandez si les lacunes en matière de surveillance étaient délibérées.

Senator Carignan: They could be, especially since the objective is national security. These are not simply financial issues.

Mr. Swales: We only found that there was not enough staff in certain locations and over a certain period of time. We did not look for all the reasons.

Senator Carignan: Why not?

Mr. Swales: We realized that there were problems caused by the number of people assigned to the area. The evidence showed that how people were assigned and the decisions made in different regions were the problems rather than a systematic issue.

Senator Carignan: You relied only on the manager's or the supervisor's response without considering that they could be acting in bad faith?

[*English*]

Ms. Cheng: This is not an investigative audit, so it is not a forensic audit as such. We don't go into those levels of detail. My understanding is that whenever we deal with the RCMP or refer cases to the RCMP, they require a lot more evidence for them to take on the case and see if there's a criminal element so that they can follow up.

This is an audit of the administration and the management by the agency. We don't go into that level of detail whereby we would have the information to provide to the RCMP so that they can take it on and follow up.

We haven't seen anything that suggests that any employees were involved in any collusion to provide information to outsiders in order to take advantage of the system.

[*Translation*]

Mr. Swales: Yes, precisely.

[*English*]

The Deputy Chair: Mr. Stock, before I go to round two, I am left a little confused about the good work that you did with respect to housing on military bases. A number of us are quite familiar with the housing. We remember when this housing agency was created. At that time, the agency was authorized to move the rental up to market value in order to fix the units up and to provide market-value housing.

I am finding it difficult to understand where all the rental income goes now because it seems like the agency was transferring, from time to time, that amount to National Defence under its operation and maintenance general appropriation. Can you help me out?

Mr. Stock: I will try, senator.

Le sénateur Carignan : Elles pourraient l'être, d'autant plus que l'objectif est la sécurité nationale. Il ne s'agit pas ici de simples questions financières.

M. Swales : Nous avons seulement constaté que, dans certains endroits et pendant une certaine période de temps, il n'y avait pas suffisamment de personnel. Nous n'avons pas cherché à en connaître toutes les raisons.

Le sénateur Carignan : Pourquoi ne pas l'avoir fait?

M. Swales : En fait, nous avons compris qu'il y avait des problèmes liés au nombre de personnes affectées dans le domaine. Les indices démontraient que c'était la façon dont les personnes étaient affectées et les décisions prises par les différentes régions qui posaient problème, plutôt que quelque chose de systématique.

Le sénateur Carignan : Vous vous êtes seulement fiés à la réponse du dirigeant ou du superviseur sans présumer qu'il pouvait être de mauvaise foi?

[*Traduction*]

Mme Cheng : Notre vérification n'est pas à proprement parler une enquête, encore moins une enquête criminelle. Elle n'est pas aussi détaillée. Pour les cas que nous lui soumettons, la GRC a besoin de dossiers très détaillés avant de s'en charger et voir s'il y a un élément criminel lui permettant de donner suite.

Notre vérification a un caractère administratif et concerne la gestion de l'Agence. Elle n'est pas détaillée au point de nous fournir les renseignements qui permettraient à la GRC de prendre l'affaire en charge.

Nous n'avons rien trouvé qui donnerait à penser que des employés en collusion avec des personnes extérieures auraient pu leur fournir des renseignements sur le système en vue d'en tirer parti.

[*Français*]

M. Swales : Oui, c'est exactement cela.

[*Traduction*]

Le vice-président : Monsieur Stock, avant de passer à la deuxième étape, je reste un tantinet perplexe à propos du bon travail que vous avez fait concernant le logement sur les bases militaires. Nous sommes nombreux à connaître assez bien ce problème. Nous nous souvenons du moment où l'agence de logement a été créée. À cette époque, l'agence était autorisée à aligner les loyers sur les prix du marché pour pouvoir rénover les logements et fournir des logements correspondant aux exigences du marché.

J'ai quelque difficulté à comprendre où s'en vont maintenant tous ces revenus locatifs puisque, apparemment, l'ASFC en transfère, de temps à autre, une partie à la Défense nationale, au chapitre du budget général d'exploitation et de maintenance. Pouvez-vous me tirer d'embarras?

M. Stock : J'essaierai, sénateur.

The amount they receive in rental revenue is not always at market value. In some cases we found that it was below market value.

Three different programs affect the provision of housing to the military. One is relocation, which protects them to a certain extent in terms of fluctuation in value. Another one is the post-living differential, which should provide a certain amount of assistance in terms of affordability, and then there is the housing itself.

The rental revenue they receive is used for maintenance and repair. If they cannot use an amount of that within the year but believe that it would be better to put some of that money toward capital, they can't transfer it themselves. However, within the general appropriation within Defence, Defence can use that amount of their capital to provide that to the agency. So it is more of an internal allocation as opposed to changing things directly between votes of Parliament.

The Deputy Chair: I am glad you got to that. It didn't sound awfully good to me when I read that in paragraph 5.65. Where a piece of operating revenue by the housing group is moved over to DND and then DND, from their budget, finds the money that switches back to them for capital, that seems to me to be getting around the appropriations that honourable senators and members of the House of Commons have voted.

Mr. Stock: We started off having the same concern until we looked into it a little more deeply. In fact, it does not change because it is within the general appropriations of National Defence. It is not actually a transfer from one vote to another but an increase or a reduction within the votes overall within National Defence.

The amount of the revenue that they did not spend was still used by National Defence for maintenance and operating, per se, of the housing to pay for payment in lieu of taxes. It came out of the National Defence side, but it was still in support of the houses.

On the other side, they did have access to capital funds from National Defence's appropriation.

The Deputy Chair: National Defence's appropriation for capital as opposed to operation.

Mr. Stock: That's correct.

The Deputy Chair: They're two different votes.

Mr. Stock: They are two different votes, and they were used according to how it was voted from Parliament.

The Deputy Chair: But why did they have to bribe them? That's what this sounds like: "Well, we'll give you a little money you can apply for a grant in lieu of taxes out of operations, and then you'll

Les revenus locatifs qu'encaisse l'ASFC ne correspondent pas toujours à la valeur du marché. Dans certains cas, nous avons constaté qu'ils y étaient inférieurs.

Trois programmes différents ont une incidence sur la fourniture de logement au personnel militaire. L'un a trait à la réinstallation; il offre une certaine protection contre les fluctuations de prix. L'autre programme concerne les indemnités de vie chère; il vise à rendre le logement plus abordable, enfin il y a le logement lui-même.

Les revenus locatifs de l'ASFC servent à la maintenance et aux réparations. Lorsque l'ASFC ne peut employer une partie de ces fonds durant l'année et estime qu'il vaudrait mieux les transférer à son budget d'immobilisations, elle ne peut opérer ce transfert elle-même. Toutefois, dans le cadre du budget général de la défense, le ministère peut prélever un montant équivalent de son budget d'équipement pour le mettre à la disposition de l'agence. Cela s'apparente donc davantage à une réaffectation interne des fonds qu'à une modification directe des budgets votés par le Parlement.

Le vice-président : Je suis content que vous en veniez à ce point. Ça ne m'a pas fait la meilleure des impressions à la lecture du paragraphe 5.65. Quand l'agence du logement transfère une fraction de son revenu d'exploitation au ministère de la Défense nationale et que le ministère prélève sur son budget un montant équivalent qu'il lui renvoie au titre du budget d'équipement, ça m'a tout l'air d'une manœuvre pour contourner les budgets que les honorables sénateurs et députés ont adoptés.

M. Stock : Nous avions les mêmes préoccupations au départ, avant d'examiner plus à fond la situation. En fait, ça ne change rien puisque ça reste dans le cadre du budget général de la Défense nationale. Il ne s'agit pas vraiment d'un transfert d'un budget à un autre, mais d'une augmentation ou d'une diminution dans le cadre des budgets généraux de la Défense nationale.

La fraction des revenus non dépensés a quand même été utilisée par le ministère au seul titre des opérations et de la maintenance concernant le logement pour couvrir les paiements en remplacement des impôts. C'est sorti du budget de la Défense nationale, mais c'était toujours à l'appui du logement.

Par ailleurs, l'ASFC a eu accès aux fonds destinés à l'équipement inscrits au budget de la Défense nationale.

Le vice-président : Le budget d'immobilisations de la Défense nationale par opposition à son budget d'exploitation.

M. Stock : C'est exact.

Le vice-président : Il s'agit de deux budgets différents.

M. Stock : Il s'agit de deux budgets différents qui ont été employés conformément aux vœux du Parlement qui les a adoptés.

Le vice-président : Mais pourquoi ont-ils dû leur offrir un pot-de-vin? Voici de quoi ça a l'air : « On va vous donner un peu d'argent que vous pourrez employer comme subvention à la place

free up some money for us out of your capital budget to do what Parliament had already voted for in capital." Am I missing something here?

Mr. Stock: It is a convoluted process, I grant you that, but it is still a way that the agency tried to devote something toward the capital side. I would not repeat the bribe aspect. It is more of a negotiation between the agency —

The Deputy Chair: An inducement.

Ms. Cheng: Mr. Chair, if I may, DND is such a large entity. The housing authority is a small component within that special operating agency. DND has this big bucket of operational O&M money and also capital money. In essence, at the end of the day, DND's spending is still in line with those votes. However, within that a lot of the smaller organizations are able to swap money internally so that overall it does not upset the balance that Parliament has voted to give to DND. They're living within their O&M budget, within their capital budget, but in there they're trying to trade.

When you look at the reason for it, we don't read anything negative into it. It shows the scenario of a housing agency struggling to say, "Here is my source of funds. How can I best make use of that to upgrade the housing that some of you actually have seen? How do we try to make best use of that money?" They're looking for as much leeway within the system of parliamentary votes to help them do that.

One of the things I believe the team has looked at is they're also trying to see if there's any way to give them multi-year funding for capital. If they can get that, it would be a lot more helpful than this January funding to try to do construction.

The Deputy Chair: Mr. Stock's investigative reporting here has been reported to Treasury Board; do they understand what is going on here?

Mr. Stock: This was within the National Defence portfolio audit.

The Deputy Chair: Yes.

Mr. Stock: Other than our regular briefings with Treasury Board Secretariat personnel, we would have advised them and they would have read the report.

The Deputy Chair: Time doesn't permit to go further into this, but I want to express my concern that I see a little red flag here. If you go back and think about this and feel you can enlighten me more on this matter by writing a response, I would certainly appreciate that.

des taxes provenant des opérations, et puis vous débloquerez des fonds pour nous, prélevés sur votre budget d'équipement, pour faire ce que le Parlement avait déjà prévu dans le budget d'équipement qu'il a adopté. » Il y a quelque chose qui m'échappe ici?

M. Stock : C'est un processus alambiqué, je vous l'accorde, mais c'est par ce moyen que l'agence a essayé de financer en partie ses dépenses d'équipement. Je ne reprendrais pas l'aspect relatif aux pots-de-vin. Il s'agit plutôt d'une négociation entre l'ASFC...

Le vice-président : Une incitation.

Mme Cheng : Monsieur le président, avec votre permission, le ministère de la Défense nationale est une institution tellement grosse. L'agence de logement est un petit élément de cet organisme de service spécial. Le ministère puise dans un grand réservoir où se trouvent ses fonds de maintenance et d'exploitation et aussi ses fonds d'équipement. En fin de compte, les dépenses du ministère sont conformes aux budgets. Mais, dans les limites des budgets du ministère bon nombre d'organismes plus petits sont en mesure de procéder à des transferts internes de fonds tout en respectant l'équilibre entre les budgets que le Parlement a accordés à la Défense nationale. Sans sortir du cadre du budget d'exploitation ni du budget d'immobilisations, on cherche à négocier.

Quand on cherche à s'expliquer le pourquoi, on ne trouve rien de mal à cela. Le scénario qui apparaît, est celui d'une agence de logement qui se débat et dit : « Voici ma source de financement. Comment l'employer au mieux pour rénover les logements que certains d'entre vous avez vus? Comment employer au mieux ces fonds? » Elle cherche à avoir le plus de latitude possible dans le cadre du système des budgets parlementaires pour atteindre cet objectif.

L'équipe de vérificateurs s'est également penchée sur un autre problème concernant les efforts de l'agence pour essayer d'obtenir un financement pluriannuel au titre des immobilisations. Si elle peut l'obtenir, ça lui sera bien plus utile qu'une entrée de fonds en janvier pour financer la construction de logements.

Le vice-président : Le compte rendu d'enquête de M. Stock a été communiqué au Conseil du Trésor; celui-ci comprend-t-il ce qui se fait ici?

M. Stock : Cela s'est fait dans le cadre de la vérification du portefeuille de la Défense nationale.

Le vice-président : Oui.

M. Stock : En dehors de nos réunions régulières d'information, nous avons pu conseiller le personnel du Secrétariat du Conseil du Trésor qui a sans doute lu le rapport.

Le vice-président : Le temps nous manque pour poursuivre l'examen de cette question, mais je voudrais signaler ma préoccupation et agiter un petit drapeau rouge. Si, dans le cours de vos réflexions, vous pensez pouvoir m'éclairer davantage sur le sujet en envoyant une réponse écrite, je vous en serais reconnaissant.

Senator White: Since 2004, CBSA has literally gone from being a revenuer to being one of the largest police agencies in the country. It follows a little in line with oversight because realistically everybody has made recommendations in the past decade that would have changed some parts of what CBSA has done.

Did you make a recommendation that legislation be changed so they could actually search on exportation rather than have to have reasonable or probable grounds?

Ms. Cheng: We rarely — and I wouldn't want to say never — make a recommendation to say that the legislation should be changed. We usually point to problem/outcome/impact of existing legislation and allow management and the government to decide that legislation should be changed in whatever fashion.

That's not the way we tend to approach as a solution.

Certainly, if it's a limitation, in this particular case we actually went as far as saying that it is a limitation. It is up to management to decide whether they want to live with it or that they should make a case to make the changes and amendments necessary to give the authority required for them to discharge its mandate.

Senator White: That was not really my question, so I will continue, Mr. Chair.

Some countries have gone to what is considered to be "trusted partners"; in other words, a highly bondable company that CBSA or the equivalent in Australia, for example, would allow. If you put your sea container through that company, they have already been cleared. They actually do the search on the sea container so that the border agency doesn't have to or seldom does.

Did you look at any other models outside of Canada and make any recommendations? And I apologize; I didn't look for it here.

Mr. Swales: Those exist primarily on the import side in Canada.

Senator White: They do.

Mr. Swales: So we didn't look at them in the context of this audit.

Senator Ngo: I want to follow up on the question from Senator White regarding housing. Did the OAG report uncover the main reason why the Canadian Armed Forces will use military housing even if private housing is available?

Mr. Stock: No, we did not. We sought answers, but we did not receive an explanation. Part of this was that no agency has actually provided the value of housing in the last couple of years

Le sénateur White : Depuis 2004, l'ASFC est passée de la condition d'agent du fisc à celle d'un des plus importants corps policier du pays. Ça va dans le sens souhaité par les vérificateurs parce que, au cours des 10 dernières années, presque tout le monde a fait des recommandations visant à modifier telle ou telle partie des activités de l'ASFC.

Avez-vous recommandé que l'on modifie la législation pour permettre à l'agence d'enquêter sur les exportations plutôt que d'exiger d'elle qu'elle ait un motif raisonnable ou probable d'enquêter?

Mme Cheng : Il n'arrive que rarement — pour ne pas dire jamais — que l'on recommande de modifier la législation. En général, on signale des problèmes, des conséquences, des incidences de la législation en vigueur et on laisse à la direction et au gouvernement le soin de décider si la législation doit être modifiée d'une manière ou d'une autre.

Ce n'est pas dans cette direction que l'on cherche une solution à nos problèmes.

Certes, si une contrainte semble imputable à la législation, nous n'hésitons pas à le signaler comme nous l'avons fait dans ce cas. C'est à la direction de décider s'il convient de faire avec ou plutôt de défendre la thèse que des changements et des modifications sont nécessaires dans les compétences attribuées à l'agence pour qu'elle puisse s'acquitter de son mandat.

Le sénateur White : Ce n'était pas vraiment la question que je posais, aussi vais-je poursuivre, monsieur le président.

Certains pays se sont adressés à des « partenaires fiables » par quoi il faut entendre une entreprise présentant des garanties solides qui pourraient être agréée par l'ASFC ou son équivalent en Australie. Si vous confiez votre conteneur maritime à cette société, il a déjà été contrôlé. C'est la compagnie qui effectue le contrôle du conteneur, ce qui évite à l'agence des frontières d'avoir à le faire ou ce qu'elle ne fait que rarement.

Avez-vous examiné les modèles retenus en dehors du Canada et présenté des recommandations? Et je vous prie de m'excuser, mais je n'ai pas cherché ici.

M. Swales : De telles sociétés existent au Canada surtout pour les importations.

Le sénateur White : C'est exact.

M. Swales : Nous ne nous y sommes pas intéressés, de ce fait, dans le cadre de notre vérification.

Le sénateur Ngo : Je souhaite revenir sur la question abordée par le sénateur White concernant le logement. Est-ce que le rapport du Vérificateur général a révélé le motif pour lequel les forces armées canadiennes ont recours à des logements militaires tandis que des logements privés sont disponibles?

M. Stock : Non. Nous avons cherché des réponses, mais on ne nous a pas donné d'explication. C'est en partie due au fait qu'aucune agence ne fournit d'estimations de la valeur des

since the Canadian Mortgage and Housing Corporation has not provided that information. They have updated what they could, but no explanation has been provided.

Certain base commanders have certain views as to whether their members should be living on base or not. There are many members that need to live on base, for instance, if they need to be able to be in the air in 15 minutes, they need to be close by, living on base. From the operational point of view, there are requirements.

Bases have change considerably over time. For example, five years ago, Petawawa may have been in a position where housing might not have been needed. But with the medium heavy-lift helicopters, the Chinooks, being based at Petawawa now, they have needed housing.

There are long-term considerations as to whether to keep the housing they have and whether or not they prefer to have the members living on base or in the community.

Senator Mitchell: You are not suggesting that if there were vacant military houses on the base that somehow they shouldn't be available and that a family should be encouraged to go off base? You're saying that if everything is filled up, don't build new houses; try to use the private sector?

Mr. Stock: If the private sector can provide it, government policy is that the private sector should provide it unless there are operational reasons otherwise.

Senator Mitchell: Is there any argument to be made for a private sector contract to manage military housing?

Mr. Stock: I'm sure there is, but we did not consider that or recommend it.

The Deputy Chair: You just want that former residence of yours at Base Gagetown to be fixed up; right?

That concludes our meeting with the Auditor General's office. I hope you will take back our regards to the Auditor General. I'm sorry he couldn't make it, but we're actually pleased he didn't make it because we had the chance to meet with you again. Thank you very much, Ms. Cheng, Mr. Swales and Mr. Stock.

Colleagues, we will suspend for one minute. I have a little bit of information to pass on to you and then receive any input you might have.

(The committee continued in camera.)

logements depuis que la Société canadienne d'hypothèques et de logement a cessé de le faire, il y a deux ans. Elle a actualisé les données comme elle le pouvait, mais on ne nous a donné aucune explication.

Certains commandants de bases ont leur propre idée sur la question de savoir si leurs personnels devraient vivre sur la base ou non. Nombreux sont les militaires qui ont besoin de vivre sur la base, par exemple, si l'on attend d'eux qu'ils puissent être à bord d'un avion dans les 15 minutes, il faut qu'ils soient à proximité, qu'ils vivent sur la base. Du point de vue opérationnel, il y a des exigences.

Les bases ont beaucoup changé au fil du temps. Il y a cinq ans, par exemple, on n'avait peut-être pas besoin de logements des familles à Petawawa. Mais maintenant que les hélicoptères de transport moyen à lourd, les Chinook, y sont basés, le besoin de logements existe.

Des considérations à long terme entrent en jeu au moment de décider s'il faut garder les logements dont on dispose et s'il vaut mieux que le personnel vive sur la base ou dans la communauté.

Le sénateur Mitchell : Vous n'êtes pas en train de laisser entendre que, s'il y avait des logements militaires vacants sur la base, ils pourraient, pour une raison ou une autre, ne pas être disponibles et qu'une famille pourrait se voir encouragée à vivre en dehors de la base? Vous dites que si tout est complet, il ne faut pas construire de nouvelles maisons, qu'il faut essayer de recourir au secteur privé?

M. Stock : Si le secteur privé peut y pourvoir, la politique du gouvernement veut que l'on s'adresse au secteur privé, sauf contre-indication pour des motifs opérationnels.

Le sénateur Mitchell : Y a-t-il des arguments en faveur de la gestion sous contrat par le secteur privé des logements militaires?

M. Stock : Je suis certain qu'il y en a, mais nous n'avons pas examiné la question et nous n'avons pas fait de recommandation dans ce sens.

Le vice-président : Tout ce que vous voulez, c'est que votre ancienne résidence sur la base de Gagetown soit retapée; est-ce que je me trompe?

Voilà qui conclut notre réunion avec le Bureau du vérificateur général. Je vous prie de transmettre nos salutations au vérificateur général. Je suis désolé qu'il ait eu un empêchement, mais d'un autre côté, cela nous aura donné le plaisir de vous revoir. Merci beaucoup, madame, merci monsieur Swales et monsieur Stock.

Chers collègues, nous suspendons nos travaux un instant. J'ai quelques informations à vous communiquer, après quoi vous pourrez me faire part de vos commentaires.

(La séance se poursuit à huis clos.)

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

OTTAWA, Monday, March 7, 2016

The Standing Senate Committee on National Security and Defence met this day at 12:57 p.m. to examine and report on Canada's national security and defence policies, practices, circumstances and capabilities; and to study and report on security threats facing Canada.

Senator Daniel Lang (*Chair*) in the chair.

[*English*]

The Chair: I'd like to welcome you all to the Standing Senate Committee on National Security and Defence for Monday, March 7, 2016.

Before we begin, I'd like to introduce the people around the table. My name is Dan Lang, senator for Yukon, and on my immediate left is the clerk of the committee. I'd like to invite each senator to introduce themselves and state the region they represent, starting with our deputy chair.

Senator Day: Joseph Day from New Brunswick.

[*Translation*]

Senator Carignan: Good afternoon. I am Senator Claude Carignan, Leader of the Opposition.

Senator Dagenais: Senator Jean-Guy Dagenais, Quebec.

[*English*]

Senator Kenny: Colin Kenny, Ontario.

Senator White: Vernon White, Ontario.

Senator Beyak: Senator Lynn Beyak, Ontario.

Senator Ngo: Senator Ngo, Ontario.

The Chair: Today we'll be hearing from four panels and then go in camera to consider future business of the committee.

Joining us on panel 1 is Michel Coulombe.

Welcome back to the committee. We're pleased to have you here so you can update Canadians on the threats to the security of Canada.

The committee was informed in late 2014 that over 318 Canadians were radicalized and involved in terrorist activities; 145 of these Canadians were overseas, 93 Canadians were trying to leave the country and 80 had returned. One year ago, when Mr. Coulombe appeared before this committee, he informed us that the numbers had increased. Last week, he informed the public that 60 more Canadian foreign fighters had been identified in terrorist acts and returned back to Canada.

OTTAWA, le lundi 7 mars 2016

Le Comité sénatorial permanent de la sécurité nationale et de la défense se réunit aujourd'hui, à 12 h 57, dans le but d'étudier, afin 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 Daniel Lang (*président*) occupe le fauteuil.

[*Traduction*]

Le président : Je vous souhaite tous la bienvenue à la réunion du Comité sénatorial permanent de la sécurité nationale et de la défense du lundi 7 mars 2016.

Avant de commencer, j'aimerais présenter les personnes qui se trouvent autour de la table. Je m'appelle Dan Lang, sénateur du Yukon, et, tout juste à ma gauche, se trouve le greffier du comité. J'aimerais inviter chaque sénateur à se présenter en précisant la région qu'il représente. Nous allons commencer par le vice-président.

Le sénateur Day : Joseph Day, du Nouveau-Brunswick.

[*Français*]

Le sénateur Carignan : Bonjour. Je suis le sénateur Claude Carignan, leader de l'opposition.

Le sénateur Dagenais : Sénateur Jean-Guy Dagenais, du Québec.

[*Traduction*]

Le sénateur Kenny : Colin Kenny, de l'Ontario.

Le sénateur White : Vernon White, de l'Ontario.

La sénatrice Beyak : Sénatrice Lynn Beyak, de l'Ontario.

Le sénateur Ngo : Sénateur Ngo, de l'Ontario.

Le président : Nous rencontrons aujourd'hui quatre groupes de témoins, puis nous poursuivrons à huis clos pour étudier les travaux futurs du comité.

Notre premier témoin est Michel Coulombe.

Nous sommes ravis de vous accueillir de nouveau et heureux que vous soyez là afin de mettre les Canadiens au courant des menaces qui pèsent sur la sécurité du Canada.

À la fin de 2014, le comité a été informé du fait que plus de 318 Canadiens étaient radicalisés et participaient à des activités terroristes. Du nombre, 145 se trouvaient à l'étranger, 93 tentaient de quitter le pays, et 80 étaient revenus ici. Il y a un an, lorsque M. Coulombe a comparu devant le comité, il nous a dit que les chiffres avaient augmenté. La semaine dernière, il a dit publiquement que 60 combattants canadiens à l'étranger de plus avaient été identifiés dans le cadre d'actes terroristes et étaient de retour au Canada.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Mr. Coulombe, this update was welcomed by our committee, and we hope CSIS continues to provide such updates to Canadians on a regular, quantitative and unambiguous fashion, as recommended by this committee in our report of last July.

Mr. Coulombe, it seems like yesterday when we experienced the attack on Parliament and Canadians witnessed the murders of Warrant Officer Vincent and Corporal Cirillo. Since then, Canadians have been made aware of terrorist activities in almost every provincial jurisdiction, and we have also witnessed attacks in Paris, Brussels, San Bernardino and Burkina Faso where Canadians lost their lives. Just today, reporter Stewart Bell reports the death of another Canadian jihadist in Libya.

The situation of Canadians, dual-nationals and the radicalism movement remains a significant concern for this committee and all Canadians, and we're looking forward to your comments. Please proceed.

[*Translation*]

Michel Coulombe, Director, Canadian Security Intelligence Service: Good afternoon, honourable senators. Thank you for your invitation today to discuss threats to the security of Canada. I will focus my remarks on the current security environment, and in particular, on the evolving threat to Canada posed by terrorism.

[*English*]

Mr. Chair, as Director of CSIS, it is my job to give the best assessment of the nature and the scope of the terrorist threat environment. I will not overstate the terrorist threat, but I feel strongly that we must resist complacency in the face of this complex and evolving environment. Minimizing this threat would be to gamble with the security of Canadians.

There has been a great deal of discussion about the impact of the attacks of October 2014. There are some who might say that this event was limited in scale and that, although a very tragic event, it should be put in perspective as two separate murders, and that the terrorist threat is being inflated.

I disagree with this analysis because it ignores important factors. First of all, we must always be mindful of the somewhat less visible but very significant impacts beyond the human tragedy that terror attacks have on our nation's psyche and our sense of security.

Second, as you are well aware, terrorist attacks also have a tremendous impact on the economy. As an example, given the significance of our cross-border trade, we are all aware of what the immediate impact of an attack could look like if the result was a lack of confidence among our partners in the United States.

Monsieur Coulombe, cette mise à jour avait été saluée par notre comité, et nous espérons que le SCRS continuera à fournir régulièrement aux Canadiens de telles mises à jour quantitatives et sans ambiguïté, comme nous l'avions recommandé dans notre rapport de juillet dernier.

Monsieur Coulombe, c'est comme si c'était hier que s'est produite l'attaque sur le Parlement et que les Canadiens ont été témoins des meurtres de l'adjudant Vincent et du caporal Cirillo. Depuis, les Canadiens ont été mis au courant d'activités terroristes dans presque chaque administration provinciale, et nous avons aussi été témoins des attaques à Paris, à Bruxelles, à San Bernardino et au Burkina Faso, où des Canadiens ont perdu la vie. Encore aujourd'hui, le journaliste Stewart Bell a signalé le décès en Libye d'un autre djihadiste canadien.

La situation des Canadiens, des personnes ayant une double nationalité et du mouvement de radicalisation reste une préoccupation importante du comité et de tous les Canadiens, et nous attendons avec impatience vos commentaires. Veuillez commencer.

[*Français*]

Michel Coulombe, directeur, Service canadien du renseignement de sécurité : Honorables sénateurs, bonjour. Je vous remercie de m'avoir invité aujourd'hui pour discuter des menaces qui pèsent sur la sécurité du Canada. Mon allocution portera essentiellement sur le contexte actuel de la sécurité et, en particulier, sur l'évolution de la menace que le terrorisme fait peser sur le Canada.

[*Traduction*]

Monsieur le président, à titre de directeur du SCRS, il m'appartient de vous présenter la meilleure évaluation possible de la nature et de l'ampleur de la menace terroriste. Sans vouloir exagérer cette menace, je crois fermement qu'il ne faut pas relâcher la vigilance dans ce contexte complexe et en évolution et qu'il est risqué pour la sécurité des Canadiens de minimiser cette menace.

Les répercussions des attaques d'octobre 2014 ont fait l'objet de nombreux débats. Certains diront que ces événements étaient d'une ampleur assez limitée, et que, quoique très tragiques, il convient de les ramener à de plus justes proportions, c'est-à-dire de les voir comme deux meurtres distincts, et que la menace terroriste n'est pas aussi grave qu'on le prétend.

Je pense que cette analyse est erronée, car elle fait fi de facteurs importants. Premièrement, nous ne devons jamais oublier les répercussions très importantes, mais moins visibles, allant au-delà de la tragédie humaine, que les attentats terroristes ont sur l'âme de la nation et sur notre sentiment de sécurité.

Deuxièmement, comme vous le savez très bien, les attentats terroristes ont également une profonde incidence sur l'économie. Par exemple, vu l'importance du commerce transfrontalier, nous sommes tous conscients des répercussions immédiates qu'un attentat pourrait avoir s'il parvenait à miner la confiance de nos partenaires aux États-Unis.

Third, this analysis does not take account of the potential terrorist attacks in Canada that have been pre-empted, and those who have been convicted of terrorism-related criminal activity.

In addition, beyond our borders, we only need to look at the recent terror attacks in Paris or San Bernardino; in Jakarta, where a Canadian was killed; or in Burkina Faso, where six Canadians lost their lives, to realize that terrorism has a global reach and that we, as a country, are not immune to its impacts. And for every terror attack that takes place in Canada or abroad, many more are disrupted.

As such, terrorism remains the service's investigative priority. All available expertise and resources are being leveraged to address the significant operational tempo.

[*Translation*]

As you will be aware, honourable senators, conflicts abroad, particularly those in Iraq and Syria, continue to shape the nature of the terrorism threat to Canada. We have never before faced a threat of the scope, scale, and complexity as that posed by extremists inspired by the violent ideologies of ISIL or al Qaeda.

Canadians with extremist views continue to seek to undertake terrorist activity, whether they remain in Canada or travel abroad. While the terrorist traveller phenomenon is not new to Canada, the volume of threats, the speed at which they evolve, and the use of technology and social media, has created significant investigative, technical, and analytical challenges for the service.

ISIL, in particular, has developed a sophisticated and effective social media presence and has succeeded in recruiting thousands of individuals to travel to Syria from all corners of the globe. ISIL also calls followers to perpetrate attacks in their own countries or to facilitate the terrorist activities of others.

Canadians are among this group. The service is currently aware of approximately 180 individuals who have an access to Canada, who are engaged in terrorist activity abroad. Of these, around 100 or so are believed to be in Turkey, Syria, or Iraq. The activities of these extremist travellers vary widely, ranging from paramilitary activity, training, and logistical support, to terrorist fundraising and studying at extremist Islamist madrasas. The participation of Canadians in these conflicts is destabilizing and harmful to the countries in which they operate, and Canada has an international obligation to prevent and deter terrorist travel.

The service is also aware of around 60 returnees. Extremists returning to Canada have the potential to pose significant threats to our national security. However, I must be clear with the

Troisièmement, cette façon de penser ne tient pas compte des complots terroristes qui ont été déjoués au Canada et des personnes reconnues coupables par les tribunaux d'infractions criminelles liées au terrorisme.

De plus, à l'étranger, il suffit de penser aux récentes attaques terroristes à Paris, à San Bernardino, à Jakarta, où un Canadien a été tué, ou au Burkina Faso, où six Canadiens ont perdu la vie, pour se rendre compte que le terrorisme a une portée mondiale et que nous, en tant que pays, ne sommes pas à l'abri de ses répercussions. Toutefois, malgré tous les attentats terroristes perpétrés au Canada ou ailleurs, un plus grand nombre encore sont perturbés.

Ainsi, les enquêtes sur le terrorisme demeurent la priorité du Service, qui met à profit l'ensemble de son savoir-faire et de ses ressources pour suivre le rythme effréné des opérations.

[*Français*]

Comme vous le savez sans doute, honorables sénateurs, les conflits à l'étranger, notamment ceux qui font rage en Irak et en Syrie, continuent de définir la menace terroriste qui pèse sur le Canada. Les extrémistes inspirés par les idéologies violentes de l'État islamique en Irak et au Levant ou Al-Qaïda font peser sur nous une menace d'une portée, d'une ampleur et d'une complexité sans précédent.

Des Canadiens aux idées extrémistes cherchent toujours à mener des activités terroristes, que ce soit en restant au Canada ou en se rendant à l'étranger. Même si le phénomène des terroristes voyageurs n'est pas nouveau au Canada, le nombre de menaces, la vitesse à laquelle elles évoluent et l'utilisation de la technologie et des médias sociaux rendent les enquêtes plus difficiles pour le service et lui posent d'importants problèmes sur les plans technique et analytique.

L'État islamique en Irak et au Levant, en particulier, a réussi, par son utilisation habile et efficace des médias sociaux, à inciter des milliers d'individus de partout dans le monde à se rendre en Syrie et en Irak. Il appelle aussi ses partisans à perpétrer des attentats dans leur pays d'origine ou à aider d'autres personnes à mener des activités terroristes.

Ce groupe compte des Canadiens. À l'heure actuelle, le service sait qu'environ 180 individus ayant des liens avec le Canada mènent des activités terroristes à l'étranger. Une centaine d'entre eux se trouveraient en Turquie, en Syrie ou en Irak. Les activités de ces voyageurs extrémistes sont extrêmement variées. Certains participent à des opérations paramilitaires ou suivent un entraînement, alors que d'autres assurent un soutien logistique, recueillent des fonds ou étudient dans des madaris islamistes extrémistes. Comme la participation des Canadiens à ces conflits nuit aux pays où ils se trouvent et les déstabilise, le Canada a l'obligation internationale d'empêcher les voyages à des fins terroristes.

Le service est aussi au courant du retour d'une soixantaine d'individus. Les extrémistes qui reviennent au Canada peuvent représenter une menace grave pour la sécurité nationale. À cet

committee when I say "potential," as returnees may respond in a number of different ways — from returning to normality, to radicalizing others, to financing or facilitating the travel of others, to planning attacks here.

[*English*]

Senators, I have referenced numbers of terrorist travellers in the past, as I believed at that time it was important to give senators and the public a sense of the scale of this phenomenon — that we were speaking of hundreds of people, not thousands. I am providing you with an update on the current numbers today.

However, I must emphasize that the numbers of "travellers" or "returnees" do not adequately capture the scale of this threat. Individuals who have never travelled — whether they aspire to or have been prevented from travelling or, for a number of reasons, choose to remain in Canada — and are engaged in threat-related activities at home are not included.

Members must understand that every extremist prevented or deterred from travelling abroad may become an individual at home who requires ongoing investigation. Both of the perpetrators of the separate October 2014 attacks desired to leave Canada but were unable to do so.

I want to assure honourable members of this committee and all Canadians that CSIS is taking every step to identify terrorists and their activities. Terrorist activity, whether travelling abroad to participate in a regional conflict, engaging in an attack plot or facilitating the activities of someone else, is rarely sudden or spontaneous, and it typically requires financial resources, planning and logistics. We are continually refining and improving our methods of identifying when an individual is moving from holding extremist ideas to taking action.

Our challenge is not just to detect complex plots over time involving multiple players, but also to identify the simpler, smaller-scale versions of the threat that often can be difficult to detect. In every case, we share information with our domestic and foreign partners, as appropriate.

Mr. Chair, while the current focus is, of necessity, terrorism and extremism, other threats to Canada's national security, such as espionage, foreign interference and cyberattacks, persist.

égard, je dois toutefois préciser qu'ils peuvent réagir de bien des façons différentes, par exemple, reprendre une vie normale, tenter de radicaliser d'autres personnes ou financer et faciliter leurs voyages, ou encore planifier des attentats ici.

[*Traduction*]

Honorables sénateurs, j'ai déjà parlé, par le passé, du nombre de voyageurs terroristes parce que, à l'époque, je croyais qu'il était important de donner aux membres du comité et au public une idée de l'ampleur de ce phénomène : nous parlions de centaines et non de milliers de personnes. Je vous fais part aujourd'hui des statistiques actuelles.

Cependant, je dois insister sur le fait que le nombre des « voyageurs » ou des « individus qui sont revenus au pays » ne permet pas de bien saisir toute l'ampleur de cette menace. Ne sont pas inclus dans ce nombre les individus qui ne sont jamais partis à l'étranger — qu'ils aspirent à le faire, aient été empêchés de voyager ou aient choisi de rester au Canada pour un certain nombre de raisons — et qui se livrent à des activités liées à la menace au pays.

Les membres du Comité doivent comprendre que chaque extrémiste que l'on empêche ou dissuade de partir à l'étranger peut devenir un individu qu'il faut surveiller de près. Les auteurs des deux attaques d'octobre 2014 souhaitaient quitter le Canada, mais n'ont pas été en mesure de le faire.

Je tiens à assurer les honorables membres du comité et tous les Canadiens que le SCRS prend toutes les mesures nécessaires pour repérer les terroristes et leurs activités. Les activités terroristes, que ce soit partir à l'étranger pour prendre part à un conflit régional, participer à un projet d'attentat ou faciliter les activités de quelqu'un d'autre, sont rarement menées de façon soudaine ou spontanée. En règle générale, elles nécessitent beaucoup de ressources financières, de planification et de soutien logistique. Le Service ne cesse de perfectionner ses méthodes afin d'en arriver à cerner le moment où un individu décide d'aller au-delà de ses idées extrémistes et de passer à l'acte.

Le défi consiste non pas à détecter uniquement les projets d'attentat complexes qui sont élaborés sur une longue période et qui font appel à de nombreux acteurs, mais aussi à identifier les menaces plus simples et de moindre envergure qui sont presque impossibles à déceler. Dans chaque cas, le Service échange des informations avec ses partenaires au pays et à l'étranger, s'il y a lieu.

Monsieur le président, même si, à l'heure actuelle, le Service doit nécessairement concentrer ses efforts sur le terrorisme et l'extrémisme, d'autres menaces pèsent toujours sur la sécurité nationale du Canada, comme l'espionnage, l'ingérence étrangère et les cyberattaques.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*Translation*]

Canada continues to be the target of malicious cyberattacks by foreign entities. These attacks have become a tool of choice for a range of hostile actors including both state and non-state actors because they are efficient, cost effective, and most importantly deniable.

A number of foreign states continue to be involved in traditional espionage and foreign interference activities as they attempt to gather political, economic, and military information in Canada through clandestine means. Such states will pursue their own national interests through covert means, targeting Canadian businesses, political institutions, and members of the diaspora. And Canada also remains a target for illicit procurement efforts by those pursuing advanced technology including weapons of mass destruction.

In short, national security threats are increasing across the spectrum. And while the immediacy of the threat of terrorism requires the focus of a significant portion of our resources, we must be vigilant against other long-term threats.

[*English*]

Our continued cooperation with other Government of Canada departments and agencies, as well as with our foreign partners, is and will continue to be integral to mitigating both domestic and international threat environments.

Honourable senators, the service is continually reassessing our operation and the security measures we have in place to respond to the dynamic and complex security environment.

With that, Mr. Chair, I conclude my remarks.

[*Translation*]

I welcome any questions.

[*English*]

The Chair: Thank you very much, Mr. Coulombe. I appreciate your opening remarks. On behalf of all members of the committee, I want to say we appreciate the agency and the work you do on behalf of Canadians. The number of plots that you have been able to identify and negate over the last number of years is to the credit of the men and women that serve with you and with the other law enforcement agencies.

You stated in your opening remarks stated you were happy to provide us "with an update on the current numbers today."

I'm not clear in respect to the exact the scope of the question of Canadian jihadists who are involved in various activities, whether it be here in Canada. The last time you were here in 2014, you clearly identified the number of individuals who were attempting

[*Français*]

Le Canada continue effectivement d'être la cible de cyberactivités malveillantes de la part d'entités étrangères. Ces activités sont devenues un instrument de choix pour un éventail d'acteurs étatiques et non étatiques hostiles, parce qu'elles sont efficaces, peu coûteuses et, plus important encore, faciles à nier.

De nombreux États étrangers continuent de se livrer à des activités traditionnelles pour tenter de recueillir, par des moyens clandestins, des informations politiques, économiques et militaires au Canada. Ces États cherchent à promouvoir leurs propres intérêts nationaux en exploitant secrètement les entreprises et les institutions politiques canadiennes ainsi que les membres de leurs communautés ethniques. Le Canada demeure aussi la cible d'activités d'approvisionnement illicites menées par des entités qui cherchent à se procurer des technologies de pointe, y compris des armes de destruction massive.

Bref, les menaces pour la sécurité nationale augmentent dans tous les secteurs. Même si l'imminence de la menace terroriste oblige le service à y consacrer une partie importante de ses ressources, il doit continuer d'être à l'affût d'autres menaces à long terme.

[*Traduction*]

Le Service doit absolument continuer de collaborer avec les autres ministères et organismes fédéraux et ses partenaires à l'étranger pour atténuer les menaces à l'échelle nationale et internationale.

Honorables sénateurs, le Service réévalue continuellement ses opérations et les mesures de sécurité qu'il a mises en place pour faire face au contexte de la sécurité complexe et en constante évolution.

Sur ce, monsieur le président, je termine mon allocution.

[*Français*]

Je suis prêt à répondre à vos questions.

[*Traduction*]

Le président : Merci beaucoup, monsieur Coulombe. J'ai bien aimé votre déclaration préliminaire. Au nom de tous les membres du comité, je tiens à dire que nous apprécions le Service et sommes reconnaissants du travail que vous faites au nom des Canadiens. Le nombre de complots que vous avez réussi à découvrir et à empêcher au cours des dernières années est tout à l'honneur des hommes et des femmes qui travaillent avec vous et au sein des autres organismes d'application de la loi.

Vous avez dit dans votre déclaration préliminaire que vous étiez heureux de nous « faire part aujourd'hui des statistiques actuelles ».

Je ne connais pas exactement la portée de la question liée aux djihadistes canadiens qui sont impliqués dans diverses activités, que ce soit ici, au Canada, ou ailleurs. Durant votre dernière visite, en 2014, vous avez mentionné le nombre précis de

to leave the country, to your knowledge, and I believe that number was in the neighbourhood of 90. Those actually involved overseas were 145, and the balance of 80 had returned.

Perhaps you could clarify for the record exactly what we're facing in regard to those three categories. For example, the 60 that you identified two weeks ago, does that mean now that there are 140 returnee jihadists in Canada?

Mr. Coulombe: Regarding the returnees, it's not 60 additional. In fact, the 80 went down to 60. There are a number of explanations for this.

People have actually come back and then returned. People were counted as returning, but after further investigation and receiving additional information, we realized that in fact when they were overseas, they were not involved in threat-related activities.

There are a number of reasons why that number fluctuated. It's not 60 additional. We have now 60 returnees that the service is aware of.

About a year ago, we were talking about 140. That number is now up to 180 people with a nexus to Canada that the service is aware are overseas, involved in threat-related activities. Of that 180, around 100 of them are in Iraq and/or Syria.

The Chair: How many Canadians looking to leave the country have been identified?

Mr. Coulombe: That's a number I don't have with me, but I would say it's probably around the same range as a year ago, 90 to 100. Again, it's very difficult. We learned of a number of people leaving after the fact, so that number does not capture the actual scale of the phenomenon.

The Chair: Thank you, Mr. Coulombe. I think that clarified the record to some degree.

[*Translation*]

Senator Dagenais: Thank you very much for your presentation, Mr. Coulombe. I would like to talk about fighters who come back from abroad. I know that some details must remain confidential. However, what resources are earmarked for the surveillance of fighters who have come back from abroad? What does this represent, cost-wise, in your budgets?

Mr. Coulombe: I do not have specific information on the number of returns. Approximately 55 per cent of our operational budget goes towards fighting terrorism.

What one must understand is that the 60 individuals who have returned are a potential threat. Some come back to their normal lives. After a certain period of time, we deem them no longer to be a threat. Others will continue to be involved in a number of ways.

personnes qui, à votre connaissance, tentaient de quitter le pays, et je crois qu'il y en avait environ 90. En outre, 145 étaient impliqués dans des activités à l'étranger, et 80 autres étaient de retour au pays.

Pouvez-vous décrire avec exactitude pour le compte rendu la situation à laquelle nous sommes confrontés actuellement relativement à ces trois catégories. Par exemple, vous avez identifié 60 personnes il y a deux semaines; cela signifie-t-il qu'il y a maintenant 140 djihadistes revenus au Canada?

M. Coulombe : Pour ce qui est des personnes qui sont revenues au pays, il n'y en a pas 60 de plus. En fait, il y en avait 80, et il y en a maintenant 60. Cela s'explique de diverses manières.

En fait, des gens sont revenus, puis sont retournés là-bas. On avait déterminé qu'ils étaient revenus, mais après une enquête plus poussée et la réception de renseignements supplémentaires, nous avons constaté que, en fait, ils étaient à l'étranger et qu'ils ne s'adonnaient pas à des activités menaçantes.

Il y a un certain nombre de raisons pour lesquelles le nombre fluctue. Il n'y en a pas 60 de plus. Le Service connaît actuellement 60 personnes qui sont revenues au pays.

Il y a environ un an, on disait qu'il y en avait 140. Le Service sait maintenant qu'il y a jusqu'à 180 personnes qui ont un lien avec le Canada, qui sont à l'étranger et qui sont impliquées dans des activités menaçantes. Du nombre, environ 100 sont en Irak ou en Syrie.

Le président : Combien de Canadiens qui tentent de quitter le pays a-t-on identifiés?

M. Coulombe : Je n'ai pas ce chiffre avec moi, mais je dirais qu'il y en a probablement à peu près autant qu'il y a un an, soit de 90 à 100. Encore une fois, c'est très difficile. Nous apprenons le départ d'un certain nombre de personnes après coup, alors le chiffre ne reflète pas l'ampleur réelle du phénomène.

Le président : Merci, monsieur Coulombe. Je crois que, dans une certaine mesure, nous avons précisé les choses pour le compte rendu.

[*Français*]

Le sénateur Dagenais : Merci beaucoup, monsieur Coulombe, de votre présentation. J'aimerais parler des combattants qui reviennent de l'étranger. Je sais que vous devez garder certains détails confidentiels. Toutefois, combien de ressources seraient consacrées à la surveillance de ces combattants qui reviennent de l'étranger? Qu'est-ce que cela représente, en termes de coûts, dans vos budgets?

M. Coulombe : Je n'ai pas les données précises sur le nombre de retours. Quant au service, nous consacrons environ 55 p. 100 du budget opérationnel à la lutte contre le terrorisme.

Il est important de comprendre que les 60 individus qui sont de retour posent potentiellement une menace. Certains reviennent et reprennent une vie normale. Après une certaine période, on juge qu'ils ne posent plus de menace. D'autres continueront d'être

For example, by funding or radicalizing other people. Because of their experience, they can sometimes facilitate the travel of others. Based on their activities, we assign resources based on the imminence of the potential threat.

With regard to the resources assigned to the surveillance of returnees, I could give you an answer at a later date given that I do not have the information with me today.

Senator Dagenais: In your opinion, are the resources assigned to the surveillance of these people, in order to make sure that they do not become radicalized once again, enough, or do you require more? We understand that there are however some grey areas.

Mr. Coulombe: We have already mentioned that, just like the RCMP, the service had to reassign resources to the fight against terrorism, amounts that were reassigned from other programs. However, as you will remember, we obtained additional resources in the last budget for the next five years so that we may increase our capacity to fight terrorism.

With regard to whether we have sufficient resources, we will never say no to additional resources. That said, I believe that current resource levels, as well as those assigned to us over the next five years, put us in a very good position to manage terrorism without negatively impacting our other programs.

[*English*]

Senator Kenny: Welcome, Mr. Coulombe.

When Jim Judd appeared before this committee some time ago, he testified that 50 per cent-plus of CSIS's resources were being spent on one country, and that was China.

Describe to the committee how your organization and your focus has changed when you come to us today and say that 55 per cent of your resources are now focused on terrorism. Where does China sit? The other responsibilities that you have, how have they changed? How have they been diminished? How has that increased the concerns that Canadians should have about our security?

Mr. Coulombe: I can't comment about the 50 per cent back when Mr. Judd was director. What I can say is that probably 50 to 55 per cent of the resources are on counterterrorism. For the service, the number two priority is espionage.

I think the difference is that we now have a much more focused program in terms of our collection and leveraging a lot more partners, both domestic and foreign, in terms of burden sharing and working together to fill intelligence gaps.

impliqués de différentes façons, par exemple dans le cadre du financement ou de la radicalisation d'autres personnes. De par leur expérience, ils pourront parfois faciliter le voyage d'autres individus. Selon leurs activités, nous affecterons des ressources en fonction de l'imminence de la menace qu'ils peuvent représenter.

Quant aux données concernant les ressources consacrées à la surveillance des individus qui sont de retour, je pourrai vous fournir une réponse plus tard, car il m'est impossible de le faire aujourd'hui.

Le sénateur Dagenais : À votre avis, les ressources affectées à la surveillance de ces gens, pour veiller à ce qu'ils ne se radicalisent pas à nouveau, sont-elles suffisantes ou en faudrait-il davantage? Nous comprenons qu'il existe tout de même des zones grises.

M. Coulombe : On avait déjà mentionné que, tout comme la GRC, le service a dû réallouer des ressources à la lutte contre le terrorisme, qu'il a puisées dans d'autres programmes. Toutefois, vous vous souviendrez, lors du dernier budget, nous avions obtenu des ressources additionnelles pour les cinq prochaines années afin d'augmenter notre capacité à lutter contre le terrorisme.

Lorsque vous nous demandez si nous avons suffisamment de ressources, nous ne dirons jamais non à davantage de ressources. Toutefois, je suis persuadé que les ressources actuelles, en plus de celles qui viendront au cours des cinq prochaines années, nous placent dans une très bonne position pour gérer le phénomène lié au terrorisme, sans avoir un impact négatif sur les autres programmes.

[*Traduction*]

Le sénateur Kenny : Bonjour, monsieur Coulombe.

Lorsque Jim Judd a comparu devant le comité il y a un certain temps, il a déclaré qu'au moins 50 p. 100 des ressources du SCRS étaient consacrées à un pays, la Chine.

Pouvez-vous dire au comité de quelle façon votre organisation et ses intérêts ont changé, puisque vous nous dites aujourd'hui que 55 p. 100 de vos ressources sont affectées au terrorisme? Qu'en est-il de la Chine? En quoi vos autres responsabilités ont-elles changé? Y a-t-il eu des réductions? Vu la situation, dans quelle mesure les Canadiens devraient-ils craindre davantage pour leur sécurité?

M. Coulombe : Je ne peux pas formuler de commentaires au sujet des 50 p. 100 lorsque M. Judd était directeur. Ce que je peux vous dire, c'est que probablement de 50 à 55 p. 100 des ressources sont consacrées au contreterrorisme. Pour le Service, la deuxième priorité est l'espionnage.

Selon moi, la différence, c'est que nous comptons maintenant sur un programme de collecte d'information beaucoup plus ciblé et nous tirons davantage profit d'un bien plus grand nombre de partenaires, au pays et à l'étranger, avec qui nous partageons la charge de travail et travaillons en collaboration afin de combler les lacunes en matière de renseignement.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Despite the fact that the number of resources allocated against other files, other than terrorism, might have gone down, we have again refined the way we work, partnerships, and the net outcome in terms of collecting the intelligence that is required, that our clients are looking for. I would say we haven't really seen a degradation of the value of our different programs, be it China or any others.

Senator Kenny: Are you telling us, then, that China isn't still a serious threat and is not the principal country involved in espionage against Canada?

Mr. Coulombe: No, that's not what I've said. What I've said is espionage is a serious threat. It's our number two priority, but despite the fact that we have possibly less or the same level of resources for those programs, we have refined the way we work in those programs in terms of a more focused collection through our regional offices and a better leveraging of the capacity of partners, be it domestic or foreign, in order to meet the requirement of the client, which is the government.

[*Translation*]

Senator Carignan: My questions will address two subjects. I would first like to discuss foreign combatants. I understand that 55 per cent of your resources are assigned to the matter?

Mr. Coulombe: Yes, to fighting terrorism and foreign combatants. As I mentioned, that is why it is dangerous to mention numbers. There are 180 people with ties to Canada who are currently abroad. However, that is just one threat among others. There are also individuals in Canada who have never intended to travel, who pose a threat, and to whom we have resources assigned.

Senator Carignan: You say that there are 180 people abroad. I understand that about a hundred of them are in Syria or in Iraq.

Mr. Coulombe: Exactly.

Senator Carignan: There are therefore 80 in other countries?

Mr. Coulombe: Yes.

Senator Carignan: You must assign a considerable amount of resources to tracking these people. One must not forget the domestic threat. Some foreign combatants or other people are a threat because they could decide to come to Canada. We have seen Europeans, Belgians and the French. These are people who have an easier time coming to Canada and can do so. However, these needs already account for 55 per cent of the budget.

I am worried because when this is all over, these people will come back to Canada or their country of origin and they will have unhindered access. How will you be able to track all of these people?

Malgré le fait que le nombre de ressources affectées à d'autres dossiers — outre le terrorisme —, a peut-être diminué, encore une fois, nous avons peaufiné notre façon de travailler et nos partenariats et amélioré nos résultats nets en ce qui a trait à la collecte des renseignements dont nos clients ont besoin. Je dirais qu'il n'y a pas vraiment eu une diminution de la valeur de nos différents programmes, que ce soit en Chine ou ailleurs.

Le sénateur Kenny : Êtes-vous en train de me dire que la Chine n'est plus une menace sérieuse et que ce n'est plus le pays qui mène le plus d'activités d'espionnage contre le Canada?

M. Coulombe : Non, ce n'est pas ce que j'ai dit. Je dis que l'espionnage est une menace sérieuse. C'est notre deuxième priorité. Cependant, malgré le fait qu'il y a peut-être moins de ressources affectées à ces programmes — ou autant qu'avant —, nous avons peaufiné nos façons de travailler dans le cadre de ces programmes en misant sur des activités de collecte de renseignements plus ciblés dans nos bureaux régionaux et en tirant davantage profit des capacités de nos partenaires, que ce soit au pays ou à l'étranger, afin de répondre aux besoins de notre client, le gouvernement.

[*Français*]

Le sénateur Carignan : Mes questions toucheront deux sujets. J'aimerais d'abord poursuivre sur le sujet des combattants étrangers. J'ai compris que 55 p. 100 des ressources y sont consacrées?

M. Coulombe : Oui, à la lutte au terrorisme et aux combattants étrangers. Comme je l'ai mentionné, voilà le danger de mettre des chiffres sur la table. Il y a 180 personnes qui ont un lien avec le Canada et qui se trouvent à l'étranger. Or, ce n'est qu'une partie de la menace. Il y a aussi des individus au Canada qui n'ont jamais eu l'intention de voyager, qui posent une menace et auxquels nous consacrons des ressources.

Le sénateur Carignan : Vous dites que 180 personnes sont à l'étranger. Je comprends qu'une centaine d'entre elles se trouvent en Syrie ou en Irak.

M. Coulombe : C'est exact.

Le sénateur Carignan : Il y en a donc 80 dans d'autres pays?

M. Coulombe : Oui.

Le sénateur Carignan : Traquer ces personnes nécessite sans doute des ressources considérables. Il y a aussi la menace interne. Certains combattants étrangers ou d'autres personnes constituent une menace, car ils pourraient décider de venir au Canada. Nous l'avons vu : il y a des Européens, des Belges et des Français. Ce sont des gens qui, normalement, accèdent plus facilement au Canada et qui peuvent venir ici. Or, ces besoins représentent déjà 55 p. 100 du budget.

Je suis inquiet car, lorsque tout cela sera terminé, ces gens reviendront au Canada ou retourneront dans leur pays d'origine, et ils auront libre accès. Comment ferez-vous pour surveiller tous ces gens?

Mr. Coulombe: You raise a very good point. We often hear that we will militarily eliminate the Islamic State, in Iraq and in Syria for example, though that will not spell the end of the terrorist threat as we know it.

There are currently 25,000 to 30,000 foreign combatants in Iraq and Syria, and as was the case in the past in Afghanistan and in Bosnia, they will one day return to their country of origin or go to another theatre of jihad.

Honestly, it is a threat we will have to continue to investigate for decades to come. My answer also comes back to what I mentioned earlier with regard to the other question.

For example, in the case of those who are abroad, the 180 individuals, when they will return, our partnerships will be our strength. Indeed, no intelligence service can face this threat alone. We must work together and share information. Some have better capacities in certain regions of the world and we must therefore work with them in order to best identify the threat.

As I mentioned, these individuals constitute different threat levels because they are involved in different types of activities. We need tools in the field and analysis grids in order to define our priorities and assign resources to the surveillance of individuals whom we deem to be the greatest threats, and fewer resources to others, all whilst regularly re-evaluating the situation.

Senator Carignan: If I understand correctly, you are preparing a plan so that when these people return to our country, you will have specific surveillance tools to evaluate these threats. Is that provided for in the plan?

Mr. Coulombe: Yes. Once again, based on the threat level, we know exactly what operational measures and tools will be used. However, we must first know when they are on their way back and, to know this, we must first know when they left from there. It is very difficult to identify all of these different factors.

Senator Carignan: Are we talking about thousands of people?

Mr. Coulombe: Yes.

Senator Carignan: I would now like to discuss a second topic.

[*English*]

The Chair: I'll put you on second round, senator.

Senator White: Thank you very much, Mr. Coulombe, for coming today. As always, it's appreciated that you're here.

In Bill C-51, the agency was given authority to work on the interruption of the Internet by Islamic State and others unnamed and its efforts to recruit Westerners. Could you give an update on success stories or whether it's been helpful?

M. Coulombe : Vous soulevez un très bon point. On entend souvent dire qu'on va éliminer militairement l'État islamique, par exemple en Irak et en Syrie, mais cela ne constitue pas la fin de la menace terroriste telle qu'on la connaît.

En Irak et en Syrie, il y a présentement de 25 000 à 30 000 combattants étrangers et, comme cela s'est produit dans le passé en Afghanistan et en Bosnie, ils vont un jour retourner dans leur pays d'origine ou aller dans un autre théâtre de djihad.

Honnêtement, c'est une menace sur laquelle il faudra continuer d'enquêter, et ce, pendant des décennies. Ma réponse revient aussi à ce que j'ai mentionné plus tôt par rapport à l'autre question.

Par exemple, dans le cas de ceux qui sont à l'étranger, les 180 individus, lorsqu'ils reviennent, c'est le partenariat qui fait la force. En fait, aucun service de renseignement ne peut faire face seul à cette menace. Il faut travailler ensemble et partager l'information. Certains ont de meilleures capacités dans certains coins du monde, donc nous devons travailler avec eux pour tenter de cerner le mieux possible la menace.

Comme je l'ai mentionné, ces individus ne représentent pas tous le même niveau de menace, parce qu'ils sont impliqués dans différents types d'activités. Il faut avoir les outils sur place, les grilles d'analyses pour être en mesure de définir les priorités et de consacrer les ressources à la surveillance des individus dont nous jugeons qu'ils représentent la plus grande menace et d'attribuer moins de ressources aux autres, tout en réévaluant la situation de façon régulière.

Le sénateur Carignan : Si je comprends bien, vous préparez un plan pour ces gens lorsqu'ils seront de retour au pays, de sorte d'avoir des outils spécifiques de surveillance pour évaluer ces menaces. Vous l'avez prévu dans le plan?

M. Coulombe : Oui. Encore une fois, selon le niveau de menace qu'ils représentent, nous savons exactement quels sont les mesures et les outils opérationnels que nous mettrons en place. Cependant, la première chose, c'est de savoir quand ils reviennent et, pour le savoir, il faut savoir qui a quitté le pays. C'est quelque chose de très complexe que de cerner l'ensemble des facettes.

Le sénateur Carignan : On parle de milliers de personnes?

M. Coulombe : Oui.

Le sénateur Carignan : J'aimerais aborder un deuxième sujet.

[*Traduction*]

Le président : Je vous ajoute à la deuxième série, monsieur le sénateur.

Le sénateur White : Merci beaucoup, monsieur Coulombe, d'être venu aujourd'hui. Comme toujours, nous sommes reconnaissants que vous soyez parmi nous.

Dans le projet de loi C-51, le Service a obtenu le pouvoir de retirer l'accès à Internet à l'État islamique et à d'autres entités non nommées, qui s'efforcent de recruter des Occidentaux. Pouvez-vous faire le point sur les réussites à ce sujet ou nous dire si cette mesure a été utile?

Mr. Coulombe: On taking down websites?

Senator White: That's correct. The U.K. has taken down dozens, I think.

The Chair: It is 55,000.

Mr. Coulombe: That was an amendment to the Criminal Code and that would be more law enforcement, the RCMP.

Senator White: It is. Obviously, you're connected to them. Do you have any indication whether or not the RCMP has been successful?

Mr. Coulombe: I don't have that information. The service could be involved in the sense of like we do on all files, sharing information with the RCMP, giving them leads, but the actual action of do we meet the threshold and then taking action to take them down would be for law enforcement, and I don't have the information.

Senator White: Since he didn't have an answer, can I ask another question?

The Chair: A very short follow-up so everybody gets an opportunity.

Senator White: This is kind of a follow-up but a different question totally.

There were concerns raised about insider information as a result of the Khawaja case when he worked at the Department of Foreign Affairs. I know it was raised through law enforcement but also through your agency. Can you give us an update as to whether or not any more has been done with federal agencies in particular? We had some questions about a year ago around integrity testing for ongoing employees so we would deal with some of the other issues that come about, like Snowden as an example.

Mr. Coulombe: Certainly. Since Mr. Momin Khawaja, which goes back to 2004, a lot has been done on what we label the "insider threat." A lot has been done. The service has the lead in terms of working together with all federal departments to strengthen the understanding of the phenomenon and also the type of measures that must be put in place to prevent, detect and deal with the insider threat, and, again, working with foreign partners in terms of understanding us. So a lot has been done.

Senator White: Has it been successful?

Mr. Coulombe: Yes, I believe so. Of course, you could always say, "Well, what about Delisle on the East Coast?" But again, when there is a case like Delisle, we learn a lot from it, and we adjust and improve the measures place in a different department.

M. Coulombe : Pour fermer des sites web?

Le sénateur White : C'est exact. D'après ce que j'en sais, le Royaume-Uni en a fermé des douzaines.

Le président : C'est 55 000.

M. Coulombe : Il s'agissait d'une modification du Code criminel, et cette question relève davantage du domaine de l'application de la loi, donc de la GRC.

Le sénateur White : C'est le cas. De toute évidence, vous entretenez des liens avec la Gendarmerie. Savez-vous si la GRC a obtenu du succès?

M. Coulombe : Je n'ai pas d'information à ce sujet. Le Service participe peut-être — comme nous participons à tous les dossiers — en mettant en commun de l'information avec la GRC, en donnant des pistes, mais, pour ce qui est de la question de savoir si les seuils sont respectés et si des mesures sont prises pour fermer les sites, cela relève du domaine de l'application de la loi, et je n'ai pas une telle information.

Le sénateur White : Puisqu'il n'a pas la réponse, puis-je poser une autre question?

Le président : Une très brève question supplémentaire afin que tout le monde ait son tour.

Le sénateur White : C'est un genre de suivi, mais c'est une tout autre question.

Des préoccupations étaient soulevées au sujet de renseignements internes en raison du dossier de Khawaja et du fait que ce dernier a travaillé pour le ministère des Affaires étrangères. Je sais que cette question a été soulevée par l'intermédiaire du domaine de l'application de la loi, mais aussi par votre service. Pouvez-vous faire le point sur cette situation et nous dire si d'autres choses ont été faites de concert avec des organismes fédéraux en particulier? Il y a environ un an, nous avions certaines interrogations au sujet du contrôle de l'intégrité des employés en poste afin qu'il soit possible de gérer certains des autres problèmes rencontrés, les cas comme Snowden, par exemple.

M. Coulombe : Bien sûr. Depuis le dossier de M. Momin Khawaja, qui remonte à 2004, beaucoup a été fait pour contrer ce que nous avons appelé les « menaces internes ». Beaucoup de mesures ont été prises. Le Service est l'organisme responsable de la collaboration entre tous les ministères fédéraux pour renforcer notre compréhension du phénomène et des types de mesures qu'il faut mettre en place pour prévenir, détecter et gérer les cas de menace interne, et, encore une fois, nous avons travaillé avec des partenaires étrangers afin de bien comprendre la situation. Je dirais donc que beaucoup de choses ont été faites.

Le sénateur White : Et les mesures ont été efficaces?

M. Coulombe : Oui, je le crois. Bien sûr, on pourrait toujours dire : « Eh bien, qu'en est-il de Delisle sur la côte Est? » Cependant, encore une fois, lorsqu'il y a un cas comme celui de Delisle, nous apprenons beaucoup, nous rajustons le tir et nous améliorons les mesures prises dans les autres ministères?

Senator Day: I'd like to explore a little further a question that Senator Kenny asked.

We read in public documents, Mr. Coulombe, that ISIS, or Daesh, is very well financed. Part of the reason for their success in the Syria and Iraq area is the fact that they're well financed and able to pay international mercenaries to come and fight for their cause.

To what extent is CSIS involved in following the money that's going there? We know about the oil and about banks being robbed, but in the broader international sense of trafficking in persons, kidnapping, and then selling the hostages back to nations, to what extent are you able to put resources into following that type of activity? Part of that has to be what you've talked about here, even though terrorism and extremism are, of necessity, your current focus, 55 per cent, and other threats to Canada's national security. Then you talked about the espionage issue. Intellectual property theft is a big one that generates a lot of insecurity to Canadian companies.

Can you talk about that aspect of money that is leaving Canada and impacting economic security for Canadians?

Mr. Coulombe: On your first question, yes, the service is involved in terrorist financing. We have a unit that works at that.

What's different with Daesh is you could almost label it as a proto-state. A lot of their financing is collecting taxes. You mentioned the petroleum industries, selling antiquities. It's very difficult to understand exactly where all the money is coming from and how to counter it, although lots of effort is put into that. But the service is involved with the financing aspect of not just of Daesh but also other terrorist organizations.

On the second question of intellectual property, especially now with cyber, if people do not take the proper measures to protect their intellectual property, it can be extremely costly for the economy of a country. It's very important. With partners like the CSE on the cyber side, we devote resources to try to counter that, but a lot of it is also education of the private sector in terms of the proper protection for their assets.

Senator Day: Could you explain to us your role in the educational aspect of Canadians?

Mr. Coulombe: Public Safety has the lead. A cyber strategy put forward. This current government has a commitment to review the cyber strategy. But one of the pillars of the current cyber strategy is engagement with the private sector in terms of the

Le sénateur Day : J'aimerais revenir à une question du sénateur Kenny et creuser un peu plus.

Monsieur Coulombe, nous avons lu dans des documents publics que l'EIIL, ou Daesh, est très bien financé. Sa réussite dans la région de la Syrie et de l'Irak s'explique en partie par le fait que l'organisation est bien financée et qu'elle peut payer des mercenaires de partout dans le monde, qui viennent lutter pour sa cause.

Dans quelle mesure le SCRS surveille-t-il l'argent envoyé là-bas? Nous sommes au courant du vol de pétrole et des vols de banque, mais d'un point de vue plus général, à l'échelle internationale, en ce qui concerne la traite des personnes, les rapts puis la vente des otages aux États, dans quelle mesure pouvez-vous consacrer des ressources à la surveillance de ce type d'activités? Cela doit être une des choses dont vous avez parlé ici, même si le terrorisme et l'extrémisme sont, nécessairement, le dossier sur lequel vous vous concentrez habituellement — 55 p. 100 de vos ressources — et qu'il y a aussi d'autres menaces qui pèsent sur la sécurité nationale du Canada. Puis, vous avez parlé de la question de l'espionnage. Le vol de propriété intellectuelle est un enjeu important qui suscite beaucoup d'insécurité chez les entreprises canadiennes.

Pouvez-vous nous parler de l'argent qui quitte le Canada et qui a un impact sur la sécurité économique des Canadiens.

M. Coulombe : Pour répondre à votre première question, oui, le Service lutte contre le financement du terrorisme. Nous avons une unité qui travaille là-dessus.

La différence avec Daesh, c'est qu'on pourrait presque le décrire comme un proto-État. Une bonne partie du financement de l'organisation vient de la collecte d'impôts. Vous avez mentionné l'industrie du pétrole, la vente d'antiquités. C'est très difficile de comprendre exactement d'où vient tout cet argent et de quelle façon gérer ce dossier, même si nous déployons beaucoup d'efforts pour y arriver. Mais, vous savez, le Service s'intéresse à l'aspect financier non seulement de Daesh, mais d'autres organisations terroristes.

Pour ce qui est de la deuxième question sur la propriété intellectuelle, et tout particulièrement maintenant à l'ère de la cybernétique, si les gens ne prennent pas les mesures appropriées pour protéger leur propriété intellectuelle, ce peut être extrêmement coûteux pour l'économie d'un pays. C'est très important. Avec des partenaires comme le CST du côté de la cybernétique, nous affectons des ressources pour tenter de lutter contre cette menace, mais une bonne partie du travail consiste à sensibiliser le secteur privé à la façon de protéger de façon appropriée ses actifs.

Le sénateur Day : Pouvez-vous nous expliquer votre rôle en matière de sensibilisation des Canadiens?

M. Coulombe : Sécurité publique est responsable. Une cyberstratégie a été mise de l'avant, et le gouvernement actuel s'est engagé à l'examiner. Un des piliers de la cyberstratégie actuelle est l'interaction avec le secteur privé pour garantir la

protection critical infrastructure, for example. The third pillar is how to educate and enable private citizens to protect themselves. So there is a cyber strategy and one of the pillars is engagement with the private sector.

Senator Day: Thank you, Mr. Coulombe.

Senator Ngo: Mr. Coulombe, comments were made by the NATO commander about jihadists flowing into Europe as refugees. Given that CSIS has a mandate to screen refugees, including the 25,000 Syrian refugees who have entered Canada, what other steps have you taken so far? Are you 100 per cent certain that none of these individuals have links to the radical jihadist movement?

Mr. Coulombe: I'll start with the last part of your question. As I have said before, we can never be 100 per cent certain. Bringing the risk down to zero is just impossible.

As I have stated before, I'm confident that the system in place was robust. All of the people were screened to the same standard as our normal refugee screening process, but to be here and state that I'm 100 per cent certain is impossible. I cannot make that statement.

The Chair: Twenty-five thousand refugees have been committed to come from Syria. Is that over and above the normal 25,000 refugees Canada takes in on an annual basis? Is that in addition? Perhaps you could give us a number. Are you able to cope if that's what the numbers are?

Mr. Coulombe: We are certainly able to cope in terms of screening the number.

Is it in addition to the normal quota? That's something I would have to check with our immigration refugee group. I don't know off the top of my head.

The Chair: Could you provide us that information?

Mr. Coulombe: Sure.

Senator Beyak: Thank you very much, Mr. Coulombe, for another very thorough report and for the excellent work you do on behalf of Canadians in securing us.

You have a recently published report on the freedom fighters and the phenomena. In it one of the contributors states that more Canadians proportionately are dying in Iraq and Syria than any other nationality. Would you be able to tell the committee approximately how many Canadians or dual nationals have died in the jihadist movement?

Mr. Coulombe: I don't have the number of people who have died. We have to be extremely careful because I know of a number of occasions where people were reported to be killed and resurfaced on Twitter. That's why in our 180, the number of people overseas, we continue to count people who have been

protection des infrastructures essentielles, par exemple. Le troisième pilier concerne la sensibilisation et l'habilitation des citoyens privés afin qu'ils se protègent eux-mêmes. Il y a donc une cyberstratégie dont l'un des piliers est la sensibilisation du secteur privé.

Le sénateur Day : Merci, monsieur Coulombe.

Le sénateur Ngo : Monsieur Coulombe, le commandant de l'OTAN a formulé des commentaires sur des djihadistes qui arrivent en Europe parmi les réfugiés. Puisque le SCRS a le mandat d'évaluer les réfugiés, y compris les 25 000 réfugiés syriens qui sont entrés au Canada, quelles mesures avez-vous prises jusqu'à présent? Êtes-vous sûr à 100 p. 100 qu'aucune de ces personnes n'a de lien avec le mouvement djihadiste radical?

M. Coulombe : Je vais commencer par répondre à la dernière partie de votre question. Comme je l'ai déjà dit, nous ne pouvons jamais être sûrs à 100 p. 100. Il est simplement impossible de réduire le risque à néant.

Comme je l'ai aussi déclaré, j'ai confiance en la robustesse du système que nous avons mis en place. Toutes les personnes ont été contrôlées conformément à la norme habituelle appliquée dans le cadre du processus normal de contrôle des réfugiés, mais je ne peux tout simplement pas vous dire que je suis sûr à 100 p. 100. C'est impossible. Je ne peux pas dire une telle chose.

Le président : On s'est engagé à accueillir 25 000 réfugiés syriens. Est-ce en plus des 25 000 réfugiés que le Canada accueille habituellement chaque année? Est-ce en plus? Pouvez-vous nous fournir un chiffre? Êtes-vous capable de suivre le rythme si ce sont bien les chiffres réels?

M. Coulombe : Nous sommes assurément capables de tous les contrôler.

Est-ce en plus des quotas habituels? Je vais devoir le confirmer auprès de notre groupe responsable de l'immigration des réfugiés. Je ne le sais pas au pied levé.

Le président : Pouvez-vous nous fournir cette information?

M. Coulombe : Bien sûr.

La sénatrice Beyak : Merci beaucoup, monsieur Coulombe, de nous avoir présenté un autre rapport exhaustif et de l'excellent travail que vous faites au nom des Canadiens pour assurer notre sécurité.

Vous avez récemment publié un rapport sur le phénomène des combattants de la liberté. L'un des collaborateurs a déclaré que, proportionnellement, plus de Canadiens meurent en Irak et en Syrie que de ressortissants de tous les autres États. Pouvez-vous dire au comité environ combien de Canadiens ou de personnes ayant une double nationalité sont morts pour la cause du mouvement djihadiste?

M. Coulombe : Je ne sais pas combien de personnes sont décédées. Il faut faire extrêmement attention, parce que je sais que, à l'occasion, nous avons déclaré que des gens étaient morts, pour ensuite les voir réapparaître sur Twitter. C'est la raison pour laquelle, lorsque nous parlons du nombre de personnes à

reported killed until we have confirmation, because too many times we have seen that type of reporting that in the end was wrong. So I can't give you a number of how many people we know or believe have been killed.

There was another report yesterday or today in Libya. We can come back, but I would take those numbers with a *grain de sel*, as we say in French.

Senator Mitchell: Thanks, Mr. Coulombe. You have probably one of the most stressful jobs in the country, and you seem to be holding up well. Thanks for doing it.

This is a very specific question. There seems to be a strange contradiction. On the one hand, you spend a great deal of your resources trying to prevent potential terrorists from leaving Canada and going to fight a terrorist war. On the other hand, we have the dual citizenship legislation that was brought in last year, which says that we would cancel Canadian citizenship for convicted terrorists and then send them back to the country of their second citizenship. How do you square that circle?

Mr. Coulombe: Well, I think that's more of a policy discussion. It's not really for me to comment. Canada is not the only one; France is now considering revoking French citizenship for people involved in terrorism.

That said, I truly believe that, as a country, we have an obligation to prevent Canadians from leaving in order to conduct terrorist and threat-related activities and killing people overseas. We have an obligation. We are signatories to an international obligation, including one that was not long ago passed by the UN exactly for that reason, to prevent people from leaving their country of origin to become involved.

To go back to your question, how you square that circle, that's a policy discussion. We use the tools that are given to us.

I'm not sure there is a contradiction. It's a complex discussion, because on the one hand I have heard the argument that if people want to leave, just let them go and they will end up being killed. Again, as a country, we have a responsibility. We cannot just say to people, "Go and fight in Iraq, Syria, Libya, Yemen and elsewhere because that problem is no longer our problem." That's why we are investigating Canadians overseas, because it is our problem.

Senator Mitchell: Exactly.

You mentioned a couple of times in your presentation the question of cybersecurity, and I'd just like to pursue it a bit further. It's very much divided jurisdictionally. We have provincial government issues and federal government issues, and we have the Department of National Defence within the

l'étranger — les 180 —, nous continuons à compter les personnes qui auraient été tuées tant que nous n'avons pas reçu de confirmation, parce que, trop souvent, nous avons reçu ce type de rapport qui s'est révélé faux. Je ne peux donc pas vous dire le nombre de personnes qui, selon nous, ont perdu la vie.

Un autre rapport est paru hier ou aujourd'hui en Libye. Nous pouvons y revenir, mais je prendrais ces chiffres avec un grain de sel, comme on dit.

Le sénateur Mitchell : Merci, monsieur Coulombe. Vous occupez probablement l'un des postes les plus stressants au pays et vous semblez très bien vous en sortir. Merci de le faire.

J'ai une question très précise à vous poser. Il semble y avoir une étrange contradiction. D'un côté, vous consacrez une bonne partie de vos ressources pour essayer d'empêcher d'éventuels terroristes de quitter le Canada et d'aller participer à une guerre terroriste. D'un autre côté, un texte législatif sur la double citoyenneté présenté l'année dernière nous permet de retirer la citoyenneté canadienne aux terroristes reconnus coupables avant de les renvoyer dans leur pays de deuxième citoyenneté. De quelle façon pouvez-vous concilier les deux?

M. Coulombe : Selon moi, il s'agit davantage d'une question de politiques. Je ne peux pas vraiment formuler de commentaires à ce sujet. Le Canada n'est pas le seul pays dans cette situation. La France envisage actuellement de révoquer la citoyenneté française des personnes reconnues coupables de terrorisme.

Cela dit, je crois vraiment que, en tant que pays, nous avons l'obligation d'empêcher les Canadiens de quitter le pays pour aller mener des activités terroristes ou menaçantes ou tuer des gens à l'étranger. C'est notre obligation. Nous avons signé des ententes et nous avons des obligations internationales, y compris une obligation qui a été adoptée il n'y a pas longtemps par les Nations Unies exactement pour cette raison, soit empêcher les gens de quitter leur pays d'origine en vue de participer à de telles activités.

Pour revenir à votre question — comment concilier les deux — c'est une question de politiques. Pour notre part, nous utilisons les outils qu'on nous donne.

Je ne sais pas s'il y a vraiment une contradiction. C'est un sujet complexe, parce que, d'un côté, j'ai entendu certains faire valoir que, si les gens veulent partir, il faut les laisser aller se faire tuer. Encore une fois, en tant que pays, nous avons une responsabilité. Nous ne pouvons tout simplement pas dire aux gens : « Allez vous battre en Irak, en Syrie, en Libye, au Yémen ou ailleurs, ce n'est plus notre problème ». C'est la raison pour laquelle nous enquêtons sur les Canadiens à l'étranger : c'est justement notre problème.

Le sénateur Mitchell : Exactement.

Vous avez mentionné à deux ou trois reprises dans votre exposé la question de la cybersécurité, et j'aimerais y revenir. C'est un dossier très fragmenté du point de vue des compétences. Il y a des enjeux liés aux gouvernements provinciaux et d'autres liés au gouvernement fédéral; et il y a le ministère de la Défense nationale

federal government. Clearly you have responsibility for the federal government up to the Department of National Defence, one might argue. Then there is the private sector.

Is all of this being coordinated by the Department of National Defence, or do you think it needs to be better coordinated? Does there need to be more focus? It's so disparate and so significant.

Mr. Coulombe: It is a complex file. You're right in the sense that DND through the Communications Security Establishment, us — you haven't mentioned the RCMP, which is another player in cybercrime.

At the federal level, there is pretty good coordination. People talk and we know our respective roles and we share information. There has been a lot of work done. I was talking about Public Safety having the lead with the cyber-strategy and engaging not just the private sector, as I mentioned earlier, but provincial, which goes down to municipal.

That engagement is taking place. Is there room for improvement? Yes, there is room for improving that dialogue with the provincial governments and with the private sector, but that dialogue is taking place.

[*Translation*]

Senator Carignan: Mr. Coulombe, you said, in the other place, that the services have used disruption powers as authorized by Bill C-51. Could you tell me how many times you used this power? In addition, could you explain how those powers were used and the reasons why this rather exceptional disruptive power is important to your service?

Mr. Coulombe: As I already stated, I believe that this is an important tool. Whether or not it is exceptional depends on your perspective; most of our foreign partners also have this capacity.

For operational reasons, I am not able to tell you how many times we used this power. But what I can say, and I mentioned it during my appearance before the House of Commons parliamentary committee, is that we have used threat mitigation measures that did not require a warrant. Therefore, we did not have to turn to a federal court. These are the only measures that we have used to this day. I cannot provide you with more details on the types of measures in question and the number of times that they have been used as that is part of our operational activities.

Senator Carignan: Could you at least provide us with an order of magnitude? Did you use these dozens or perhaps hundreds of times?

Mr. Coulombe: No. One must understand that when Bill C-51 received royal assent and became law, we did not go to work the next day and begin to use threat mitigation measures. First came

au sein du gouvernement fédéral. Il est évident qu'il y a une responsabilité pour le gouvernement fédéral, et même pour le ministère de la Défense nationale. Puis, il y a le secteur privé.

Toutes les activités sont-elles coordonnées par le ministère de la Défense nationale ou croyez-vous plutôt qu'une meilleure coordination est nécessaire? Faudrait-il concentrer davantage les efforts? C'est un dossier si complexe et à la fois si important.

M. Coulombe : C'est un dossier complexe. Vous avez raison : le MDN, par l'intermédiaire du Centre de sécurité des télécommunications, nous... vous n'avez pas mentionné la GRC, qui est un autre intervenant dans la lutte à la cybercriminalité.

À l'échelon fédéral, il y a une assez bonne coordination. Les gens se parlent, nous connaissons nos rôles respectifs et nous communiquons de l'information. Beaucoup de travail a été fait. J'ai dit que Sécurité publique était responsable de la cyberstratégie et qu'il interagissait non seulement avec le secteur privé — comme je l'ai déjà dit —, mais aussi avec les gouvernements provinciaux et même les administrations municipales.

Cette collaboration a lieu. Pourrait-on faire mieux? Oui, on pourrait améliorer le dialogue avec les gouvernements provinciaux et le secteur privé, mais des discussions ont déjà lieu.

[*Français*]

Le sénateur Carignan : Monsieur Coulombe, vous avez dit à l'autre endroit que les services ont utilisé un pouvoir de perturbation qui a été autorisé par le projet de loi C-51. Pouvez-vous nous dire combien de fois vous avez utilisé ce pouvoir? De plus, pouvez-vous nous expliquer la manière dont il a été utilisé et les raisons pour lesquelles l'accès à ce pouvoir de perturbation — qui est assez exceptionnel — est important pour votre service?

M. Coulombe : Comme je l'ai déjà dit, je crois que c'est un outil important. À savoir s'il est exceptionnel, tout dépend de la perspective dans laquelle nous l'observons; la plupart de nos partenaires étrangers ont aussi cette capacité.

Pour des raisons opérationnelles, je ne suis pas prêt à révéler le nombre de fois que nous l'avons utilisé; ce que je peux dire — et je l'ai mentionné lors de ma comparution devant le comité parlementaire de la Chambre des communes —, c'est que nous avons utilisé des mesures de réduction de la menace qui n'exigeaient pas de mandat. De ce fait, nous ne sommes donc pas obligés d'accéder à la cour fédérale. Ce sont les seules mesures que nous avons utilisées à ce jour. Je ne peux pas vous donner plus de détails concernant le genre de mesures et le nombre de fois qu'elles ont été utilisées, puisque cela relève du volet opérationnel.

Le sénateur Carignan : Pourriez-vous tout de même nous donner un ordre de grandeur? S'agit-il d'une dizaine de fois ou d'une centaine de fois?

M. Coulombe : Non. Il faut comprendre que, lorsque le projet de loi C-51 a reçu la sanction royale et qu'il est devenu loi, nous n'avons pas, dès le lendemain, commencé à instaurer des mesures

the creation of departmental directives. From these, we had to develop our operational policies and related governance. We also had to organize training where need be. We were only truly ready after a few months. Of course, we wanted to act in a responsible way given that we had a new mandate. It therefore took months. With regards to an order of magnitude on how often these measures were used, they were certainly used less than two dozen times.

Senator Carignan: Over what period of time?

Mr. Coulombe: Perhaps since the beginning of the fall.

Senator Carignan: Can we expect that this will occur more frequently in the future, given that the system is now in place?

Mr. Coulombe: Yes. Once again, it is just one tool among many, which is always used in consultation with our partners. Before taking any measure to reduce the threat, we consult the RCMP to ensure that it will not disrupt the RCMP's own investigations. There is a strong, solid oversight framework for any issue related to threat reduction.

It is difficult to provide the frequency or the number. It may so happen that in any given period, its use is not justified; therefore, we will not use it. Given that it's new, it is difficult to give you an order of magnitude by saying that on average, in a given year, it would be used a certain number of times. We will have a better idea after a longer period of time. The government will review its national security policy, and we will see what impact that will have on this measure, among others.

Senator Dagenais: Our committee had recommended that there be closer ties between your services and those of the RCMP to identify individuals who represent a security threat, and also in order to encourage greater efficiency among your services. Have you been able to strengthen ties and exchange information? Are you satisfied with how everything is working?

Mr. Coulombe: I have been with the service for 30 years now, and I have always been involved in files that require interacting with the RCMP. Ties with the RCMP have never been closer than they are currently. For example, measures are in place with RCMP divisions, at the regional level, for information sharing on a regular basis; the same is true at headquarters. We hold joint management team meetings every six months, which my team and I attend, as does Commissioner Paulson and his team, to discuss more strategic issues that affect both organizations.

About five years ago, we implemented, with the RCMP, a framework to define all procedures with respect to intelligence, when the RCMP and CSIS are carrying out a parallel investigation. We called this initiative "One Vision".

pour réduire la menace. Il y a d'abord eu l'établissement de directives ministérielles; à partir de ces dernières, il a fallu développer nos politiques opérationnelles et la gouvernance qui y est liée. Il a également fallu faire de la formation là où il y avait un besoin. Il a fallu quelques mois avant que nous soyons vraiment prêts; bien entendu, nous voulions le faire de façon responsable, étant donné qu'il s'agissait d'un tout nouveau mandat pour le service. Cela a donc pris des mois. Pour vous donner un ordre de grandeur de la fréquence d'utilisation de ces mesures, il s'agit certainement de moins de deux douzaines de fois.

Le sénateur Carignan : Sur une période de combien de temps?

M. Coulombe : Peut-être depuis le début de l'automne.

Le sénateur Carignan : Peut-on s'attendre à ce que cela se produise plus souvent à l'avenir, puisque le système est maintenant en place?

M. Coulombe : Oui. Encore une fois, ce n'est qu'un outil parmi tant d'autres, qui est utilisé toujours en consultation avec nos partenaires. Avant de prendre quelque mesure pour réduire la menace, nous consultons la GRC pour nous assurer que cela ne perturbe pas ses propres enquêtes. Il y a un système de gouvernance solide et rigoureux pour toute la question de la réduction de la menace.

Il est difficile de donner le tempo ou le nombre. Il peut arriver qu'au cours d'une période, il ne soit pas justifié de l'utiliser; ainsi, on ne l'utilisera pas. Étant donné que c'est nouveau, il est difficile de vous donner un ordre de grandeur indiquant qu'en moyenne, dans une année, on l'utilisera un certain nombre de fois. Le temps saura nous le dire. Le gouvernement réexaminera sa politique de sécurité nationale, et nous verrons aussi l'impact que cela aura, entre autres, sur cette mesure.

Le sénateur Dagenais : Notre comité avait recommandé un rapprochement entre vos services et ceux de la GRC pour identifier les individus qui constituaient une menace à la sécurité, et aussi dans le but de favoriser une plus grande efficacité entre vos services. Ce rapprochement et l'échange d'information se font-ils? Est-ce que le tout fonctionne à votre satisfaction?

M. Coulombe : Je suis au service depuis 30 ans et j'ai toujours été impliqué dans des dossiers qui exigeaient une interaction avec la GRC. La relation avec la GRC n'a jamais été au niveau où elle l'est actuellement. Par exemple, des mesures sont en place avec les divisions de la GRC, au niveau régional, pour l'échange d'information sur une base régulière; même chose au quartier général. Nous tenons des séances d'équipes de gestion conjointe tous les six mois, auxquelles prennent part mon équipe et moi, et le commissaire Paulson et son équipe, pour discuter de questions plus stratégiques qui touchent les deux organisations.

Il y a environ cinq ans, nous avions mis en place, avec la GRC, un cadre pour définir la façon de faire, quant au renseignement, lorsque la GRC et le SCRS mènent une enquête parallèle. Nous avions appelé cette initiative « Une vision ».

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

One month ago, Commissioner Paulson and I signed One Vision 2.0. After four or five years, we have learned a great deal. New court decisions have slightly changed the procedures of both organizations. We therefore updated this framework.

I could not tell you the number of conversations that occur between the service and the RCMP on a daily basis, but they are non-stop across the country.

[*English*]

The Chair: Can I follow up on that, colleagues? I think an important recommendation from our report was to ensure that there was a protocol between CSIS and the RCMP. It's not between, necessarily, yourself and Commissioner Paulson; it's actually the corporal who is in Fort St. John or in Whitehorse, he or she. Is there a requirement for them to contact CSIS to ensure, when they are reaching out to bring the community together, that the people they are reaching out to don't have a past that comes out to haunt them later on as they try to move the community ahead?

Mr. Coulombe: I understand. When I talked about the meeting between the RCMP — Commissioner Paulson — and myself, it was just to show the breadth of the interaction. But this One Vision 2.0 I was talking about, this framework, is not for me and the commissioner. It's the framework for the people working on the ground in Montreal, in Toronto, in Edmonton, in Vancouver.

The Chair: And Whitehorse.

Mr. Coulombe: And Whitehorse. What is the framework? There is no one recipe that will fit all cases. This is the framework on which to base yourself when you are interacting with your partner.

The Chair: So it's being done the ground? That's the point.

Mr. Coulombe: Oh, yes.

The Chair:

Senator Kenny: Just to follow up on your comment about screening, Mr. Coulombe, can you please tell us why we should be confident in the screening you and your people do? What sort of tests do you put forward to rely on a propos of refugees?

Mr. Coulombe: For the refugees themselves? As I said, for the 25,000 in the Syrian operation, in terms of the standard that was applied by the service for screening, it was the same standard we applied through our normal screening programs. The same types of checks, the same operation — at an increased tempo, I'll grant you that, but exactly the same measures were put in place.

Le commissaire Paulson et moi, il y a un mois, avons signé Une vision 2.0. Au bout de ces quatre ou cinq années, nous avons appris beaucoup. De nouvelles décisions de la cour ont pu modifier un peu les façons de faire entre les deux organisations. Nous avons donc mis ce cadre à jour.

Je ne pourrais pas quantifier le nombre d'échanges qui ont lieu entre le service et la GRC sur une base quotidienne, mais cela se fait sans arrêt partout au pays.

[*Traduction*]

Le président : Chers collègues, me permettez-vous de dire quelque chose à ce sujet? Selon moi, une recommandation importante de notre rapport concernait le fait qu'il devait y avoir un protocole entre le SCRS et la GRC. Et pas nécessairement pour encadrer les interactions entre vous et le commissaire Paulson, mais plutôt pour le caporal qui est à Fort St. John ou à Whitehorse, que ce soit un homme ou une femme. Lorsqu'ils font un travail d'extension pour rassembler les membres de la collectivité, ces intervenants doivent-ils communiquer avec le SCRS pour s'assurer que les gens qu'ils joignent n'ont pas un passé qui reviendra les hanter par la suite ou lorsqu'ils tentent de faire avancer les choses au niveau de la collectivité?

M. Coulombe : Je comprends. Lorsque j'ai parlé de ma réunion avec la GRC — avec le commissaire Paulson — c'était simplement pour vous montrer le niveau de collaboration. Mais l'initiative Une vision 2.0 dont j'ai parlé, ce cadre, n'a pas été mise en place pour le commissaire et moi. C'est un cadre pour les gens qui travaillent sur le terrain, à Montréal, à Toronto, à Edmonton, à Vancouver.

Le président : Et à Whitehorse.

M. Coulombe : Et à Whitehorse. En quoi consiste le cadre? Il n'y a pas une seule solution adaptée à tous les cas. C'est un cadre sur lequel s'appuyer lorsqu'on interagit avec un partenaire.

Le président : Donc, on s'en sert sur le terrain? C'est ça l'idée.

M. Coulombe : Oh, oui.

Le président :

Le sénateur Kenny : Monsieur Coulombe, par rapport à votre commentaire sur les contrôles, pouvez-vous nous dire pourquoi nous devrions faire confiance au contrôle exercé par vous et vos collègues? À quel genre de tests soumettez-vous les réfugiés?

M. Coulombe : Pour les réfugiés eux-mêmes? Comme je l'ai dit, pour les 25 000 réfugiés syriens, dans le cadre des contrôles, le Service a appliqué la même norme standard que celle dans ses programmes de contrôle habituels. C'est le même genre de vérifications — effectuées à un rythme accéléré, je vous l'accorde —, mais nous avons également mis en place les mêmes mesures.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

That's why I say I'm totally confident, because I have confidence in our screening program. It has been running for over 30 years, and the exact same was applied to this operation. But again, I want to stress, that doesn't mean the risk becomes zero.

Senator Kenny: What I was asking you was sir, is: What are the elements that give you the confidence?

Mr. Coulombe: I don't want to go into the operational details, but it's first of all important to say that normally when a red flag comes up on a file, that's when we will launch an investigation. We will dig deeper and do interviews with people.

In this case — and it was said publicly — if a red flag came up and we had no time to do this because of the tempo, that file was put aside. It is important to understand this: The moment there was a concern, that file was put aside and was no longer one of those 25,000 refugees. All of the other files — and it's not just us, it's CBSA and other partners — went through the same process, the same immigration screening that we've done every day for the last 30 years. I am confident in our system, and that system was applied to the 25,000.

The Chair: Senator White has a follow up on Senator Kenny's question.

Senator White: A lot of people misinterpret what is happening in Europe with migrants and what is happening in Canada with refugees. Could you explain the difference between the two so that Canadians understand?

Mr. Coulombe: That's a good point. It's totally different. In Europe, they have this flow of refugees that are just entering the countries without any screening. Here, what we're talking about — again, yes, it's on an accelerated basis — is bringing people in who, before they boarded the plane, had gone through every check: national security, criminal, Health Canada, and had actually received permanent residency before they arrived. All of the screening was done prior to their arrival, which is totally different from the situation in Europe.

Senator White: Just to be clear, the ones in Europe aren't vetted? They claim refugee status when they arrive. They are a migrant, literally.

Mr. Coulombe: Tens of thousands.

The Chair: Senator Ngo has a follow up on this question as well.

C'est la raison pour laquelle j'ai dit que j'étais totalement en confiance, parce que j'ai confiance en notre programme de contrôle. Le programme est en place depuis plus de 30 ans, et c'est exactement ce même programme que nous avons utilisé dans le cadre de cette opération. Encore une fois, je dois souligner que cela ne signifie pas qu'il n'y a absolument aucun risque.

Le sénateur Kenny : Ma question était la suivante, monsieur : quels éléments vous donnent cette confiance?

M. Coulombe : Je ne veux pas tomber dans les détails opérationnels, mais, pour commencer, il est important de dire que, habituellement, lorsqu'on a une inquiétude relativement à un dossier, on entreprend une enquête. Lorsque cela se produit, nous enquêtons de façon plus poussée et nous rencontrons des gens en entrevue.

Dans le cas des réfugiés syriens — et cela a été dit publiquement — s'il y avait des inquiétudes et que nous n'avions pas le temps de procéder à un tel examen, en raison du rythme opérationnel, le dossier était mis de côté. C'est important de bien comprendre : dès qu'il y avait une préoccupation, le dossier était mis de côté, et la personne était exclue des 25 000 réfugiés. Tous les autres dossiers — et ce n'est pas seulement nous, c'est l'ASFC et d'autres partenaires — ont fait l'objet du même processus. On a procédé au même contrôle des immigrants depuis 30 ans. J'ai confiance en notre système, et c'est le système qui a été utilisé pour traiter les dossiers des 25 000 réfugiés.

Le président : Le sénateur White a une question complémentaire liée à la question du sénateur Kenny.

Le sénateur White : Beaucoup de personnes se trompent sur ce qui se passe en Europe avec les migrants et ce qui se produit au Canada avec les réfugiés. Pouvez-vous expliquer la différence entre les deux afin que les Canadiens puissent bien comprendre?

M. Coulombe : C'est un bon point. C'est tout à fait différent. En Europe, il y a des groupes de réfugiés qui entrent tout simplement dans les différents pays sans contrôle. Ici, ce dont il est question — et, oui, nous procédons de façon accélérée —, c'est que nous faisons venir des personnes qui, avant d'entrer dans l'avion, ont fait l'objet de tous les contrôles requis : sécurité nationale, criminalité, Santé Canada, et ils obtiennent la résidence permanente avant d'arriver. Toutes les activités de contrôle ont été réalisées avant leur arrivée, ce qui est tout à fait différent de la situation en Europe.

Le sénateur White : Pour que ce soit bien clair : les réfugiés en Europe ne font pas l'objet d'un tel contrôle? Ils demandent le statut de réfugié lorsqu'ils arrivent? Ils sont littéralement des migrants.

M. Coulombe : Des dizaines de milliers.

Le président : Le sénateur Ngo a aussi une question de suivi.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Senator Ngo: You mentioned vetting. Can you tell us some of the difficulties or challenges for CSIS involved in verifying whether each of the refugees welcomed in Canada is in fact who he or she claims to be? Do you have any difficulties or challenges in that regard?

Mr. Coulombe: Do you mean for the 25,000, or in general?

Senator Ngo: In general. Twenty-five thousand, plus.

Mr. Coulombe: It's always a challenge, but again, in the case of 25,000, biometrics were checked. Everything was done to make sure that the person saying, "I am Mr. X" was actually Mr. X.

But I'm not going to sit here and say there were no challenges. That's why we cannot bring that risk down to zero; there is always a chance. But all of the possible measures were put in place. Again, I'm not going to talk for other agencies, but at the service, we have applied the same standards that we apply for our normal role in the immigration screening program.

[*Translation*]

Senator Carignan: One of your answers raises a question. You say that the people who are entering the country are the 25,000 individuals who are truly above suspicion and that, in the event of any doubt, they are set aside. You say that that is the practice in all countries. At least, most countries that practise refugee control have a more robust access process, as is the case in the United States, for example. This means that a rather significant number of high-risk individuals are walking around Europe and can decide, for whatever reason, to enter by other means. They could come here as students or as visitors. There are many ways to enter Canada without necessarily going through the refugee process. How can you assure us that these high-risk individuals are not using other means of entry than the one given to them by their refugee status?

Mr. Coulombe: We can ensure this thanks to information sharing among the services. When an individual has been identified as being linked to the Islamic State or having fought for the Islamic State, the information is shared.

In any case, if the individual tries to enter Canada by a process other than the refugee process, if this process is part of the service's screening program, and if the information is found in our databases, because we have exchanged information with a European service, for example, that is when the alarm bells start ringing. Once again, no system is 100 per cent effective against individuals who wish to enter the country.

Le sénateur Ngo : Vous avez parlé de contrôle. Pouvez-vous nous parler de certaines des difficultés ou de certains des défis pour le SCRS liés aux vérifications nécessaires pour confirmer l'identité des réfugiés accueillis au Canada? Faites-vous face à des difficultés ou des défis à cet égard?

M. Coulombe : Vous parlez des 25 000 réfugiés ou de façon générale?

Le sénateur Ngo : En général. Les 25 000 et plus.

M. Coulombe : C'est toujours un défi, mais, encore une fois, dans le cas des 25 000 réfugiés, les données biométriques ont été vérifiées. Tout a été fait pour que l'on puisse s'assurer que la personne affirmant « être M. X » était bel et bien « M. X ».

Je ne vais cependant pas vous dire qu'il n'y a pas eu de défis. C'est la raison pour laquelle nous ne pouvons pas éliminer totalement le risque. Il y a toujours un risque, mais toutes les mesures possibles ont été prises. Encore une fois, je ne peux pas parler au nom des autres organismes, mais, au sein du service, nous avons appliqué les mêmes normes que celles que nous appliquons habituellement dans le cadre de notre programme de contrôle de l'immigration.

[*Français*]

Le sénateur Carignan : Une de vos réponses soulève une question. Vous dites que ceux qui entrent sont les 25 000 individus qui sont vraiment hors de tout soupçon et que, dès qu'on a un doute, on les met de côté. Vous dites que c'est la pratique dans tous les pays. Du moins, la plupart des pays qui exercent un contrôle des réfugiés ont un processus d'accès plus solide, comme c'est le cas aux États-Unis, par exemple. Cela signifie qu'une quantité assez importante de personnes à risque se promènent en Europe et peuvent décider, pour une raison quelconque, d'entrer par d'autres voies. Elles pourraient venir à titre d'étudiants ou de visiteurs. Il y a une multitude de façons d'entrer au Canada sans nécessairement passer par le statut de réfugié. Comment pouvez-vous nous assurer que ces personnes à risque n'utilisent pas d'autres voies d'entrée que celle que leur accorde leur statut de réfugié?

M. Coulombe : Nous pouvons nous en assurer grâce au partage d'information entre les services. Lorsqu'un individu a été identifié comme étant lié à Daesh ou ayant combattu pour Daesh, l'information est partagée.

De toute façon, si l'individu tente d'entrer au Canada par un autre processus que par celui de son statut de réfugié, que ce processus fait partie du programme de filtrage du service et que de l'information se trouve dans nos banques de données, parce que nous avons échangé de l'information avec un service européen, par exemple, c'est à ce moment-là que sonne le signal d'alarme. Encore une fois, aucun système n'est entièrement à l'épreuve des individus qui veulent entrer.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*English*]

Senator Beyak: Mr. Coulombe, last June our Senate committee had a report on terror. We identified the Muslim Brotherhood as a concern. Other nations in the world, the U.K. and the United States, are currently scrutinizing the Muslim Brotherhood carefully. I wonder if CSIS has made any recommendations to our government about the Muslim Brotherhood.

Mr. Coulombe: We have looked at the Muslim Brotherhood; and we are looking at the Muslim Brotherhood.

A word of caution: I would say that it is very difficult to talk about "the" Muslim Brotherhood. The Muslim Brotherhood in Egypt is different from the one in Jordan and from the ones anywhere else in that part of the world. To label as "Muslim Brotherhood," in my opinion, is the wrong way to approach this.

But we have looked at this. We are in discussion with our partners in terms of what they have and whether they have them listed. As far as I know, for example, the U.K. has not listed the Muslim Brotherhood.

It is not just the Muslim Brotherhood because all potential terrorist organizations are assessed in terms of listing them under the Criminal Code, for example. Do they pose a threat here? Would it be justified for the service to devote resources against them?

Senator Mitchell: Mr. Coulombe, you mentioned the 60 returnees. A question that immediately jumps to mind is: Why aren't they all in jail? What is it they did or didn't do over there that wasn't intense enough such that they would be arrested the moment they arrived?

Mr. Coulombe: Well, that is a question for the RCMP. Having information that somebody was involved in threat-related activities overseas does not necessarily mean that the information meets the Criminal Code threshold. Is it enough for the RCMP to charge an individual? It's a pretty difficult thing to do. Again, it's more for the RCMP to answer. There is a fair bit of a difference between the threshold for us to launch an investigation and the threshold to charge somebody under the Criminal Code. Proving that the person was actually in Iraq and Syria fighting, financing and on social media is a difficult task.

Senator Mitchell: It isn't just that you exchange information with the RCMP, as the legislation allows you to exchange information with 16 other agencies and departments. Has any effort been made to write memorandums of understanding on how that information can be used and had how long it can be kept?

[*Traduction*]

La sénatrice Beyak : Monsieur Coulombe, en juin, notre comité sénatorial a produit un rapport sur le terrorisme. Nous avons déterminé que les Frères musulmans étaient une source de préoccupation. D'autres États, le Royaume-Uni et les États-Unis, suivent actuellement de près les Frères musulmans. Je me demande si le SCRS a formulé des recommandations à notre gouvernement au sujet de ce groupe.

M. Coulombe : Nous avons déjà examiné l'organisation des Frères musulmans, et nous continuons de les avoir à l'œil.

J'aimerais faire une mise en garde : on peut difficilement parler des Frères musulmans comme étant « une seule entité ». Les Frères musulmans en Égypte sont différents des Frères musulmans de la Jordanie et de partout ailleurs dans cette partie du monde. Selon moi, il ne faut pas mettre tous les Frères musulmans dans le même panier.

Cependant, nous nous sommes penchés sur leur cas. Nous discutons actuellement avec nos partenaires pour obtenir les renseignements qu'ils possèdent et déterminer s'ils les ont inclus dans leurs listes. Par exemple, d'après ce que j'en sais, le Royaume-Uni n'a pas ajouté les Frères musulmans à sa liste.

Ce ne sont pas seulement les Frères musulmans qui nous intéressent; toutes les organisations terroristes possibles sont évaluées pour que l'on puisse déterminer si elles sont doivent être visées par le Code criminel, par exemple. Tel ou tel groupe représente-t-il une menace pour le Canada? Serait-il justifié pour le service de consacrer des ressources à tel ou tel dossier?

Le sénateur Mitchell : Monsieur Coulombe, vous avez mentionné que 60 personnes étaient revenues au pays. La question qui me vient immédiatement à l'esprit est la suivante : pourquoi ne sont-elles pas toutes en prison? En quoi ce qu'elles ont fait ou n'ont pas fait là-bas n'est-il pas suffisant pour qu'on les arrête dès leur retour?

M. Coulombe : Eh bien, c'est une question à poser à la GRC. Le fait de posséder des renseignements selon lesquels une personne a été impliquée dans des activités menaçantes à l'étranger ne signifie pas nécessairement que les renseignements en question respectent le seuil établi dans le Code criminel. Est-ce suffisant pour que la GRC dépose des accusations? Ce peut être difficile à prouver. Encore une fois, c'est à la GRC qu'il faut poser la question. Il y a une assez grande différence entre le seuil requis pour mener une enquête et le seuil requis pour accuser quelqu'un au titre du Code criminel. Il est difficile de prouver la présence effective d'une personne en Irak ou en Syrie pour se battre ou qu'elle s'adonnait à des activités de financement ou était présente sur les médias sociaux.

Le sénateur Mitchell : Vous n'échangez pas seulement des renseignements avec la GRC, puisque la loi vous permet de le faire avec 16 autres organismes et ministères. Des efforts ont-ils été déployés pour rédiger des protocoles d'entente sur la façon dont l'information peut être utilisée et sa durée de conservation?

Mr. Coulombe: Yes, we are working with a number of federal departments. We have started to work on the MOU where that exchange of information is the highest between the two organizations.

Senator Day: Mr. Coulombe, during your earlier remarks you talked about extremists who were prevented from leaving Canada also pose a serious workload for you and your organization, even though they haven't travelled but perhaps more so because they haven't travelled. I wonder if we could take a practical example. You went on to say that both perpetrators of the separate October 14 attacks — the two soldiers in Saint-Jean-sur-Richelieu and one soldier in Ottawa — desired to leave Canada but were unable to do so. Can you explain to us in general terms CSIS's role and how it happened that they were unable to leave? How did you know, how were you able to say that they were prevented from leaving, and how would that increase your workload?

Mr. Coulombe: Well, specifically those two cases I do not remember all the details. We know that Couture-Rouleau attempted to leave the country and the RCMP intervened at least on one occasion or maybe two. Zehaf-Bibeau had applied for a passport, but it was being reviewed in terms of his application. How we became aware of this is something operationally that I don't want to get into.

We are aware of a number of people who want to leave, and that certainly adds to our workload. Also, a number of people under investigation by the service or the RCMP have never expressed a desire to leave. This whole issue of people leaving or wanting to leave is not the only terrorist threat here. Some people who have no desire or no capacity to travel, for whatever reason, still pose a threat. That's why I'm always a bit wary when we focus so much on how many Canadians are overseas and how many returnees there are. Yes, it's important; but it is just one aspect of this whole phenomenon of terrorism today.

Senator Day: I want to understand how you want us to take your comment. Did you want us to believe that you knew that these two individuals wanted to leave Canada to participate in terrorist activities abroad? Did you know that?

Mr. Coulombe: I would qualify that and say that we suspected. Again, it goes back to suspicion, to reasonable grounds and charging somebody.

Senator Day: Yes, I understand.

The Chair: I'd like to ask a couple of questions. First, I want to go back to Senator Mitchell's point in respect of the number of Canadians identified as either involved directly or indirectly in terrorism activity. From my understanding, that's against the law. Now it depends on which section of the Criminal Code or other

M. Coulombe : Oui, nous travaillons en collaboration avec un certain nombre de ministères fédéraux. Nous avons commencé à rédiger un PE qui permettra de maximiser l'échange d'information entre les deux organisations.

Le sénateur Day : Monsieur Coulombe, vous avez parlé tantôt des extrémistes dont on a empêché le départ du Canada. Ces personnes représentent une importante charge de travail pour vous et votre organisation, et ce, même si elles ne sont pas allées à l'étranger et, en fait, peut-être encore plus pour cette raison. Je me demande si nous ne pourrions pas utiliser un exemple concret. Vous avez dit ensuite que les deux auteurs des attaques du 14 octobre — celles contre les deux soldats à Saint-Jean-sur-Richelieu et le soldat à Ottawa — voulaient quitter le Canada, mais n'ont pas pu le faire. Pouvez-vous nous expliquer de façon générale le rôle du SCRS à cet égard et de quelle manière on leur a interdit de partir? Comment le saviez-vous? Pourquoi pouvez-vous dire qu'on les a empêchés de partir? Et en quoi cela accroît-il votre charge de travail?

M. Coulombe : Eh bien, dans ces deux cas précis, je ne me souviens plus de tous les détails. Nous savons que Couture-Rouleau a tenté de quitter le pays et que la GRC est intervenue à au moins une occasion, peut-être deux. Zehaf-Bibeau avait présenté une demande de passeport, mais elle faisait l'objet d'un examen dans le cadre de son traitement. Pour ce qui est de savoir comment nous l'avons appris, c'est une question opérationnelle dont je ne veux pas parler.

Nous savons qu'un certain nombre de personnes veulent partir, et, bien sûr, cela accroît notre charge de travail. De plus, un certain nombre de personnes qui font l'objet d'une enquête du service ou de la GRC n'ont jamais exprimé leur désir de partir. Les personnes qui partent ou qui veulent partir ne constituent pas la seule menace terroriste au pays. Des personnes qui ne veulent pas partir ou n'ont pas la capacité de le faire — pour quelque raison que ce soit — peuvent quand même être une menace. C'est la raison pour laquelle je suis toujours réticent à l'idée de mettre trop l'accent sur le nombre de Canadiens qui sont à l'étranger et le nombre de personnes revenues au pays. Oui, c'est important, mais il ne s'agit quand même seulement que d'un des aspects du phénomène actuel du terrorisme.

Le sénateur Day : J'aimerais comprendre de quelle façon vous voulez que nous interprétions ce que vous dites. Essayez-vous de nous dire que vous saviez que ces deux personnes voulaient quitter le pays pour participer à des activités terroristes à l'étranger? Vous le saviez?

M. Coulombe : Je dirais plutôt que nous avions des soupçons. Encore une fois, c'est une question de soupçons et de motifs raisonnables au moment de porter des accusations.

Le sénateur Day : Oui, je comprends.

Le président : J'aimerais poser deux ou trois questions. Premièrement, je veux revenir à ce qu'a dit le sénateur Mitchell au sujet du nombre de Canadiens dont il a été déterminé qu'ils avaient participé directement ou indirectement à des activités terroristes. D'après ce que j'en comprends, agir ainsi est contre la

statutes, but it's against the law. We read in the newspaper yesterday that four British citizens, I believe, were charged under the terrorism act for wanting to leave Britain for the purpose of being involved in the jihadist Islamic movement in Syria and Iraq.

I don't quite understand, and maybe I'm just a boy from Whitehorse: We have 90 to 100 Canadians identified as wanting to leave this country. We have already experienced the situation where two individuals had wanted to leave this country and were denied. They then committed murder and an attack on Parliament. Why isn't anyone being charged for being involved in these activities? Why are we leaving them on the street, similar to what Senator Mitchell is talking about, and similarly, if you could respond to me, those that are coming back? Am I missing something here?

Mr. Coulombe: No, and it's not a question of avoiding the question. This is really a law enforcement question. This is for the RCMP. I don't want to mislead the committee. I don't want to say something that is wrong in terms of the RCMP's role and explanation. This is really for the RCMP to answer.

Senator Kenny: On this, I thought your answer was that the amount of information you collected didn't meet the test of the Criminal Code.

Mr. Coulombe: It's not just the information we collect; the RCMP is conducting a criminal investigations. Again, collecting evidence to the threshold of being able to charge somebody when their activities are taking place in a conflict zone like Iraq and Syria is not a simple task. Again, the RCMP would be better placed to explain the challenges and the reasons, to answer your question.

The Chair: Colleagues, I want to thank Mr. Coulombe for being as frank as he is. We appreciate the position you have and we want to again commend your organization for the job they're doing. Hopefully we continue to negate the plots that are out there and that you have to scrutinize and try to cope with. Thank you.

Joining us on panel 2 today is our Chief of the Defence Staff, General Jonathan Vance. General Vance grew up in a military family and at the age of 13 started uniform life as an army cadet. He joined the Canadian Armed Forces in 1982 and was commissioned as an infantry officer in 1986. He has commanded at all levels within the field force, from platoon

loi. Évidemment, il reste à savoir au titre de quel article du Code criminel ou aux termes de quelle autre loi, mais un tel comportement est illégal. Nous avons lu hier dans les journaux que quatre citoyens britanniques, si je ne m'abuse, ont été accusés au titre d'une loi sur le terrorisme parce qu'ils avaient voulu quitter la Grande-Bretagne et se joindre au mouvement islamique djihadiste en Syrie et en Irak.

Je ne suis pas sûr de comprendre, c'est peut-être parce que je ne suis qu'un simple gars de Whitehorse : nous avons déterminé que de 90 à 100 Canadiens veulent quitter le pays. Nous nous sommes déjà retrouvés dans la situation où deux personnes qui voulaient quitter le pays et n'ont pas pu le faire ont ensuite commis des meurtres et perpétré une attaque sur le Parlement. Pourquoi est-ce que personne n'est accusé de participer à de telles activités? Pourquoi ces gens sont-ils libres comme l'air, un peu comme ce dont a parlé le sénateur Mitchell? Et, dans un même ordre d'idées — si vous voulez bien me répondre —, on pourrait dire la même chose de ceux qui reviennent au pays. Est-ce qu'il y a quelque chose qui m'échappe?

M. Coulombe : Non, et je ne tente pas d'éluder la question. C'est vraiment une question qu'il faut poser aux organisations responsables de l'application de la loi. C'est une question qu'il faut poser à la GRC. Je ne veux pas vous dire n'importe quoi. Je ne veux pas vous fournir des renseignements erronés sur le rôle de la GRC ou ses motifs. C'est vraiment la GRC qui peut répondre à cette question.

Le sénateur Kenny : À ce sujet, je croyais que vous aviez répondu que les renseignements que vous aviez obtenus ne respectaient pas les critères établis dans le Code criminel.

M. Coulombe : Ce n'est pas seulement les renseignements que nous recueillons; la GRC mène des enquêtes criminelles. Encore une fois, ce n'est pas une sinécure de recueillir suffisamment d'éléments de preuve pour respecter le seuil juridique et accuser quelqu'un pour des activités auxquelles il s'est adonné dans une zone de conflit comme l'Irak et la Syrie. Encore une fois, la GRC serait mieux placée pour vous expliquer les défis et ses motifs et répondre à votre question.

Le président : Chers collègues, je tiens à remercier M. Coulombe d'être aussi franc. Nous comprenons la position dans laquelle vous vous trouvez et nous voulons encore une fois féliciter votre organisation du travail qu'elle fait. J'espère que nous continuerons à contrecarrer les complots fomentés sur lesquels vous devez enquêter et que vous devez essayer de gérer. Merci.

Notre deuxième témoin aujourd'hui est le chef d'état-major de la Défense, le général Jonathan Vance. Le général Vance vient d'une famille militaire et il a commencé à porter l'uniforme à 13 ans, au sein des cadets de l'armée. Il s'est joint aux Forces armées canadiennes en 1982, et il est devenu officier d'infanterie en 1986. Il a assuré un commandement à tous les échelons au sein

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

commander to brigade commander and in combat operations as joint task force commander.

Following his tours in Afghanistan, General Vance served in Army Headquarters as Chief of Staff Land Strategy and as Director of the Strategic Joint Staff at National Defence Headquarters. He completed a tour as Deputy Commander of the Allied Join Force Command in Naples in July 2014, before assuming his position as Commander of the Canadian Joint Operations Command in September of the same year.

His decorations include the Order of Military Merit in the rank of commander, the Meritorious Service Cross with bar and Mention in Dispatches, and in 2011 he was awarded the Vimy Award for his contributions to the defence and security of Canadians.

General Vance was promoted to his current rank and formally appointed as the Canadian Armed Forces Chief of the Defence Staff in July 2015. Congratulations.

General Vance, welcome to the committee. The floor is yours.

General Jonathan Vance, Chief of the Defence Staff, National Defence and the Canadian Armed Forces: Mr. Chair, senators, ladies and gentlemen, thank you for having me here today.

[*Translation*]

I am happy to have the opportunity to provide you with a brief update on the refocused military mission, and I will be happy to take your questions at the end.

[*English*]

As you are aware, last month the Prime Minister announced a new whole-of-government approach to the crisis in Iraq and Syria. This approach looks at security, diplomacy, humanitarian assistance and development. The Canadian Armed Forces will be part of this comprehensive approach and continue to play an important role in the fight against ISIL.

I have total confidence in this new approach. It indeed represents a greater commitment along a critical path for the ultimate defeat of ISIL.

A thorough analysis of the evolving situation has been conducted by me and my staff. Overall, we will increase the number of deployed personnel on Operation IMPACT to roughly 830 people from approximately 650 before.

des forces de campagne, de commandant de peloton à commandant de brigade et dans le cadre d'opérations de combat, en tant que commandant de la force opérationnelle interarmées.

Après des périodes de service en Afghanistan, le général Vance a servi au Quartier général de l'Armée de terre en tant que chef d'état-major — Stratégie et directeur d'état-major interarmées stratégique au Quartier général de la Défense. Il a terminé une période de service en tant que commandant adjoint de la Force interarmées alliée à Naples en juillet 2014, avant d'occuper son poste actuel de commandant du Commandement des opérations interarmées du Canada en septembre de la même année.

Parmi ses décorations, mentionnons l'Ordre du mérite militaire au grade de commandant, la Croix du service méritoire avec barrette et Citation à l'ordre du jour, et en 2011, il a obtenu le prix Vimy, pour sa contribution à la défense et à la sécurité des Canadiens.

Le général Vance a été promu à son grade actuel et officiellement nommé en tant que chef d'état-major de la Défense des Forces armées canadiennes en juillet 2015. Félicitations.

Général Vance, nous vous souhaitons la bienvenue au comité. La parole est à vous.

Général Jonathan Vance, chef d'état-major de la Défense, Défense nationale et les Forces armées canadiennes : Monsieur le président, honorables sénateurs, mesdames et messieurs, merci de m'accueillir aujourd'hui.

[*Français*]

Je suis heureux d'avoir l'occasion de vous fournir une brève mise à jour sur la mission militaire redéfinie, et c'est avec plaisir que je répondrai à vos questions à la fin.

[*Traduction*]

Comme vous le savez, le mois dernier, le premier ministre a annoncé une nouvelle approche pangouvernementale concernant la crise en Irak et en Syrie. Cette approche se penche sur la sécurité, la diplomatie, l'aide humanitaire et le développement. Les Forces armées canadiennes feront partie de cette approche exhaustive, et continueront leur rôle important dans la lutte contre l'EIIL.

J'ai entièrement confiance en cette nouvelle approche. Elle représente en effet un engagement plus long dans une trajectoire critique en vue de vaincre définitivement l'EIIL.

Mon personnel et moi avons réalisé une analyse approfondie de la situation en constante évolution. Et dans l'ensemble, le nombre de militaires déployés dans le cadre de l'Opération IMPACT passera d'environ 650 à approximativement 830.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Operation IMPACT will have as its main effort the train, advise and assist role with the Kurd forces in the north. We will also significantly increase our intelligence capacity. Our Polaris air refueller and Aurora surveillance aircraft will continue to serve as critical enablers for the coalition effort.

We will also be offering a ministerial liaison team to the Government of Iraq as part of a coalition effort. This team will help connect with Iraqi ministries and will be led by a Canadian general officer.

Capacity-building efforts will be undertaken in Jordan and Lebanon, although they are still being scoped at this time.

An increased medical presence to support Canadian and coalition personnel and to offer support to the Iraqi security forces will be put in place as part of the new force.

We also intend to deploy a small helicopter detachment with aircrew and support personnel. This will provide safe, reliable and dedicated transport for our troops and for our *materiél* and equipment and be used *in extremis* for casualty evacuation.

Although there are many risks associated with this new operation, the Canadian Armed Forces are well trained, prepared and ready to participate in this train, advise and assist mission. Indeed, we will prevail.

Such missions belong to a new chapter for Canada on the operational spectrum, where we and others support those inside conflict zones for their benefit, as well as to meet coalition and Canadian objectives.

[*Translation*]

We continue to operate as part of the coalition, and we are all in the battle against ISIL together. In this armed conflict, the coalition continues to successfully target ISIL's personnel, infrastructure, command and control nodes, equipment and supply routes.

It has prevented ISIL from retaking territory and is continuing its mission to halt, degrade, and ultimately defeat ISIL. Defeating ISIL will require well-trained, well-advised and well-assisted ground forces.

[*English*]

Therefore the coalition is intensifying all lines of effort, including train, advise and assist missions to ensure local forces are successful. The other lines of operation include stabilization,

Dans le cadre de l'Opération IMPACT, on se concentrera sur la formation, la prestation de conseils et l'assistance avec les forces kurdes dans le Nord. Nous allons aussi considérablement augmenter nos capacités en matière de renseignement. Notre ravitailleur en vol Polaris et notre aéronef de surveillance Aurora continueront de servir d'instruments essentiels à l'effort de la coalition.

Nous fournirons également une équipe de liaison ministérielle au gouvernement de l'Irak dans le cadre des efforts de la coalition. L'équipe aidera à communiquer avec les ministères irakiens et sera dirigée par un officier général canadien.

On réalisera des efforts de renforcement des capacités en Jordanie et au Liban, même si on en détermine encore la portée en ce moment.

Dans le cadre de la facilitation de la nouvelle force, on assurera une plus grande présence médicale à l'appui du personnel canadien et de la coalition et de l'assistance aux forces de sécurité irakiennes.

Nous avons l'intention de déployer un petit détachement d'hélicoptères avec équipage et personnel de soutien. Cette mesure fournira un transport sécuritaire, fiable et spécialisé pour nos troupes, notre matériel et notre équipement, et sera utilisée, in extremis, pour évacuer des victimes.

Bien qu'il y ait de nombreux risques associés à cette nouvelle opération, les Forces armées canadiennes sont bien formées et prêtes à participer à cette mission de formation, de prestation de conseils et d'assistance. Et soyez assurés que nous vaincrons.

De telles missions font partie d'un nouveau chapitre pour le Canada en ce qui concerne le spectre opérationnel, où, comme d'autres, nous appuierons ceux et celles dans les zones de conflit pour leur venir en aide et pour atteindre les objectifs de la coalition et du Canada.

[*Français*]

Nous continuons à mener nos opérations à titre de membre de la coalition, et nous sommes tous ensemble dans la lutte contre l'État islamique. Dans ce conflit armé, la coalition continue et réussit à cibler le personnel, l'infrastructure, les centres de commandement et de contrôle, l'équipement et les routes d'approvisionnement de l'État islamique.

Elle a empêché l'État islamique de reconquérir du terrain et elle continue sa mission pour arrêter, dégrader et ultimement vaincre l'État islamique. La défaite de l'État islamique nécessitera des forces terrestres bien formées, bien conseillées et bien assistées.

[*Traduction*]

La coalition intensifie donc toutes les lignes d'effort, y compris la formation, la prestation de conseils, et l'aide aux missions, de manière à s'assurer que les forces locales réussissent leurs

stopping ISIL finances, counter-messaging and stopping foreign fighter flow.

Local forces want to continue to be successful, and they welcome our support. They have already countered ISIL throughout Iraq, including on the Kurdish-held northern front lines.

So the degradation continues, and we have played an active role. I'm very proud of the CF-18 contributions to the coalition's efforts to stop ISIL militarily in Iraq and contribute to their degradation. We are working towards this next phase of the campaign because the realities of the mission demand it. The mission is evolving.

We started in the North, and we're continuing in the North. We developed relationships there, and it's critical terrain. The ultimate objective, I think, in the mid to long term, will be the Iraqi Security Forces' effort to free Mosul. Where we are deploying, we will be providing support to those who are working to contain ISIL in Mosul and ultimately lead to their defeat there. We will work with our partners in Northern Iraq, where we've developed those strong relationships, and in doing so help to assure the defence and security of Northern Iraq as well, providing, in its unstable environment, an element of stability as the campaign continues. But the whole-of-government effort Canada is undertaking will also address the region as a whole.

[*Translation*]

Ladies and gentlemen, our refocused military mission against ISIL is part of a comprehensive approach to the region, which is made up of our military contributions, as well humanitarian assistance, development and diplomatic efforts.

[*English*]

The coalition will continue to target ISIL's personnel infrastructure, command and control nodes, their equipment and their supply routes. We will continue to train local and indigenous forces to enable them to stabilize the northern flank with increased capacity and capabilities.

Our efforts will further empower local forces, enhance intelligence and support local governance and coalition forces. It will have risks, but our personnel are well trained and ready.

I'm intensely proud of the work we have done and will continue to do. We always stand ready to deliver for Canada and Canadians and for those in the world that Canada has decided to support militarily.

Thank you.

opérations. Les autres volets opérationnels incluent la stabilisation, la saisie des finances de l'EIIL, les messages pour contrer les messages extrémistes et l'interruption des flux de combattants étrangers.

Les forces locales veulent continuer à réussir leurs missions et accueillent favorablement notre soutien. Elles ont déjà contré l'EIIL partout en Irak, incluant les lignes de front du Nord dirigées par les Kurdes.

La dégradation se poursuit donc, et nous avons joué un rôle actif. Je suis très fier de la contribution des CF-18 dans le cadre des efforts de la coalition visant à arrêter l'EIIL au moyen de forces militaires en Irak et à contribuer à la dégradation de ce groupe. Nous nous tournons vers la prochaine étape de la campagne puisque les réalités de la mission l'exigent. La mission évolue.

Nous avons commencé dans le Nord, et nous continuons dans le Nord. Nous avons établi certains liens à cet endroit, et concernant son terrain crucial. Selon moi, l'objectif ultime, à moyen ou long terme, est de faciliter les efforts des forces de sécurité irakiennes pour libérer Mossoul. De notre zone de déploiement, nous fournirons un soutien à ceux qui luttent pour contenir l'EIIL à Mossoul et, au bout du compte, le vaincre à cet endroit. Nous continuerons notre travail avec nos partenaires dans le nord de l'Irak, où nous avons créé des liens solides, et, ce faisant, les aiderons aussi à assurer la défense et sécurité dans le nord de l'Irak, favorisant ainsi, dans un environnement instable, une certaine stabilité tandis que la campagne se poursuit. L'effort pangouvernemental auquel le Canada participe s'attachera cependant à l'ensemble de la région.

[*Français*]

Mesdames et messieurs, notre mission militaire redéfinie contre l'État islamique fait partie d'une approche exhaustive dans la région. Elle comprend nos contributions militaires, l'aide humanitaire, ainsi que des efforts diplomatiques et de développement.

[*Traduction*]

La coalition continuera à cibler le personnel, l'infrastructure, les nœuds de commandement et de contrôle, le matériel et les routes d'approvisionnement de l'EIIL. Nous continuerons à former des forces locales et indigènes afin de leur permettre de stabiliser le flanc nord avec plus de capacités et compétences.

Nos efforts accroîtront les capacités des forces locales et du renseignement, et appuieront le gouvernement local et les forces de la coalition. La mission comporte des risques, mais notre personnel est bien formé et prêt à les affronter.

Je suis extrêmement fier du travail que nous avons réalisé et que nous continuerons à effectuer. Nous sommes toujours prêts à faire notre mieux pour le Canada et les Canadiens, ainsi pour ceux et celles que le Canada a décidé de soutenir militairement.

Merci.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*Translation*]

Senator Dagenais: General Vance, thank you very much for your testimony. I would like to come back to Operation Impact, which was carried out in Iraq and Syria with a view to neutralizing the Islamic State. I would like you to tell us about the success of your contribution to military operations. In addition, how do you view your future operations, which will include members of the Canadian Armed Forces?

Gen. Vance: Thank you, senator. I am more comfortable answering your question in English.

[*English*]

Gen. Vance: You asked two questions: to describe the successes to date and then look ahead to next operations.

If you recall, back in 2013 and 2014, as ISIL was developing, Canada participated with a number of coalition nations in a rapid response to the region. It was an emergency situation. ISIL was advancing down the Euphrates and Tigris River valleys. Baghdad was their objective, and their momentum had increased dramatically as a result of the Iraqi Security Forces failing to halt their advance. The immediate reaction of our allies was to stop ISIL, prevent the collapse of Baghdad and try to stabilize the situation as much as possible. The initial mission was to militarily stop ISIL in Iraq, support the training necessary to put Iraqi Security Forces back on the offensive, ultimately contribute to wider regional stability by looking at Syria, and then manage regional dynamics such that regional actors, nations, could participate in this coalition, providing a wider element of stability.

The coalition as a whole absolutely, categorically stopped ISIL in Iraq. They were stopped. It's a challenging, determined enemy, and they adapt, as does any force. They adapt to the pressure that the coalition puts on them. That means they stopped advancing on a large front, and you've seen the TV coverage with flags and armoured columns. They can't do that anymore. The air power and the Iraqi Security Forces that were in place at the time have effectively stopped.

Now there have been some minor and in some cases — in Ramadi — very substantial skirmishes and battles on the periphery. But, ultimately, there have been no game changers, and ISIL has been pushed back, losing about 40 per cent of the territory that they had taken over.

Nonetheless, it wasn't just a matter of stopping them. The coalition nations wanted to degrade and ultimately defeat ISIL. The defeat of ISIL militarily in Iraq will come as a result of continued degradation, which we participated in, and ultimately putting Iraqi Security Forces on the offensive so that they can reclaim their terrain, clear ISIL from within their country and re-establish the reach of governance that is necessary to go in behind where ISIL has been.

[*Français*]

Le sénateur Dagenais : Général Vance, merci beaucoup pour votre témoignage. J'aimerais revenir à l'opération Impact qui s'est déroulée en Irak et en Syrie, toujours dans le but de neutraliser l'État islamique. J'aimerais que vous nous parliez du succès de votre contribution sur le plan des opérations militaires. Aussi, comment voyez-vous la perspective de vos prochaines opérations, qui incluront les membres des Forces armées canadiennes?

Gén Vance : Merci, sénateur. Je suis plus à l'aise de répondre en anglais.

[*Traduction*]

Gén Vance : Vous me demandez deux choses : de décrire les réussites jusqu'à présent, et de parler des prochaines opérations.

Si vous vous rappelez bien, en 2013 et en 2014, lorsque l'EIIL gagnait du terrain, le Canada a participé, avec un certain nombre d'États de la coalition, à une intervention rapide dans la région. Il s'agissait d'une situation d'urgence. L'EIIL progressait dans les vallées de l'Euphrate et du Tigre. Son objectif était Bagdad, et sa progression s'est accélérée considérablement en raison de l'incapacité des forces de sécurité irakiennes à freiner son avancée. La réaction immédiate de nos alliés consistait à arrêter l'EIIL, à prévenir la chute de Bagdad et à essayer de stabiliser le plus possible la situation. La mission initiale était d'arrêter militairement l'EIIL en Irak, d'offrir un soutien nécessaire en matière de formation pour permettre aux forces de sécurité irakiennes de reprendre l'offensive et, au bout du compte, de contribuer à la stabilité générale de la région en se tournant vers la Syrie, puis en gérant la dynamique régionale, de façon à ce que les intervenants et les États de la région puissent participer à la coalition et ainsi accroître la stabilité.

Dans l'ensemble, la coalition a arrêté l'EIIL net en Irak. On a freiné son avancée. C'est un ennemi difficile et déterminé et il s'adapte, comme toute force le fait. L'EIIL s'adapte aux pressions exercées par la coalition. Cela signifie qu'il a arrêté d'avancer sur de larges fronts; vous avez tous vu à la télévision les colonnes de blindés, drapeaux battants. Il ne peut plus le faire. La puissance aérienne et les forces de sécurité irakiennes qui étaient en place à ce moment-là l'ont arrêté efficacement.

Il y a eu bien sûr, en périphérie, des échauffourées et des batailles mineures ou, dans certains cas, très importantes, comme à Ramadi. Cependant, au bout du compte, rien n'a vraiment changé la donne, et l'EIIL a été repoussé. Il a perdu environ 40 p. 100 du territoire qu'il avait envahi.

Cependant, l'objectif n'était pas seulement d'arrêter ces combattants. Les États de la coalition voulaient miner l'EIIL et, au bout du compte, le vaincre. La défaite militaire de l'EIIL en Irak découlera de la dégradation continue de ses forces, processus auquel nous participons, et, un jour, lorsque les forces de sécurité irakiennes pourront reprendre l'offensive et récupérer le terrain perdu, chasser l'EIIL de leur pays et rétablir leur influence pour récupérer les régions perdues aux mains de l'ennemi.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

There is a lot of support politically that Iraq will need to do this — to remain a viable, unitary state that will effectively govern its people. That, I would suggest to you, is the ultimate state we want to get to.

The military part of this operation is condition-setting for that. Get rid of the clear and present danger of ISIL. Defeat ISIL *in situ* by, with and through Iraqi Security Forces.

Canada's part in this, I think, was tremendous. We responded very quickly with the CF-18s as part of a coalition air effort to stop this very rapidly advancing enemy, and that happened. We also contributed intelligence assets, air refuelling to support the other coalition efforts, and some key staff officers throughout the area, and we started with a modest train, advise and assist mission with Iraqi Kurds. All of that contributed to the North, with our coalition allies and the Peshmerga and the Kurds being relatively stable along the line they established, and to our part in ensuring that ISIL was stopped, that degradation commenced and that our staff officers contributed to overall campaign management.

The next steps in this campaign militarily — I stress "militarily" because the defeat of ISIL in all of its forms, its ideology, its attractiveness to the disenfranchised, will take a wide effort that involves a political solution and addressing some of the causes as to why this happened. Our role in Operation IMPACT is to look at the military situation in Iraq and Syria, but principally Iraq.

The next steps are to increase the holding power, the defensive capability, and improve, through the train, advise and assist mission, the performance of Peshmerga forces in the North, such that they can hold and effectively repel any ISIL attacks and contribute to the effort that will, over the next several months, develop. It's very difficult to put a timeline on it, but, in 2016 or 2017, I would suggest to you that the battle for Mosul will develop. It's already starting.

If you think of Ramadi, that was a difficult battle, lots of back and forth. Iraqi Security Forces have been largely successful there. It's not entirely complete. Ramadi will be a city inside Iraq that is going to need a great deal of attention from the government in terms of providing services and so on, but, militarily, Ramadi is almost done.

The next significant battle — and potentially the last significant battle of this campaign — with the fall of Mosul and ISIL eliminated from Mosul, could very well see the end of Mosul being militarily significant in any way in Iraq, at least for the time

L'Irak aura besoin de beaucoup de soutien politique pour y arriver et rester un État uni et viable capable de gouverner de façon efficace sa population. Voilà, à mon avis, notre objectif ultime.

Le volet militaire de cette opération vise à mettre en place les conditions pour y arriver. Il faut se débarrasser du danger immédiat que représente l'EIIL : les forces de sécurité irakienne doivent vaincre l'EIIL sur place; c'est avec et par eux qu'on y arrivera.

Le rôle du Canada dans ce processus était, selon moi, majeur. Nous avons réagi très rapidement avec nos CF-18 dans le cadre des efforts aériens de la coalition pour freiner l'avancée très rapide de l'ennemi, et ça a été une réussite. Nous avons aussi fourni des actifs liés au renseignement et un soutien en matière de ravitaillement en vol dans le cadre des autres efforts de la coalition et grâce à la présence d'officiers d'état-major clés un peu partout dans la région. En outre, nous avons entrepris une mission modeste de formation, de consultation et d'assistance auprès des Kurdes irakiens. Tout cela a été bénéfique dans le Nord, où nos alliés de la coalition et les Peshmergas et les Kurdes bénéficient d'une situation relativement stable le long de la ligne de front qu'ils ont établie. Ces efforts nous ont aussi permis de jouer notre tôle et de nous assurer que l'EIIL est arrêtée, que le processus de dégradation commence et que nos officiers d'état-major contribuent à la gestion générale de la campagne.

Les prochaines étapes dans cette campagne militaire — et je souligne qu'il s'agit d'une campagne « militaire », parce que vaincre l'EIIL sous toutes ses formes, son idéologie et le fait qu'elle soit attrayante pour les laissés pour compte, exigera de grands efforts, y compris une solution politique et des efforts pour éliminer certaines causes sous-jacentes à la situation. Notre rôle dans le cadre de l'Opération IMPACT est d'examiner la situation militaire en Irak et en Syrie, mais principalement en Irak.

Les prochaines étapes consistent à accroître la force de maintien, à renforcer les capacités défensives et à améliorer, grâce à la mission de formation, de consultation et d'assistance, le rendement des forces peshmergas dans le Nord, afin qu'elles puissent tenir leurs positions et repousser efficacement les attaques de l'EIIL et contribuer aux efforts des prochains mois. C'est très difficile de définir un calendrier, mais, selon moi, en 2016 ou en 2017, on luttera pour Mossoul. En fait, le processus est déjà enclenché.

Dans le cas de Ramadi, la bataille a été difficile, et il y a eu beaucoup d'avancées et de reculs. En général, les forces de sécurité irakiennes ont connu du succès là-bas. Ce n'est pas totalement fini. Ramadi est une ville d'Irak que le gouvernement devra vraiment avoir à l'œil en ce qui a trait à la prestation des services et ce genre de choses, mais, d'un point de vue militaire, le travail à Ramadi est presque fini.

La prochaine bataille importante — et peut-être la dernière grande bataille de cette campagne — visera à concrétiser la chute de Mossoul et à en expulser l'EIIL. Mossoul arrêtera peut-être par le fait même d'être un pôle militaire important en Irak, du

being. We don't know how that battle will go. That battle has yet to be designed. It will be conducted by Iraqi Security Forces. They have to get trained. They need the numbers to be able to handle that incredibly difficult fight. ISIL has been preparing defensive positions in Mosul for a long time. It's a defended city. We will be on terrain that essentially surrounds the northern and eastern flanks of Mosul, though not right on the city limits, with the Peshmerga. Therefore, the Kurdish forces there will form a strong part of the contain function, to prevent ISIL from being able to escape easily from Mosul. The Mosul dam will be in our vicinity, a key piece of infrastructure that the coalition is determined to help Iraq maintain in good order. It's a question mark whether or not it will hold.

So this battle develops and is completed in the next two years, potentially. No military estimate can determine exactly when it will happen, but that's when we hope it will happen.

To get to that point, ISIL still needs to be targeted well by coalition air forces and by Iraqi ground forces. The battle has to be won elsewhere. Ultimately, we'll be contributing to that through increased staff in the coalition; increased intelligence capacity through the Auroras and through our own process to allow for even greater and more effective and rapid targeting of ISIL on the ground; and, finally, with our forces in the North supporting that contain function.

Senator Day: General, thanks for being here.

Could you clarify for the record whether the coalition is a coalition of the willing, coalition of the United Nations, or a coalition of NATO members?

Gen. Vance: It's a coalition of the willing, senator. It consists of over 60 nations all up, 40 nations contributing military forces.

Senator Day: Thank you.

I think you made the point, but perhaps we could expand on it a bit. You're going up to 830 personnel under the revised coalition. Is this coalition terminology of whole-of-government or is that just Canada's terminology? Are we within the coalition with respect to the whole-of-government aspect? Outside of the military portion of that, does it involve other countries as well as Canada?

Gen. Vance: Right. The 830 are contributing to the military coalition effort. The military part of this coalition, although your point is valid, the coalition is political as well. The nations have agreed to collaborate against this threat. The military part is, I suppose, more clearly defined as we put headquarters on the ground and contribute with command and control relationships that allow our forces to be used by coalition partners.

moins pour un certain temps. Nous ne savons pas de quelle façon cette bataille sera menée. Les plans n'ont pas encore été définis. Elle sera menée par les forces de sécurité irakiennes, dont les troupes doivent être formées. Il doit y avoir suffisamment de combattants pour mener un combat qui sera extrêmement difficile. L'EIIL prépare ses positions défensives à Mossoul depuis longtemps. C'est une ville défendue. Nous occuperons des terrains qui, essentiellement, entourent les flancs nord et est de Mossoul, sans être directement aux limites de la ville, avec les Peshmergas. Par conséquent, les forces kurdes là-bas joueront un rôle important pour contenir l'EIIL et empêcher ses combattants de fuir facilement Mossoul. Le barrage de Mossoul sera dans notre secteur. Il s'agit d'une infrastructure que la coalition est déterminée à aider les Irakiens à maintenir en bon état. On ne sait pas encore s'il tiendra.

Cette bataille aura donc lieu et pourrait être terminée d'ici un an ou deux. Aucune estimation militaire ne permet de déterminer exactement quand cela se produira, mais c'est ce que nous espérons.

Pour y arriver, il faut que les forces aériennes de la coalition et les forces irakiennes sur le terrain continuent de cibler efficacement l'EIIL. Il faut gagner la bataille ailleurs. Au bout du compte, nous contribuerons à la lutte en augmentant les effectifs de la coalition, en renforçant la capacité de renseignement grâce aux Aurora et à notre propre processus, qui nous permet d'être plus efficaces et de cibler rapidement l'EIIL sur le terrain et, enfin, grâce à nos forces dans le Nord qui soutiennent la fonction de confinement.

Le sénateur Day : Général, merci d'être là.

Pouvez-vous préciser, pour le compte rendu, si la coalition est une coalition de pays volontaires, une coalition des Nations Unies ou une coalition des membres de l'OTAN?

Gén Vance : Il s'agit d'une coalition de pays volontaires, monsieur le sénateur. Elle est composée de plus de 60 États en tout, et 40 États participent militairement.

Le sénateur Day : Merci.

Je crois que vous en avez déjà parlé, mais nous pourrions peut-être en dire plus à ce sujet. Il y aura jusqu'à 830 militaires déployés dans le cadre des efforts de la nouvelle coalition. Est-ce du point de vue pangouvernemental de la coalition ou seulement dans la perspective canadienne? Fait-on partie de la coalition du point de vue pangouvernemental? Outre la dimension militaire, d'autres pays en font-ils partie, en plus du Canada?

Gén Vance : D'accord. Les 830 militaires contribuent aux efforts de la coalition militaire. Le volet militaire de cette coalition, même si votre point est valide... La coalition est aussi de nature politique. Les États ont accepté de travailler en collaboration pour combattre la menace. Le volet militaire est, j'imagine, mieux défini, puisqu'un quartier général a été aménagé sur le terrain et qu'on contribue par l'intermédiaire d'un commandement et de liens de contrôle, qui permettent à nos forces d'être utilisées par les partenaires de coalition.

That said, it is a wider coalition. It has aspirations among multiple lines of effort — stabilization, humanitarian support, countering the ISIL message, stopping foreign fighters. It takes a multi-agency, whole-of-government effort to try to deal with this. Many nations are contributing to that. Not all nations contribute the same way. Canada, in this mission, has decided to contribute in a particular way.

I think it's correct to say that the coalition of the willing is largely used to describe the military coalition, but I think it's accurate to say that this is a coalition of nations that are using any number of instruments of power and persuasion to deal with this.

Senator Day: To round this out, the number of 830 is military personnel only. Can you give us the global figure for Canada of the whole-of-government approach? How many more?

Gen. Vance: I don't have those figures available, senator, in terms of numbers of other Canadians that will be on the ground participating and contributed by the departments of the Government of Canada.

Senator Day: Is there a budget for this whole-of-government approach that was recently announced? Do we know what other departments or who is coordinating all of the government activities?

Gen. Vance: The military part of this, the approximately $300 million —

The Chair: Per year?

Gen. Vance: — for one year has been announced. I'm not really in a position to answer how the other government departments will be coordinated.

We do know that where they touch the military directly, we will actively coordinate with them be it for intelligence gathering or for diplomatic activities in Baghdad or elsewhere. I'll give you an example.

As we look at the capacity-building effort in Lebanon and Jordan, as we scope those missions out, there may be roles for military as well as other government departments to meet the needs of those two nations. At this stage, however, I don't have any details on how those other government departments will contribute, although they already are in many ways, including the tracking of foreign fighters.

Senator Day: But you're not meeting together here in Canada?

Cela dit, c'est une coalition plus vaste. Elle a des aspirations multiples relativement aux efforts : stabilisation, soutien humanitaire, messages visant à contrer l'idéologie de l'EIIL et arrestation des combattants étrangers. Il faut un effort multiorganismes et pangouvernemental pour y arriver. Beaucoup d'États participent à ces efforts. Tous les États ne participent pas de la même façon. Dans le cadre de cette mission, le Canada a décidé de participer d'une façon précise.

On peut probablement dire que la notion de coalition des pays volontaires est utilisée principalement pour décrire l'effort militaire, mais je crois qu'il faut aussi dire qu'il s'agit d'une coalition d'États qui utilisent toute une gamme d'instruments de pouvoir et de persuasion pour gérer la situation.

Le sénateur Day : En résumé, les 830 sont composés uniquement de militaires. Pouvez-vous nous donner un chiffre global de la participation pangouvernementale canadienne? Combien de personnes de plus?

Gén Vance : Je n'ai pas de chiffres, monsieur le sénateur, en ce qui a trait au nombre d'autres Canadiens qui seront sur le terrain, qui pourront participer et qui sont employés par les autres ministères du gouvernement du Canada.

Le sénateur Day : Un budget lié à cette approche pangouvernementale a-t-il récemment été annoncé? Savez-vous quels autres ministères ou quels autres intervenants coordonnent l'ensemble des activités du gouvernement?

Gén Vance : Le budget militaire s'élève à environ 300 millions de dollars...

Le président : Par année?

Gén Vance : ... pour une année; c'est ce qui a été annoncé. Je ne peux pas vraiment vous dire de quelle façon les autres ministères seront coordonnés

Nous savons cependant que, lorsqu'il sera directement question de l'armée, nous assurerons une coordination active avec eux, que ce soit pour la collecte de renseignements ou dans le cadre d'activités diplomatiques à Bagdad ou ailleurs. Je vais vous donner un exemple.

Tandis que nous examinons les efforts de renforcement des capacités au Liban et en Jordanie et que nous déterminons la portée de ces missions, certains rôles devront peut-être être assumés par des militaires, et d'autres, par des ministères du gouvernement, afin de répondre aux besoins de ces deux États. En ce moment, cependant, je n'ai pas de renseignements sur la façon dont les autres ministères du gouvernement participeront, même s'ils participent déjà de bien des façons, y compris en faisant un suivi des combattants étrangers.

Le sénateur Day : Mais vous ne vous réunissez pas ici, au Canada?

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Gen. Vance: For those things that affect my part of the campaign, we do meet with other government departments to determine what it is that we're going to do and how we actually operationalize that.

The Chair: That's an interesting question. I don't know, General Vance, if you can take it upon yourself to ask the various departments, or whomever it is, to provide us with the overall information so that we all know, including yourself, just exactly what we are committed to doing over there.

Gen. Vance: Perhaps I didn't quite understand your question. The overall Canadian effort has many parts to it. For example, the movement of Syrian refugees out has been a part of relieving the region of part of the challenges that they're dealing with. To contribute to development assistance, that is largely done through the good offices of the Canadian government but through partners on the ground. I don't have a military connection directly to that. I'm an expert at where we have a military connection to the whole-of-government effort. Where we do not, we can certainly participate in a wider response.

The Chair: General, we'll inquire of other agencies.

[*Translation*]

Senator Carignan: Thank you, General, for joining us. I have several questions for you.

First of all, my question is for the army general: Are we at war against ISIL?

Gen. Vance: Thank you for asking me this question.

[*English*]

I've seen this question asked before. I want to be perfectly clear with you about the use of the term "war." I think it is asked sometimes as a way to clarify something that is so complex as to try and boil it down to a single word. The word "war" today is used to describe many things. It's used to describe a major effort, a major undertaking — the war on drugs or the war on poverty. You can name any number of things that have the word "war" attached to it.

"War," as a legal state between two states, is one way of looking at war and largely has not been used for a long, long time. It's been addressed by the Kellogg-Briand Pact and by the UN Charter. It is simply not used in this context today. We are party to an armed conflict against a non-state actor. That's the legal terminology. We are a lawful party to an armed conflict against a non-state actor.

Gén Vance : En ce qui a trait aux éléments qui ont un impact sur l'aspect de la campagne dont je suis responsable, nous rencontrons des représentants d'autres ministères du gouvernement pour déterminer ce que nous prévoyons faire et de quelle façon nous procéderons sur le terrain.

Le président : C'est une question intéressante. Je ne sais pas, général Vance, si vous pourriez demander aux divers ministères — ou peu importe qui sont les responsables — de nous fournir des renseignements généraux afin que nous puissions tous savoir — vous y compris — ce que nous nous sommes engagés à faire exactement là-bas.

Gén Vance : Je n'ai peut-être pas bien compris votre question. En général, le Canada participe sur de nombreux fronts. Par exemple, le déplacement des réfugiés syriens est l'une des choses qui ont été faites dans la région pour éliminer certaines des difficultés auxquelles les gens sont confrontés. Pour ce qui est de la contribution liée à l'aide au développement, ce travail est confié en grande partie aux bons soins du gouvernement canadien, mais aussi d'autres partenaires sur le terrain. Je n'ai aucun lien militaire direct relativement à ces choses. Mon expertise concerne la façon dont l'effort militaire s'inscrit dans l'effort pangouvernemental. Lorsque ce n'est pas le cas, nous pouvons assurément participer à une intervention plus générale.

Le président : Général, nous nous renseignerons auprès d'autres organismes.

[*Français*]

Le sénateur Carignan : Merci, général, d'être présent parmi nous. J'ai quelques questions à vous poser.

Premièrement, je m'adresse au général de l'armée : sommes-nous en guerre contre l'État islamique?

Gén Vance : Je vous remercie de me poser cette question.

[*Traduction*]

Ce n'est pas la première fois qu'on pose cette question. Je veux être parfaitement clair avec vous au sujet de l'utilisation du mot « guerre ». Je crois qu'on pose parfois cette question pour essayer de comprendre une situation extrêmement complexe en la résumant en un mot. Ce mot, « guerre », est utilisé de nos jours pour décrire de nombreuses choses : on l'utilise pour décrire un effort majeur, une grande entreprise, comme la guerre contre la drogue ou la guerre contre la pauvreté. Il y a beaucoup de choses auxquelles on associe le mot « guerre ».

La « guerre » en tant que situation juridique entre deux États est l'une des définitions possibles, mais elle n'a pas été utilisée depuis fort longtemps. Cette question a été abordée dans le Pacte Kellogg-Briand et la Charte des Nations Unies. On ne l'utilise tout simplement plus dans ce contexte de nos jours. Nous participons à un conflit armé contre un adversaire non étatique. Voilà pour la terminologie juridique. Nous sommes une partie licite à un conflit armé contre un adversaire non étatique.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

The word "war" doesn't enter the lexicon, and it doesn't necessarily matter. From my perspective, it doesn't change the status of my forces. Whether we put the "war" word against it, it doesn't alter the benefits and allowances that the soldiers get. What guides the mission is the intent of the Government of Canada and the tasks that come out of that and the tasks, ultimately, that I assign the forces.

To answer your question specifically, no, Canada is not at a declared state of war.

[*Translation*]

Senator Carignan: Your answer is interesting; it makes reference to legal and recognized states, namely, typical states.

Part of your answers also demonstrated your approach to borders. However, it seems that in this region, borders no longer count. States that normally lead or manage institutions no longer do so; these are traditional states that we are seeing. There are many radical groups. Furthermore, the Tony Blair Faith Foundation claimed that 75 per cent to 80 per cent of the groups fighting Assad were Islamic radicals. It is hard to know what is what.

However, can you tell us which groups the Canadian Armed Forces are working with? Who are the good guys and who are the bad guys? With which groups have we had positive experiences and who are our opponents? Whether it be in Iraq, Syria, Lebanon, Jordan, Libya or Yemen, can you give us a list of our friends and foes?

[*English*]

Gen. Vance: Our allies in Iraq are the coalition and, ultimately, the Iraqi government. Our adversary in Iraq is the Islamic State, ISIL. That's our adversary.

We are not conducting military operations in Syria in this refocused mission, but the adversaries throughout the region are many. The challenges are many. Ultimately, the ISIL phenomenon that grew out of Syria and Iraq is our principal focus.

But I think the world has agreed and is trying to wrestle to find ways to get to a solution in Syria that will involve and has been involving military force. From the coalition's perspective and from Canada's perspective, the adversary of note is ISIL.

There are others involved in Syria, and that's what makes it so complex and doesn't lend itself to a simple solution. There are many other groups at play, such as the regime forces and those who are opposing the regime but who would also oppose ISIL. There's ISIL. There are various subordinate actors to ISIL in the region, such as the al-Nusra Front, as well as various types of other forces, indigenous and foreign, that make Syria intensely complex.

Le mot « guerre » ne fait pas partie du lexique, et cela n'a pas nécessairement d'importance. De mon point de vue, cela ne change rien au statut de mes forces. Qu'on associe le mot « guerre » à ce qui se passe ne modifie en rien les avantages et les indemnités que les soldats reçoivent. Ce qui oriente la mission, c'est l'intention du gouvernement du Canada et les tâches qui en découlent de même que les tâches qui, au bout du compte, sont attribuées aux forces.

Donc pour répondre précisément à votre question, non, le Canada n'a pas déclaré l'état de guerre.

[*Français*]

Le sénateur Carignan : Votre réponse est intéressante; elle fait référence aux États tels qu'ils se situent dans un monde légal et reconnu, soit des États typiques.

Une partie de vos réponses a aussi démontré votre approche en ce qui concerne les frontières. Cependant, il semble que dans cette région, les frontières ne tiennent plus. Les États qui mènent ou gèrent normalement les institutions ne le font plus, ce ne sont pas les mêmes États traditionnels que l'on voit. Il y a une multitude de groupes radicaux. La fondation Tony Blair a d'ailleurs affirmé que de 75 à 80 p. 100 des groupes qui se battaient contre Assad étaient des radicaux islamiques. Il est difficile de s'y retrouver.

Cependant, pouvez-vous nous dire avec quels groupes travaille l'armée canadienne? Qui sont les bons et qui sont les vilains? Avec quels groupes a-t-on des échanges positifs et qui sont les adversaires? Que ce soit en Irak, en Syrie, au Liban, en Jordanie, en Lybie ou au Yémen, pouvez-vous nous donner une liste de nos adversaires et de nos amis?

[*Traduction*]

Gén Vance : Nos alliés en Irak sont la coalition et, au bout du compte, le gouvernement irakien. Notre adversaire en Irak, c'est l'État islamique, l'EIIL; c'est notre adversaire.

Nous ne menons pas d'opérations militaires en Syrie dans le cadre de cette mission recentrée, mais il y a de nombreux adversaires dans la région. Les défis sont nombreux. Au bout du compte, le phénomène de l'EIIL qui a vu le jour en Syrie et en Irak est notre principale cible.

Cependant, je crois que les intervenants mondiaux sont d'accord et qu'ils essaient de trouver une solution en Syrie qui n'exigera pas une intervention militaire. Du point de vue de la coalition et du point de vue du Canada, notre adversaire digne de mention est l'EIIL.

Il y a d'autres intervenants en cause en Syrie, et c'est ce qui rend la situation aussi complexe et ce qui ne se prête pas à une solution toute simple. Il y a de nombreux autres groupes en jeu, comme les forces du régime et celles qui s'opposent au régime, mais qui s'opposent aussi à l'EIIL. Puis il y a l'EIIL. Il y a aussi de nombreuses entités subordonnées à l'EIIL dans la région, comme le Front al-Nusra et divers types d'autres forces, nationales et étrangères, qui rendent la situation en Syrie extrêmement complexe.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

At this point in time, Canada is not conducting operations against any forces in Syria.

To go wider, from a military mission and planning perspective in the wider region, particularly in Lebanon and Jordan, the adversary is anything that would deliberately destabilize those two countries and therefore contribute to wider regional instability, which would just not be productive or useful, nor would it contribute to an ultimate resolution of this conflict.

I'll end by saying that I think it's well known and well understood that we are in the midst of a wider conflict — a conflict that has been going on for millennia, with challenges that have been going on for a long time between two major sects of the Islam faith, Shia and Sunni, regional power posturing that pits Iran and Saudi Arabia against each other, and various proxy efforts that go on as a result.

I can't sit here and tell you that it's all clear as to how we will proceed. At this point in time, the contribution of Operation IMPACT is to deal with a clear and present massively destabilizing effort that is causing untold harm to civilians and that could potentially contribute to wider, faster and more dangerous destabilization of the region. So the military defeat of ISIL in Iraq is our principal effort now.

I believe Canada, like other nations, will track very closely and contribute where they can regionally. We are doing that, in part.

Senator Kenny: General, I just wanted to go back briefly to the all-of-government concept that Senator Day raised. It's my impression that an all-of-government approach is somewhere between a "mixed bag" and a "disaster." This committee, when it first went to Kabul in Afghanistan a little over a decade ago, we found that the colonel who was commanding Camp Julien had never met Chris Alexander, who was our ambassador there. We found similar problems on subsequent visits going back. Our impression was that the CF had their act together, but it was very hard to tell what the rest of government was doing.

This isn't something that you're accountable for. Having said that, I have a bit of the impression that we're going down the same road when I hear "all of government" in that the CF is doing stuff, but nobody is quite sure what anyone else is doing.

Gen. Vance: I think we do know what we're doing as a country. It's been announced and spoken to by ministers as to what each ministry is undertaking in the region.

There are marked differences between this mission and the events and operations that will make up the mission, and Afghanistan. In Afghanistan, for example, we had territorial responsibility — "battle space ownership," we call it. We don't

En ce moment, le Canada ne mène pas d'opérations contre des forces en Syrie.

À plus grande échelle, du point de vue de la mission militaire et de la planification dans la région tout entière, particulièrement au Liban et en Jordanie, l'adversaire, c'est toute entité qui tente sciemment de déstabiliser ces deux pays et, par conséquent, d'accroître l'instabilité à l'échelle de la région, ce qui n'est pas productif, ni utile et ne contribue pas à la résolution ultime du conflit.

Je terminerai en disant que, selon moi, les gens savent bien et comprennent qu'il s'agit d'un conflit plus général — un conflit qui dure depuis un millénaire —, qui concerne des problèmes de longue date entre deux branches majeures de l'islam, les chiites et les sunnites, qui luttent pour une position de puissance dans la région, et qui oppose l'Iran et l'Arabie saoudite, avec tous les efforts secondaires qui en découlent.

Je ne peux pas vous dire que nous savons tous exactement de quelle façon nous procéderons. En ce moment, la contribution de l'Opération IMPACT consiste à gérer les importants efforts clairs et évidents qui visent la déstabilisation, lesquels sont extrêmement préjudiciables pour les civils et pourraient contribuer à une déstabilisation plus générale, plus rapide et plus dangereuse dans la région. Par conséquent, la défaite militaire de l'EIIL en Irak est notre principale tâche en ce moment.

Je crois que, comme d'autres pays, le Canada suivra la situation de très près et apportera sa contribution là où il le pourra, à l'échelon régional. Nous faisons cela, en partie.

Le sénateur Kenny : Monsieur, je voulais simplement revenir brièvement sur la notion pangouvernementale qu'a soulevée le sénateur Day. J'ai l'impression qu'une approche pangouvernementale se situe quelque part entre le « fourre-tout » et le « désastre ». Lorsque nous — les membres du comité — sommes allés pour la première fois à Kaboul, en Afghanistan, il y a un peu plus de 10 ans, nous avons découvert que le colonel qui commandait le camp Julien n'avait jamais rencontré Chris Alexander, qui était notre ambassadeur là-bas. Nous avons observé des problèmes semblables au cours de visites subséquentes. Nous avions l'impression que les Forces canadiennes avaient les choses en main, mais il était très difficile de pouvoir dire ce que faisait le reste du gouvernement.

Il ne s'agit pas d'une chose dont vous êtes responsable. Cela dit, j'ai l'impression que nous empruntons la même voie lorsque j'entends le terme « pangouvernemental », puisque les Forces canadiennes font des choses, mais que personne n'est vraiment certain de ce que font les autres.

Gén Vance : Je pense que nous savons ce que nous faisons en tant que pays. Les activités entreprises par chaque ministère dans la région ont été annoncées et abordées par les ministres.

Il y a des différences marquées entre cette mission et les événements et les opérations qui constitueront la mission, et ce que l'on a connu en Afghanistan. En Afghanistan, par exemple, nous assumions une responsabilité territoriale — nous appelons

have that in Iraq. The Government of Iraq is the Government of Iraq, and their security forces are the ones who not only want to but need to address this. Their government apparatus, their ability to extend government, their ability to address the grievances and bring together a unitary state and address the challenges of governance writ large are their responsibility. We are there militarily to set conditions for them to ultimately be able to do that.

The whole-of-government effort, be it supporting the migration of refugees, to contributing to development and aid relief, capacity-building for borders and wider regional stability, is, perhaps in your experience, somewhat more indirect than you would have witnessed at the tactical level in Afghanistan

The Canadian Armed Forces in Afghanistan occupied a relatively small tactical footprint — an important one, nonetheless, but tactical. The money and effort that Canada spent through its whole-of-government approach, with expert officers to direct where the funds went, contributed to a wide range of government programs in Afghanistan.

So it didn't necessarily connect, and it didn't necessarily have to. When you're on a tight focus like you had in Kandahar, where we wanted the support of other government efforts to appear and be successful after we cleared territory, that's slightly different; that's counter-insurgency warfare. This is Iraq's war to fight, and we are supporting Iraq and the region with contributions through various Canadian government ministries and others to address a wider range than just the military effort.

If you look at the foreign fighter, we collaborate with allies and regional partners in an effort to stop foreign fighters. That's a whole-of-government effort. It's got funding, it's got people, and it's an important effort. It doesn't necessarily contribute directly to better security in the territory we're on or where we're flying from, but it does contribute to the region.

So I think in this case, in this operation, just like our coalition partners, everybody, I think, is largely undertaking the same efforts: contribute militarily to deal with the military problem, but there is a wider effort that includes all manner of governance and support to populations.

Senator Kenny: When we were at Camp Julien in Kabul, the principal operation of the Canadian soldiers who were there was evaluating the training that Afghans were getting, and they were very frustrated with their work. The reason they were frustrated was that at the time there was a restriction on them from going into combat with the soldiers they were training.

cela la « propriété du champ de bataille ». Nous n'avons pas cette responsabilité en Irak. Le gouvernement de l'Irak, c'est le gouvernement de l'Irak, et ses forces de sécurité sont celles qui non seulement veulent régler cette situation, mais qui doivent le faire. L'appareil gouvernemental, la capacité d'étendre le gouvernement, de régler les griefs, de favoriser un État unitaire et de régler les problèmes de gouvernance au sens large, c'est sa responsabilité. Nous y sommes, d'un point de vue militaire, pour fixer les conditions qui finiront par lui permettre de faire cela.

L'effort pangouvernemental — qu'il s'agisse d'appuyer la migration des réfugiés ou de contribuer aux mesures de développement et d'aide, au renforcement des capacités frontalières et à une plus grande stabilité régionale — est — peut-être, selon votre expérience — un peu plus directe que ce dont vous auriez été témoin d'un point de vue tactique en Afghanistan.

Les Forces armées canadiennes en Afghanistan occupaient un territoire tactique relativement petit — il n'en était pas moins important, mais il était tactique. L'argent et l'effort investis par le Canada grâce à son approche pangouvernementale, ainsi que les agents experts chargés d'acheminer les fonds, ont contribué à un vaste éventail de programmes gouvernementaux en Afghanistan.

Alors, des liens n'ont pas nécessairement été établis, et ça n'était peut-être pas nécessaire. Quand nos efforts sont extrêmement concentrés, comme à Kandahar, où nous voulions faire apparaître les efforts du gouvernement et connaître du succès après avoir dégagé le territoire, c'est légèrement différent; il s'agit d'une guerre anti-insurrectionnelle. C'est à l'Irak de mener cette guerre, et nous appuyons l'Irak et la région grâce à des contributions faites par l'entremise de divers ministères et autres organismes canadiens dans le but d'améliorer un vaste éventail d'aspects, pas uniquement l'effort militaire.

En ce qui concerne le combattant étranger, nous collaborons avec les alliés et les partenaires régionaux dans un effort visant à arrêter les combattants étrangers. Il s'agit d'un effort pangouvernemental. C'est financé, des gens y sont affectés, et il s'agit d'un effort important. Il ne contribue pas nécessairement directement à améliorer la sécurité dans le territoire où nous nous trouvons ou d'où provient notre aéronef, mais il contribue à la région.

Alors, je pense que, dans le cas de cette opération, tout comme nos partenaires de la coalition, tout le monde — selon moi — déploie en grande partie les mêmes efforts : il s'agit d'apporter une contribution militaire afin de régler le problème militaire, mais il y a un effort plus vaste qui comprend tout ce qui est lié à la gouvernance et qui soutient les populations.

Le sénateur Kenny : Quand nous étions au camp Julien, à Kaboul, la principale opération des soldats canadiens qui étaient là-bas était l'évaluation de la formation que les Afghans recevaient, et ils étaient très frustrés par leur travail. La raison de leur frustration était qu'à ce moment-là, une restriction leur était imposée : ils ne pouvaient aller combattre avec les soldats qu'ils formaient.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Could you tell us whether you think that restriction is going to be true if our soldiers don't go into combat with the people they're training now?

Gen. Vance: We're always careful about that term "going into combat," because that's one way to describe it. "Going on operations" is another way to describe it. So they weren't just restricted from going to fight with them; they were restricted from going on patrols with them where no fighting occurred. They were restricted from being with them during the conduct of their daily missions. At that point in time in the campaign, if you're speaking of early in the campaign, out of Camp Julien, that was the method that the coalition or, at that time, ISAF, was undertaking. That was the effort. We weren't equipped — nobody was — to be accompanying Afghan forces. In fact, we had to use our training effort to try to increase their capacity.

To relate that to today, again, is comparing two very different conflicts. We are in the north with the Kurds dealing with a classic call-out of citizenry to protect their land. These are civilians. There are some elements of professionalized and partly professionalized forces, but they're almost exclusively civilians that need training on the use of small arms, their weapons, and that need to understand how defensive battles are conducted, to protect themselves, and to use a map and compass all the way through to how to read a GPS to get something done.

It's largely a defensive posture that we're supporting, with the ability to conduct offensive operations. We do not accompany them on offensive operations, but we do support them in their effort to plan their defence. Should they come under attack — and they have — we will be there with them in the advise-and-assist function to help them run their defensive operation.

So we are largely with them as we conduct training in the background and behind their lines, as they conduct planning forward and where we have the ability and the mandate to defend ourselves and those who we are with. If we are with them and they're being attacked, we can respond, but our principal effort is to help them do it themselves and do it well.

As they would move forward to conduct offensive operations beyond their line, into ISIL territory, we help them with the planning of it, and that can mean planning their routes, planning the weapons they will use, planning the preparatory fires they will use, working out all of the command and control methods that are necessary to be successful. We'll help them with the planning. We'll help them with the targeting, but we won't go with them. We're not accompanying them.

Pourriez-vous nous dire si vous pensez que cette restriction sera imposée à nos soldats s'ils ne vont pas combattre avec les personnes qu'ils forment actuellement?

Gén Vance : Nous sommes toujours prudents en ce qui concerne le terme « aller combattre » parce que c'est une façon de décrire la situation. « Participer à des opérations » en est une autre. Par conséquent, ils n'étaient pas simplement limités pour ce qui est d'aller combattre avec eux; la limite s'appliquait aux patrouilles avec ces soldats, où aucun combat n'avait lieu. Ils n'avaient pas le droit d'être avec eux durant la conduite de leurs missions quotidiennes. À ce moment-là, de la campagne — si vous parlez du début de la campagne —, au camp Julien, c'était la méthode qu'employait la coalition ou, à l'époque, la FIAS. Voilà l'effort qui était déployé. Nous n'étions pas équipés — personne ne l'était — pour accompagner les forces afghanes. De fait, nous devions utiliser nos efforts de formation pour tenter d'accroître leur capacité.

Encore une fois, lier cet événement à la situation actuelle, c'est comparer deux conflits très différents. Nous sommes dans le Nord avec les Kurdes à nous occuper d'un appel classique auprès des citoyens ayant pour but de protéger leurs terres. Il s'agit de civils. Il y a certains éléments de forces professionnalisées et partiellement professionnalisées, mais elles sont presque exclusivement civiles et ont besoin d'une formation sur l'utilisation de petites armes — leurs armes —, et elles doivent comprendre comment mener des batailles défensives, se protéger et utiliser une carte et une boussole; elles doivent même apprendre comment lire un GPS pour arriver à accomplir quelque chose.

Nous appuyons principalement une force défensive ayant la capacité de mener des opérations offensives. Nous n'accompagnons pas ces gens durant les opérations offensives, mais nous les appuyons dans leur effort de planification de leur défense. S'ils se font attaquer — et c'est déjà arrivé —, nous serons là avec eux à exercer la fonction de conseiller et d'assistant afin de les aider à mener leur opération défensive.

Ainsi, nous sommes surtout avec eux pendant que nous donnons la formation en arrière-plan et derrière leurs lignes, alors qu'ils mettent la planification à exécution, dans une situation où nous avons la capacité et le mandat de nous défendre nous-mêmes ainsi que les personnes qui sont avec nous. Si nous sommes avec eux et qu'ils sont attaqués, nous pouvons intervenir, mais notre effort principal consiste à les aider à le faire par eux-mêmes et à bien le faire.

Au moment où ils mèneront des opérations offensives au-delà de leurs lignes, en territoire de l'État islamique, nous allons les aider à planifier ces opérations, et cela peut signifier la planification de leurs itinéraires, la planification des armes qu'ils utiliseront, des tirs préparatoires qu'ils utiliseront, l'organisation de toutes les méthodes de commandement et de contrôle qui sont nécessaires pour réussir. Nous allons les aider à effectuer la planification. Nous les aiderons en ce qui a trait au ciblage, mais nous n'irons pas avec eux. Nous ne les accompagnons pas.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

That is not unusual for the coalition forces right now. It's consistent with what our allies are doing as well, in large part because they need to and want to do this themselves. They just need the training and the capacity to do it.

Senator White: Thanks for that, general. Thanks for coming here today.

I wonder if you can give us an update on DND personnel in Europe in relation to Russia and Ukraine. It was on our radar heavily about a year and a half ago, but I'm not sure we're heard much on it lately.

Gen. Vance: Thanks for the question, senator.

We have Operation UNIFIER, which is being conducted in West Ukraine, that principally focuses on training infantry, training at the rifle company level and below, with a mandate or a ceiling on our effort of about 205 people. That goes up and down, depending on how many people are in theatre at any point in time, because we also contribute to military police training, counter-ID training, flight safety training and logistics training.

Senator White: In the Ukraine?

Gen. Vance: In the Ukraine.

So the bulk of the effort is training the proper Ukraine army as they rotate out of the line, give them expert training on small unit tactics, but we're also contributing to a wider effort to the military police, flight safety programs, and so on. That is a specific effort with allies in Ukraine.

The wider NATO posture under Operation REASSURANCE includes the deployment of our ship right now, the HMCS *Fredericton*, which is deployed in the Aegean. We have a persistent rotational presence with about a company size, a little over 100 people, who are persistently present on the ground doing infantry army training in Poland and elsewhere, but recently it's been principally in Poland.

We have contributed to the air policing effort, and may do so again. So we've done Baltic air policing. In the past we've done Icelandic air policing, and we may do so again. In fact, that air policing mandate will start to include southern air policing. In the army, navy and air force realms, we have contributed and will continue to contribute.

There's one other aspect to this, if I may. The alliance has worked hard to ensure that the training tempo has increased, that we demonstrate the capacity to operate large forces, high-tech,

Il ne s'agit pas d'une situation inhabituelle pour les forces de la coalition en ce moment. Elle correspond à ce que font également nos alliés, en grande partie parce que les Kurdes doivent et veulent le faire par eux-mêmes. Ils ont seulement besoin de la formation et de la capacité nécessaires pour le faire.

Le sénateur White : Je vous remercie, monsieur le général. Merci de votre présence aujourd'hui.

Je me demande si vous pouvez nous faire un compte rendu sur le personnel du MDN en Europe relativement à la Russie et à l'Ukraine. Il s'agissait de l'une de nos grandes priorités il y a environ un an et demi, mais je ne suis pas certain que nous en ayons entendu beaucoup parler dernièrement.

Gén Vance : Merci de me poser la question, monsieur le sénateur.

Nous menons l'Opération UNIFIER, dans l'ouest de l'Ukraine; cette opération est axée principalement sur l'entraînement de l'infanterie, la formation à l'échelon de la compagnie de carabiniers et aux échelons inférieurs, et elle s'assortit d'un mandat ou d'un plafond d'environ 205 personnes relativement à notre effort. Ce chiffre fluctue en fonction du nombre de personnes présentes sur le théâtre des opérations à un moment donné, parce que nous contribuons également à la formation des membres de la police militaire et à l'instruction en matière de contre-identification, de sécurité en vol et de logistique.

Le sénateur White : En Ukraine?

Gén Vance : En Ukraine.

Alors le gros de l'effort consiste à entraîner les bons soldats de l'armée ukrainienne lorsqu'ils sortent de la ligne par rotation, à leur donner une instruction spécialisée sur les tactiques de petites unités, mais nous contribuons également à un vaste effort visant la police militaire, les programmes de sécurité en vol, et ainsi de suite. Il s'agit d'un effort visant précisément nos alliés en Ukraine.

La position générale de l'OTAN dans le cadre de l'Opération REASSURANCE comprend le déploiement actuel de notre navire — le NCSM *Fredericton* — dans la mer Égée. Nous assurons une présence par rotation grâce à un petit groupe d'environ la taille d'une compagnie, qui compte un peu plus de 100 personnes, lesquelles assurent une présence persistante sur le terrain et offrent une instruction à l'infanterie en Pologne et ailleurs, mais, récemment, principalement en Pologne.

Nous avons contribué à l'effort lié aux services de police aériens, et nous pourrions le refaire. Alors, nous avons offert des services de police aériens dans la région baltique. Dans le passé, nous avons fourni des services de police aériens en Islande, et nous pourrions le refaire. De fait, ce mandat lié aux services de police aériens va commencer à inclure de tels services dans le Sud. Dans les domaines de l'armée, de la marine et de la force aérienne, nous avons apporté une contribution et continuerons de le faire.

Il y a un autre aspect à cela, si je puis me permettre. L'alliance a travaillé d'arrache-pied pour assurer l'accélération de la cadence de l'instruction et pour que nous affichions la capacité nécessaire

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

high-quality armed forces. So we did that last fall in exercise Trident Juncture on the Iberian Peninsula, and Canada played a significant role in that. We were one of four nations that provided a brigade headquarters on the ground, ran a significant amount of the training and contributed over 1,000 people, including ships and aircraft and people on the ground.

All up, the alliance is quite active to both reassure allies and demonstrate to Russia this deterrent effect.

Senator White: We've seen those shifts since October. That is expected to be our continued role in that area, I take it. We see a shift in the Middle East. That's why I'm asking.

Gen. Vance: Sorry?

Senator White: We're not seeing a shift away to something different as we saw in the Middle East since October, since the election. Do we anticipate this will be our continued activity there?

Gen. Vance: At this point in time, I have no direction from the government to undertake any changes, no.

Senator Mitchell: Thanks, general. Before I get to the topic, I'd just like to acknowledge your efforts to deal with harassment in the military and say that your leadership and taking it on in the way you've done is exemplary, and I wish you well on that very important effort.

I'm interested in getting a sense of the magnitude of the training. So you've outlined that it looks like you're training largely raw, civilian recruits. Are you training 10,000? Are you training 5,000? Can you say? A year from now, how many will you train and what is the critical mass that needs to be trained? Also, what portion of all the training being done by coalition forces are we contributing to?

Gen. Vance: The magnitude of the training is interesting. I don't have firm figures on who in the Peshmerga forces is available at any one time for operation. It's a sort of continuum where an individual shows up for their rotation. They come from home and say: "Okay, I'm ready for operations. I'm going to operate for three days." If that person has already received their training, they may get a bit of a refresher to make sure they can use their weapon properly, and then they do their time on the line.

If an operation is being conceived to adjust the line — think of almost like World War I, where they wanted to move the line forward onto more advantageous ground — there is a battle procedure that occurs. Those who will be participating in that

pour exploiter des forces armées d'envergure, de pointe et de qualité. C'est donc ce que nous avons fait l'automne dernier durant l'exercice Trident Juncture, dans la péninsule ibérique, et le Canada a joué un rôle important dans le cadre de cet exercice. Nous faisons partie des quatre pays qui ont fourni un quartier général de brigade sur le terrain, offert une partie importante de l'instruction et apporté une contribution de plus de 1 000 personnes, y compris des vaisseaux et des aéronefs ainsi que des gens sur le terrain.

Somme toute, l'alliance est pas mal active pour ce qui est de rassurer les alliés et de montrer cet effet dissuasif à la Russie.

Le sénateur White : Nous observons ces changements depuis le mois d'octobre. Il devrait s'agir de notre rôle continu dans ce domaine, à ce que je sache. Nous observons un changement au Moyen-Orient. C'est pourquoi je pose la question.

Gén Vance : Pardon?

Le sénateur White : Nous n'observons pas un changement vers quelque chose de différent, comme cela a été le cas au Moyen-Orient depuis l'élection, au mois d'octobre. Est-il prévu qu'il s'agira de notre activité continue là-bas?

Gén Vance : Pour le moment, je n'ai reçu aucune directive de la part du gouvernement pour entreprendre quelque changement que ce soit, non.

Le sénateur Mitchell : Merci, monsieur le général. Avant que j'en vienne au sujet à l'ordre du jour, je voudrais seulement souligner les efforts que vous avez déployés afin de régler le problème d'harcèlement dans l'armée et vous dire que votre leadership et la façon dont vous vous êtes attaqué au problème sont exemplaires, et je vous souhaite bonne chance relativement à cette initiative très importante.

Je voudrais avoir une idée de l'ampleur de l'instruction. Selon votre description, on dirait que vous entraînez principalement des recrues civiles inexpérimentées. En formez-vous 10 000? En formez-vous 5 000? Pouvez-vous le dire? D'ici un an, combien en formerez-vous et quelle est la masse critique qui doit recevoir l'instruction? En outre, quelle portion de l'instruction donnée par les forces de la coalition assurons-nous?

Gén Vance : L'ampleur de l'instruction est intéressante. Je n'ai pas de chiffres fixes concernant les personnes qui, dans les forces peshmergas, sont disponibles à un moment donné aux fins de l'opération. Il s'agit d'un genre de continuum où une personne se présente pour sa rotation. Les gens arrivent de chez eux en disant : « D'accord, je suis prêt pour les opérations. Je vais participer à une opération pour trois jours. » Si cette personne a déjà reçu son instruction, elle pourrait recevoir une petite formation de recyclage pour que l'on puisse s'assurer qu'elle peut utiliser son arme adéquatement, puis elle fait son temps sur la ligne.

Si une opération est conçue pour rajuster la ligne — presque comme dans le cas de la Première Guerre mondiale, où on voulait faire avancer la ligne de front jusqu'à un terrain plus avantageux —, une procédure de combat est appliquée. Les

operation, through the Peshmerga chain of command, will be rehearsed and trained up specifically for that, and then they will conduct that operation.

There's not a set figure that we're going through. We're not building an army; we're building an effect that will last as long as it needs to last. Ultimately, as I described, perhaps foreshadowing the battle of Mosul, they will need to reinforce the line, I suspect at times, with all they have available to make certain that they don't get penetrated or lose any terrain.

Right now, I don't have a good sense of the all-up numbers, because we're expanding our territory. In the territory that we're in right now, we're in the range of 400 to 500, but I think we want to improve that. We want to make certain that there are still more and more people available, subject to operations. We're going to be mentoring and training, advising and assisting in other sectors of the line.

We're also looking at professionalizing some discrete forces. One of the programs will try to take conventional forces and give them a bit more focused training. This is where we're going to equip people. So we will try to take a roughly a battalion size of 300 to 400, give them training for months, and equip them so that they have a stronger core of more professional fighters that can reinforce the line, if necessary, or conduct defensive operations — potentially even in time to support the battle on Mosul.

Senator Beyak: Thank you, General Vance.

I was called to the Senate three years ago. Prior to that, since 2005, I worked in the United States, United Kingdom and Europe with political associates on national defence and security and anti-terror efforts. One of our major concerns in all the nations was the use of chemical warfare. Recent media reports have indicated that the Islamic State is using mustard gas in Northern Iraq. Could you comment on the accuracy of those reports? And, given our commitment to more personnel in the region, do you have any concerns about chemical warfare there?

Gen. Vance: Thank you, senator, for your question. I have concerns about all threats against our forces, chemical attack being one of them. So absolutely, I share your concerns.

We can mitigate it. We have the best detection equipment in the world, and we have great protection equipment. We believe that with the improvement to our intelligence gathering, we'll try to forecast if in fact there's an imminent threat of the use of chemical weapons. That only will account for so much, and the

personnes qui participeront à cette opération, par l'intermédiaire de la chaîne de commandement peshmerga, répéteront cette procédure et seront entraînées à cette fin précise, puis elles mèneront l'opération en question.

Nous n'avons pas de chiffre fixe à atteindre. Nous ne mettons pas sur pied une armée; nous créons un effet qui durera aussi longtemps que nécessaire. Au bout du compte — comme je l'ai décrit, cela laisse peut-être présager la bataille de Mossoul —, il faudra renforcer la ligne je suppose, par moments, grâce à toutes les ressources disponibles pour s'assurer qu'il n'y a pas de brèche ou que les forces ne perdent pas de terrain.

Pour l'instant, je n'ai pas une bonne idée des chiffres cumulatifs, car nous élargissons notre territoire. Sur le territoire où nous nous trouvons actuellement, nous sommes dans la fourchette des 400 à 500 soldats, mais je pense que nous voulons améliorer cette situation. Je veux m'assurer qu'il y a toujours de plus en plus de gens disponibles et pouvant participer aux opérations. Nous allons offrir des services de mentorat et d'instruction, des conseils et de l'aide dans d'autres secteurs de la ligne.

Nous envisageons également de professionnaliser certaines forces distinctes. L'un des programmes tentera de donner une formation un peu plus ciblée à des forces conventionnelles. C'est là que nous allons équiper les gens. Ainsi, nous tenterons d'entraîner pendant quelques mois un groupe de 300 à 400 personnes, à peu près la taille d'un bataillon, et de l'équiper afin qu'il soit doté d'un noyau de combattants professionnels qui peuvent renforcer la ligne, au besoin, ou mener des opérations défensives — peut-être même, en temps voulu, pour appuyer la bataille de Mossoul.

La sénatrice Beyak : Merci, monsieur le général Vance.

J'ai été appelée au Sénat il y trois ans. Auparavant — depuis 2005 —, j'ai travaillé avec des associés politiques aux États-Unis, au Royaume-Uni et en Europe sur la défense et la sécurité nationales et dans le cadre d'efforts antiterroristes. L'une des préoccupations majeures de tous les pays était le recours aux armes chimiques. Des reportages récents dans les médias ont indiqué que l'État islamique utilise du gaz moutarde dans le nord de l'Irak. Pourriez-vous formuler un commentaire concernant l'exactitude de ces reportages? En outre, compte tenu de notre engagement à augmenter le personnel dans la région, avez-vous des préoccupations au sujet du recours à des armes chimiques là-bas?

Gén Vance : Merci de votre question, madame la sénatrice. J'ai des préoccupations au sujet de toutes les menaces qui pèsent sur nos forces, notamment les attaques chimiques. Alors, absolument, je partage vos préoccupations.

Nous pouvons les atténuer. Nous disposons du meilleur équipement de détection au monde, et notre équipement de protection est excellent. Nous croyons que, grâce à l'amélioration de notre collecte de renseignements, nous pourrons prévoir s'il y a effectivement une menace imminente d'utilisation d'armes

potential is that we could be surprised by its use. We have the equipment that's immediately at hand and the drills to protect ourselves.

The reports that ISIL is the possession of rudimentary mustard and chlorine chemicals and rudimentary delivery means are accurate. It is rudimentary and relatively small-scale, but I don't take any solace in that. It could grow and it could get more dangerous if they were to get their hands on other types of chemical weapons, be they nerve agents or otherwise. I don't have any indication of that right now, but it is a huge concern.

It's also, if you can imagine, a concern because of the impact it could have on a civilian populace. Although we can protect ourselves, we have witnessed, as a global community, what happens when civilians get hit with chemical weapons. It's a terrible thing.

The Chair: I'd like to follow up with a couple of questions and then Senator Kenny has a question on a different subject.

I want to stay with the Middle East. First of all, the conflict seems to be getting wider and broader in respect to the various regions that are getting involved. We have had discussion about Libya, and I think last week you mentioned Libya in your address to the Canadian Defence Association. I know on the weekend there were apparently air strikes that took place on the Libya-Tunisia border, I believe. Have we been asked to participate, and do we have any Canadians involved, at this stage, in respect to that particular conflict?

Secondly, with respect to Saudi Arabia, there has been a fair amount of debate in respect of the question of the military equipment being provided to Saudi Arabia. Because of the transaction with Saudi Arabia, are any Canadians involved on the ground there either directly or indirectly? It seems to be getting broader and broader, and all of a sudden, as I think Senator Kenny pointed out, you find out this is a lot bigger than anybody else thought it was.

The third question I have relates to the one posed by Senator Carignan. I don't think his question was answered, and the question, I think, has to be about the good guys versus the bad guys. Do we have a list of those organizations that we will support? There are a lot of organizations there that aren't ISIL, necessarily, but they believe in the same objectives. With ISIL, the difference is they just want to be number one versus number two. Do you have that list? Could you take a note of that, general?

Gen. Vance: To clarify that last question, Mr. Chair, is that in Iraq, or in the region?

chimiques. Cette prévision tiendra compte de facteurs limités, et il est possible que nous soyons surpris par l'utilisation de ces armes. L'équipement est à notre disposition immédiate, et nous pratiquons des exercices afin de nous protéger.

Les reportages selon lesquels l'État islamique est en possession de produits chimiques rudimentaires à base de moutarde et de chlore et de moyens rudimentaires pour le répandre sont exacts. C'est rudimentaire et relativement à petite échelle, mais cela ne me réconforte aucunement. La situation pourrait prendre des proportions plus vastes et devenir plus dangereuse si l'État islamique mettait la main sur d'autres types d'armes chimiques, qu'il s'agisse de gaz neuroplégiques ou d'autre chose. Rien ne m'indique que c'est le cas pour l'instant, mais il s'agit d'une énorme préoccupation.

C'est également une préoccupation — si vous pouvez l'imaginer — en raison des conséquences que cela pourrait avoir sur une population civile. Même si nous pouvons nous protéger, nous avons été témoins, en tant que communauté mondiale, de ce qui arrive lorsque des civils sont frappés par des armes chimiques. C'est terrible.

Le président : J'aimerais revenir sur deux ou trois questions, puis le sénateur Kenny aura une question à poser sur un autre sujet.

Je veux rester dans le sujet du Moyen-Orient. Tout d'abord, le conflit semble se répandre et s'élargir du point de vue des diverses régions qui y prennent part. Nous avons tenu une discussion au sujet de la Libye, et je pense que vous avez mentionné ce pays la semaine dernière dans le discours que vous avez adressé à l'Association de la défense du Canada. Je sais que, durant la fin de semaine, il semblerait que des frappes aériennes aient eu lieu à la frontière de la Libye et de la Tunisie, je crois. Nous a-t-on demandé de participer, et y a-t-il des Canadiens impliqués, à ce stade, relativement à ce conflit en particulier?

Deuxièmement, en ce qui concerne l'Arabie saoudite, il y a eu un débat assez animé sur la question de l'équipement militaire fourni à ce pays. En raison de la transaction avec l'Arabie saoudite, y a-t-il des Canadiens impliqués sur le terrain, directement ou indirectement? Le conflit semble se propager de plus en plus et, tout d'un coup — je pense que le sénateur Kenny l'a signalé —, on découvre qu'il est beaucoup plus important que quiconque l'aurait pensé.

Ma troisième question est liée à celle qu'a posée le sénateur Carignan. Je ne pense pas qu'on ait répondu à sa question, et je pense qu'elle devait être au sujet des bons contre les méchants. Avons-nous une liste des organisations que nous allons appuyer? Y a-t-il beaucoup d'organisations là-bas qui ne sont pas nécessairement l'État islamique, mais qui ont les mêmes croyances et objectifs? Dans le cas de l'État islamique, la différence, c'est simplement qu'il veut être le premier plutôt que le deuxième. Avez-vous cette liste? Pourriez-vous en prendre note, monsieur le général?

Gén Vance : Pour clarifier la dernière question, monsieur le président, est-ce en Irak, ou bien dans la région?

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

The Chair: In the region.

Gen. Vance: To take your questions one at a time, we're not on the ground in Libya. We have not contributed, as a nation, to those strikes. We are involved in the efforts under way to keep abreast of what is going on there through small groups. Not coalitions, because we haven't put together a coalition, but Italy has been leading an effort to have a look at this problem. We have been an observer in that. We're doing everything we can to stay abreast of what's going on and what is being contemplated.

We do that, largely, to be in a good position to offer the Government of Canada options should it wish to act. We're not presaging anything or foreshadowing any decisions, but it's prudent military information and intelligence gathering to make certain that if the government does ask, I'm in a position to provide useful options.

We are not in Saudi Arabia in a military sense or operating with Saudi Arabia at all. This is an equipment purchase. We are not tied to that equipment or operating with them.

I will check, however, to make certain there's no function that DND has to assure any sort of quality assurance or delivery. I don't know. I've never been involved in a major deal like this. I don't feel like I am on this one either; that is to say, I don't have any forces assigned to it. But just to be thorough in the response, if there is any departmental involvement in the delivery of that equipment, we'll certainly take that on notice and get back to you.

Finally, we've got lots of lists of bad guys.

The Chair: Do we have any good guys?

Gen. Vance: Right. There's the coalition and the states in the area. We can do our level best to provide, on notice, the list of terror actors on the ground, the violent extremist groups that we think are on the ground.

You asked, as an end to that, whether they are good guys or bad guys: That's a judgment call.

Let's look at Libya, for example. If we were to act militarily there in concert with the Government of Libya, the Government of Libya would be the good guy, and all the forces arrayed against a legitimate government's ability to rule, including ISIL, would fall under that "bad guy" category. But that government doesn't exist yet and is still being pulled together.

At this time, if I were to start to list those people who are on the suspect list of who might be good or bad, I wouldn't be doing anybody a service. What you need is a professional response from the Armed Forces, something better than I can give right here. I can walk you around the world and tell you who I think are, but ultimately those standing in the way of progress aren't necessarily

Le président : Dans la région.

Gén Vance : Pour répondre à vos questions une à la fois, nous ne sommes pas sur le terrain en Libye. Nous n'avons pas contribué, en tant que pays, à ces frappes. Nous participons aux efforts en cours afin de nous tenir au courant de ce qui se passe là-bas par l'entremise de petits groupes. Il ne s'agit pas de coalitions, car nous n'avons pas mis sur pied une coalition, mais l'Italie dirige un effort visant à étudier ce problème. Nous avons été un observateur dans ce conflit. Nous faisons tout notre possible pour nous tenir au courant de ce qui se passe et de ce qui est envisagé.

Nous le faisons en grande partie dans le but d'être bien placés pour offrir des options au gouvernement du Canada s'il souhaitait agir. Nous ne prévoyons rien et ne laissons présager aucune décision, mais il s'agit d'une collecte prudente de renseignements militaires et de renseignement visant à nous assurer que, si le gouvernement pose la question, je serai en position de présenter des options utiles.

Nous ne sommes pas en Arabie saoudite au sens militaire du terme, et nous n'y menons aucune opération. Il s'agit d'un achat d'équipement. Nous ne sommes pas liés à cet équipement et ne l'utilisons pas pour mener des opérations.

Toutefois, je vérifierai pour m'assurer que le MDN n'exerce aucune fonction qui soit liée à l'assurance de la qualité ou à la livraison. Je ne sais pas. Je n'ai jamais pris part à une transaction majeure comme celle-là. Je n'ai pas l'impression d'y prendre part non plus, c'est-à-dire qu'aucune de mes forces n'est affectée à cette transaction. Mais, simplement pour répondre à la question avec rigueur, si le ministère participe d'une manière ou d'une autre à la livraison de cet équipement, nous allons certainement le remarquer et vous en informer.

Enfin, nous avons beaucoup de listes de méchants.

Le président : Y a-t-il des bons?

Gén Vance : Bien sûr. Il y a la coalition et les États dans la région. Nous pouvons faire de notre mieux pour fournir, moyennant un préavis, la liste des terroristes sur le terrain, des groupes extrémistes violents que nous croyons être sur le terrain.

Pour clore cette question, vous avez demandé s'il s'agissait de bons ou de méchants : c'est selon le jugement de chacun.

Regardons la Libye, par exemple. Si nous menions une opération militaire là-bas, de concert avec le gouvernement du pays, il serait le bon, et toutes les forces dressées contre la capacité d'un gouvernement légitime de diriger, y compris l'État islamique, se retrouveraient dans la catégorie des « méchants ». Mais ce gouvernement n'existe pas encore, et il est encore en cours de formation.

En ce moment, si je commençais à dresser une liste des personnes qui pourraient être des bons ou des méchants ou qui sont soupçonnées d'être l'un ou l'autre, je ne rendrais service à personne. Ce qu'il vous faut, c'est une réponse professionnelle des Forces armées, quelque chose de mieux que ce que je peux vous donner maintenant. Je peux faire le tour du monde avec vous et

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

good guys and bad guys. I can sponsor the view of the Canadian Armed Forces of the known violent extremist groups, how they're affiliated and the nation-states that we're trying to support, but in some of them we may not have a fully-fledged credible partner.

With regard to Syria, Canada has been categorical about the Assad regime, but there needs to be a credible partner on the ground. Ultimately, there has to be, if we're going to ever work with Syria, not militarily, and have normal relations, at some time in the future there has to be a legitimate government. Who forms that government and how well that comes to pass is history that has yet to be written. We'll do the best we can, and if it's not satisfactory, I'm more than happy to keep trying.

Senator Kenny: On a different topic, general, I have a question on unmanned air vehicles. Go back to 2006. The CF was looking for, I believe, 15 UAVs under a program called JUSTAS. We've gone through several stops and starts on it. Right now, we're hearing maybe in 2023 there will be a fleet. We don't have any friendly allies who don't have UAVs. Everybody else seems to be equipped with them. They seem like awfully useful tools for the military to have. What's taking so long? Why don't we have UAVs available now?

Gen. Vance: We have some UAVs available, small ones. You're talking about the larger armed UAV — the Predator, the Reaper and the Global Hawk. I agree with you, senator, that we need them. The Joint Unmanned Surveillance and Target Acquisition System program, JUSTAS, is alive and well. I am working on it and have increased the priority on this. I don't know if 2023 is actually accurate now. After I've spoken to the project, I need to see what the delivery date might be now. If it was 2023 before speaking to them and it's 2023 after I speak to them, I'd be concerned.

I agree that we need UAVs. I'm of the opinion that we need armed UAVs. We need UAVs for a number of reasons, not the least of which is surveillance of our own territory: to have a constant presence in high-risk areas for search and rescue to pinpoint the spot right away; to conduct surveillance against humanitarian disasters and threats; to look closely at the ice pack and downstream effects if something is going to be flooded out; and for operations overseas.

Senator Kenny: You've convinced me, but where's the roadblock?

Gen. Vance: There's no roadblock.

vous dire ce que j'en pense, mais, en fin de compte, les personnes qui font obstacle au progrès ne sont pas nécessairement des bons et des méchants. Je peux faire la promotion du point de vue des Forces armées canadiennes concernant les groupes extrémistes violents connus, la façon dont ils sont affiliés et les États-nations que nous tentons d'appuyer, mais certains d'entre eux ne sont peut-être pas des partenaires tout à fait crédibles pour nous.

En ce qui concerne la Syrie, le Canada a été catégorique au sujet du régime Assad, mais il doit y avoir un partenaire crédible sur le terrain. Au bout du compte, il le faut, si nous voulons un jour travailler avec la Syrie, non pas sur le plan militaire, et entretenir des relations normales, à un certain moment dans l'avenir, il devra y avoir un gouvernement légitime. On ne sait pas encore qui formera ce gouvernement et comment sa mise sur pied se déroulera, mais l'histoire le dira. Nous ferons de notre mieux et, si ce n'est pas satisfaisant, je serai ravi de continuer à essayer.

Le sénateur Kenny : Sur un autre sujet, monsieur le général, j'ai une question concernant les véhicules aériens sans pilote. Retournons en 2006. Les Forces canadiennes étaient à la recherche — je crois — de 15 véhicules aériens sans pilote dans le cadre d'un programme appelé JUSTAS. Il y a eu une véritable valse-hésitation à cet égard. En ce moment, on nous dit qu'il y a aura peut-être une flotte en 2023. Tous nos amis alliés possèdent des véhicules aériens sans pilote. Tout le monde semble être équipé de ces véhicules. On dirait qu'il s'agit d'outils extrêmement utiles pour les armées. Pourquoi est-ce que cela nous prend si longtemps? Pourquoi n'avons-nous pas déjà accès à des véhicules aériens sans pilote?

Gén Vance : Nous avons accès à certains véhicules aériens sans pilote — des petits. Vous faites allusion aux grands véhicules aériens sans pilote qui sont armés — le Predator, le Reaper et le Global Hawk. Je suis d'accord avec vous, monsieur le sénateur : nous en avons besoin. Le programme du Système interarmées de surveillance et d'acquisition d'objectifs au moyen de véhicules aériens sans pilote — JUSTAS — se porte très bien. Je travaille là-dessus, et j'ai augmenté son degré de priorité. Je ne sais pas si 2023 est une date exacte, maintenant. Après que j'aurai parlé aux responsables du projet, il faudra que je voie quelle pourrait être la date de mise en œuvre, maintenant. Si c'était 2023 avant que je leur aie parlé et que ça l'est encore après, je serais préoccupé.

Je suis d'accord avec le fait que nous avons besoin de véhicules aériens sans pilote. Je suis d'avis qu'ils doivent être armés. Nous en avons besoin pour un certain nombre de raisons, notamment pour la surveillance de notre propre territoire : pour assurer une présence constante dans les régions à risque élevé à des fins de recherche et de sauvetage et pour pouvoir repérer immédiatement le lieu d'un événement; pour exercer une surveillance contre les catastrophes humanitaires et les menaces; pour étudier de près la banquise et les effets en aval, si quelque chose va être inondé; et pour les opérations outre-mer.

Le sénateur Kenny : Vous m'avez convaincu, mais où est l'obstacle?

Gén Vance : Il n'y a pas d'obstacle.

Senator Kenny: We don't have them. It's been a long time since 2006.

Gen. Vance: We need to keep working on it. There's no roadblock.

The Chair: General, can we keep you for two more minutes? Senator Day would like to ask you a question. I know it will be short.

Senator Day: Are we providing assistance to the Kurdish regional government in Northern Iraq, or are we providing assistance to the Iraqi government?

Gen. Vance: What sort of assistance? Military assistance?

Senator Day: Yes, the military assistance that we're giving now, the participation that's going on in Northern Iraq.

Gen. Vance: The train, advise and assist mission is focused in Northern Iraq, in Kurdish territory, centred really on Erbil. We are assisting their local forces with training, advising and assisting. We are going to be contributing through the wider coalition effort. Staff is important to get all the needed work done at the various coalition headquarters. We're contributing directly to the Iraqi government in Baghdad, we hope. We're still scoping out how we'll do it through this ministerial liaison team, which will be Canadian-led.

I believe we're providing military assistance to Iraq in general by the contribution of intelligence and refuelling. It's indirect, but we're certainly supporting their effort to rid themselves of ISIL. That's the military assistance we're providing.

Does that answer your question?

Senator Day: I'm just wondering to what extent the Kurdistan Regional Government is independent of Iraq as far as our activities are concerned. That's what I was getting to.

Gen. Vance: I understand. They are not independent of Iraq in our eyes; they are a regional government. We are in Northern Iraq because Baghdad says we can be in Northern Iraq. We clear customs in Baghdad. We have an absolute desire for there not to be any internal political challenges to the capacity for Iraq to deal with this threat. At the same time, we don't normally interfere with the internal dynamics of a country. It would do us no good if there were an internal struggle between Kurdistan and Iraq while they have a clear and present danger right in front of them.

The Chair: General, thank you very much for your time. You've given us a little more time than we had allocated, which we appreciate. I want to convey our thanks through you to the men and women serving in the Canadian Armed Forces. Once again, thank you for appearing.

Le sénateur Kenny : Nous n'en avons pas. Cela fait longtemps : depuis 2006.

Gén Vance : Nous devons continuer à travailler là-dessus. Il n'y a pas d'obstacle.

Le président : Monsieur le général, pouvons-nous vous garder pour deux minutes de plus? Le sénateur Day voudrait vous poser une question. Je sais qu'elle sera brève.

Le sénateur Day : Prêtons-nous assistance au gouvernement régional kurde dans le nord de l'Irak, ou bien au gouvernement irakien?

Gén Vance : Quel genre d'assistance? Une assistance militaire?

Le sénateur Day : Oui, l'assistance militaire que nous fournissons actuellement, la participation qui a lieu dans le nord de l'Irak.

Gén Vance : En réalité, la mission de formation, de conseils et d'assistance dans le nord de l'Irak, en territoire kurde, est axée sur Erbil. Nous aidons les forces locales kurdes grâce à une formation, à des conseils et à de l'assistance. Nous allons apporter notre contribution dans le cadre de l'effort de la coalition dans son ensemble. Le personnel est important pour effectuer tout le travail nécessaire dans les divers quartiers généraux de la coalition. Nous aidons directement le gouvernement irakien, à Bagdad — nous l'espérons. Nous évaluons encore la façon dont nous allons le faire par l'intermédiaire de cette équipe de liaison ministérielle qui sera dirigée par des Canadiens.

Je crois que nous fournissons une assistance militaire à l'Irak en général en offrant des renseignements et de l'avitaillement. C'est une assistance indirecte, mais nous appuyons certainement les efforts déployés par ce pays afin de se débarrasser de l'État islamique. Voilà l'assistance militaire que nous fournissons.

Est-ce que cela répond à votre question?

Le sénateur Day : Je me demande seulement dans quelle mesure le gouvernement régional kurde est indépendant de l'Irak en ce qui concerne nos activités. C'est là que je voulais en venir.

Gén Vance : Je comprends. Il n'est pas indépendant de l'Irak, à nos yeux; il s'agit d'un gouvernement régional. Nous sommes dans le nord de l'Irak parce que Bagdad dit que nous pouvons y être. Nous passons la douane à Bagdad. Nous souhaitons absolument qu'il n'y ait pas de difficultés politiques internes liées à la capacité de l'Irak de faire face à cette menace. En même temps, nous ne nous immisçons habituellement pas dans la dynamique interne d'un pays. Nous ne tirerions aucun avantage d'une lutte interne entre Kurdes et Irakiens pendant qu'ils sont confrontés à un danger clair et présent.

Le président : Monsieur le général, merci beaucoup de votre temps. Vous nous en avez accordé un peu plus que ce que nous avions alloué, et nous vous en sommes reconnaissants. Je veux que vous transmettiez nos remerciements aux hommes et aux femmes qui servent dans les Forces armées canadiennes. Encore une fois, merci de votre présence.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Joining us on our third panel today from the Canada Revenue Agency is Ms. Cathy Hawara, Director General, Charities Directorate, Legislative Policy and Regulatory Affairs Branch; and Mr. Alastair Bland, Director, Review and Analysis Division, Charities Directorate, Legislative Policy and Regulatory Affairs Branch.

Ms. Hawara and Mr. Bland, welcome back to the committee. I recall your presentation a number of months ago, and I think we all felt that it was very well prepared and well done. We have one hour for the panel and I understand you have an opening statement.

Cathy Hawara, Director General, Charities Directorate, Legislative Policy and Regulatory Affairs Branch, Canada Revenue Agency: Yes, I do. Good afternoon, Mr. Chair. Thank you very much.

[*Translation*]

I would like to thank you for the invitation to appear before the committee once again. My name is Cathy Hawara, and I am the Director General of the Charities Directorate of the Canada Revenue Agency (CRA). With me today is Alastair Bland, Director of the Review and Analysis Division.

We are pleased to be able to provide the committee with an update on the charities program in relation to the risk of terrorist abuse, further to our appearance before the committee last year.

As you are aware, the CRA is the federal regulator of over 86,000 registered charities. The Charities Directorate oversees this function and ensures that the tax incentives reserved for charities are only made available to organizations that operate for exclusively charitable purposes and that charitable funds and services reach intended, legitimate beneficiaries.

To address concerns around the risk of terrorist exploitation of the charitable sector, the Charities Directorate formally established the Review and Analysis Division in 2003. The division focuses especially on protecting the integrity of the charity registration system from the threat of terrorism.

[*English*]

The Review and Analysis Division takes a risk-based approach to the detection and suppression of terrorist financing activities within the charitable sector. It conducts in-depth reviews of applications for charitable registration based on the presence and

Aujourd'hui, nous accueillons, pour notre troisième groupe de témoins, Mme Cathy Hawara, directrice générale, Direction des organismes de bienfaisance, Direction générale de la politique législative et des affaires réglementaires, et Alastair Bland, directeur, Division de l'examen et de l'analyse, Direction des organismes de bienfaisance, Direction générale de la politique législative et des affaires réglementaires, de l'Agence du revenu du Canada.

Madame Hawara et monsieur Bland, je vous souhaite de nouveau la bienvenue au comité. Je me souviens de l'exposé que vous avez présenté il y a quelques mois, et je pense que nous avons tous estimé qu'il avait été bien préparé et bien fait. Nous disposons d'une heure pour entendre le groupe, et je crois savoir que vous avez une déclaration préliminaire.

Cathy Hawara, directrice générale, Direction des organismes de bienfaisance, Direction générale de la politique législative et des affaires réglementaires, Agence du revenu du Canada : Oui, j'en ai une. Bonjour, monsieur le président. Merci beaucoup.

[*Français*]

J'aimerais vous remercier de m'avoir invitée à comparaître encore une fois devant ce comité. Je m'appelle Cathy Hawara et je suis la directrice générale de la Direction des organismes de bienfaisance de l'Agence du revenu du Canada. Je suis accompagnée d'Alastair Bland, directeur de la Division de la revue et de l'analyse.

Nous sommes heureux de pouvoir donner au comité une mise à jour sur le programme des organismes de bienfaisance en ce qui a trait au risque d'abus à des fins terroristes, ce qui donne suite à notre comparution de l'an dernier devant le comité.

Comme vous le savez, l'Agence du revenu du Canada est l'organisme de réglementation fédérale de plus de 86 000 organismes de bienfaisance enregistrés. La Direction des organismes de bienfaisance exerce cette fonction. Elle s'assure que les incitatifs fiscaux réservés aux organismes de bienfaisance ne profitent qu'à des organismes administrés exclusivement à des fins de bienfaisance et que les fonds et les services de bienfaisance parviennent aux bénéficiaires voulus et légitimes.

En 2003, pour répondre aux préoccupations concernant le risque d'exploitation du secteur de la bienfaisance à des fins terroristes, la Direction des organismes de bienfaisance a établi officiellement la Division de la revue et de l'analyse, laquelle se consacre spécialement à la protection de l'intégrité du système d'enregistrement des organismes de bienfaisance contre la menace terroriste.

[*Traduction*]

La Division de la revue et de l'analyse adopte une approche fondée sur les risques vis-à-vis de la détection et du refoulement des activités de financement du terrorisme dans le secteur de la bienfaisance. Elle mène des examens en profondeur des demandes

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

extent of terrorist financing risks and selects organizations for audit based on the potential risk of abuse posed to the charitable sector and Canadian society as a whole.

Like the Charities Directorate's general functions, the division's role is administrative. While it cannot confirm or validate that terrorism as a criminal activity or offence has occurred, it can take steps to disrupt activities where there is a risk of terrorist abuse. Where risks related to terrorism financing are identified, the division chooses the most appropriate course of action, taking into consideration the circumstances of each case. This includes refusing to register organizations as charities, imposing sanctions or penalties, or revoking registered status.

The division also takes steps to share relevant information related to the risk of terrorist financing with national security partners. During our appearance before the committee last year, we noted that the CRA was authorized to share certain charity-related information with the RCMP, CSIS and FINTRAC. This authority was recently broadened with the coming into force of the Security of Canada Information Sharing Act. The CRA may now share taxpayer information with 16 government institutions designated in Schedule 3 of that act.

The sharing of this information is not without limit. As was previously the case, the CRA may only disclose information when it is relevant to an investigation of a threat to the security of Canada or an investigation of a terrorism offence. In addition, information will only be shared when it is relevant to the receiving institution's national security responsibilities. The CRA has updated its internal policies and procedures to reflect this change.

[*Translation*]

We would be pleased to answer any questions the members of the committee may have. Thank you.

[*English*]

The Chair: Thank you very much. Before we go to questions, I want to set the scene in respect to your previous presentation that was given here on June 1.

You gave us information that eight charities had their status revoked because of links in one manner or another to terrorism, and you committed to tabling this list with the committee. My office and the clerk's office have followed up on numerous

d'enregistrement des organismes de bienfaisance en fonction de la présence de risques de financement des activités terroristes et de l'ampleur de ces risques. Elle sélectionne ensuite les organismes à vérifier en fonction du risque d'abus possible qui se présente au secteur de la bienfaisance et à la société canadienne dans son ensemble.

Tout comme les fonctions générales de la Direction des organismes de bienfaisance, le rôle de la division est d'ordre administratif. Même si la division ne peut ni confirmer ni valider qu'il s'est produit un acte terroriste sous forme d'activité ou d'infraction criminelle, elle peut prendre des mesures pour perturber ces activités lorsqu'il y a un risque d'abus à des fins terroristes. Lorsqu'on relève des risques liés au financement des activités terroristes, la division choisit la ligne de conduite la plus appropriée, en tenant compte des circonstances propres à chaque cas. Cela comprend le refus d'enregistrer des organismes en tant qu'organismes de bienfaisance, l'imposition de sanctions et de pénalités, et la révocation de l'enregistrement.

La division prend également des mesures pour communiquer à ses partenaires de la sécurité nationale des renseignements pertinents liés au risque de financement des activités terroristes. Lors de notre comparution de l'an dernier devant le comité, nous avons fait observer que l'ARC était autorisée à communiquer certains renseignements liés aux organismes de bienfaisance à la GRC, au SCRS et au CANAFE. Cette autorisation a été élargie récemment par l'entrée en vigueur de la Loi sur la communication d'information ayant trait à la sécurité du Canada. L'ARC peut désormais communiquer les renseignements portant sur des contribuables à 16 institutions gouvernementales désignées à l'annexe 3 de cette loi.

La communication de ces renseignements n'est pas illimitée. Comme c'était le cas auparavant, l'ARC peut seulement divulguer des renseignements lorsqu'ils sont pertinents par rapport à une enquête sur une menace à la sécurité du Canada ou à une enquête sur une infraction terroriste. De plus, les renseignements ne seront communiqués que lorsqu'ils sont pertinents par rapport aux responsabilités en matière de sécurité nationale de l'institution destinataire. L'ARC a mis à jour ses politiques et ses procédures internes pour tenir compte de ce changement.

[*Français*]

Nous serons heureux de répondre à toute question que les membres du comité pourraient avoir. Je vous remercie.

[*Traduction*]

Le président : Merci beaucoup. Avant que nous ne passions aux questions, je veux présenter le contexte de l'exposé précédent que vous avez présenté ici le 1er juin.

Vous nous aviez fourni des renseignements selon lesquels huit organismes de bienfaisance s'étaient vu révoquer leur statut parce qu'ils étaient liés d'une manière ou d'une autre au terrorisme, et vous vous étiez engagée à présenter cette liste au comité. Mon

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

occasions so we would have that information for members of the committee. Could you update us in respect to that information and are you going to be tabling it today?

Ms. Hawara: Thank you, chair.

We had prepared the package and we were ready to forward it on to the committee. Unfortunately, the dissolution of Parliament prevented us from sharing it with the committee, but it is ready and we will share it with the committee. I don't have it with me today. It is a rather voluminous package, but it will be provided to the committee very shortly.

The Chair: You say it is a voluminous document. I would have thought it would be a three-page document outlining the organizations that had their charitable status removed, and where and how and what was being done about it.

Ms. Hawara: As a package, we have prepared a number of letters that were sent to the organizations confirming our intention to revoke. Each letter can be quite lengthy. In total, we have six letters to share with the committee, one of which has been translated into French to give the committee a sense of that, so that's what I refer to. There's a short cover memo attaching a number of lengthy letters.

The Chair: Colleagues, I want to pursue this further because I remember our conversation fairly clearly. I think it's important for the record to point out that we're trying to understand the scope of terrorism financing in Canada, either coming into Canada or going outside of Canada. In conjunction with that, are you going to provide us with a list of the organizations, the amount of money that's involved in the types of transactions that have been identified and if any of these cases have been referred on to other law enforcement agencies?

Ms. Hawara: The letters that will be provided to the committee provide detailed information about what we found during the audits, and it will get into some of the details of what you're looking for in terms of money transfers.

Each case is different, but the letters provide a full account of what we found during the course of these audits. That's why we thought they were the best documents to put in front of the committee. It will give you a sense of what we have found in those instances where we've conducted audits and proceeded with revocation.

The Chair: I will conclude by asking if we can expect them to be mailed to us within the week.

Ms. Hawara: I will make best efforts, absolutely.

Senator Kenny: Is there any reason why we can't have a short summary as well?

bureau et celui du greffier ont effectué un suivi à de nombreuses occasions afin que nous puissions présenter cette information aux membres du comité. Pourriez-vous faire le point relativement à cette information? Allez-vous présenter cette liste aujourd'hui?

Mme Hawara : Merci, monsieur le président.

Nous avions préparé le dossier et étions prêts à le transmettre au comité. Malheureusement, la dissolution du Parlement nous a empêchés de vous le communiquer, mais il est prêt, et nous allons vous le communiquer. Je ne l'ai pas apporté aujourd'hui. Il s'agit d'un dossier assez volumineux, mais il sera fourni au comité sous peu.

Le président : Vous dites que c'est un document volumineux. J'aurais cru qu'il s'agirait d'un document de trois pages décrivant les organisations dont le statut d'organisme de bienfaisance a été révoqué, où et comment cela avait eu lieu et ce qui était fait à ce sujet.

Mme Hawara : Nous avons préparé, sous forme de dossier, un certain nombre de lettres qui ont été envoyées aux organisations pour confirmer notre intention de révoquer leur enregistrement. Chaque lettre peut être très longue. Au total, nous avons six lettres à communiquer au comité, dont l'une a été traduite en français pour donner une idée au comité, alors c'est de cela que je parlais. Une courte note de présentation est jointe à un certain nombre de longues lettres.

Le président : Chers collègues, je veux approfondir cette question parce que je me rappelle assez clairement notre conversation. Je pense qu'il est important, pour le compte rendu, de signaler le fait que nous essayons de comprendre la portée du financement du terrorisme au Canada, financement qui entre au pays ou qui en sort. En plus de ce dossier, allez-vous nous fournir une liste des organisations, de la somme d'argent qui est en cause et des types de transactions qui ont été recensées, et préciser si certains de ces cas ont été renvoyés à d'autres organismes d'application de la loi?

Mme Hawara : Les lettres qui seront fournies au comité présentent des renseignements détaillés sur ce que nous avons découvert durant les audits, et elles contiendront certains des détails que vous souhaitez connaître en ce qui concerne les transferts de fonds.

Chaque cas est différent, mais les lettres présentent un compte rendu complet de ce que nous avons découvert dans le cadre de ces audits. C'est pourquoi nous avons pensé qu'il s'agissait des meilleurs documents à présenter au comité. Ils vous donneront une idée de ce que nous avons découvert dans les cas où nous avons effectué des audits et procédé à la révocation.

Le président : Je conclurai en vous demandant si nous pouvons nous attendre à les recevoir par la poste dans le courant de la semaine.

Mme Hawara : Je ferai de mon mieux, certainement.

Le sénateur Kenny : Y a-t-il une raison pour laquelle nous ne pouvons pas également obtenir un bref résumé?

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

The Chair: A verbal summary here right now?

Senator Kenny: No, a short summary of what the document said. You talked about a three-pager in addition to the material they're forwarding. You don't have a firm commitment for a week, so they're going to take a while. Give us a summary and —

The Chair: No, I'm sorry; you misinterpreted me, senator. All I expected from them was a short summary of what the eight charities were and a breakdown. That's what I was expecting to receive, which we didn't receive. I have received nothing, if that's what you're —

Senator Kenny: No, what I'm suggesting is that there's other material coming. Let's also have what you were expecting.

The Chair: Perhaps you want to elaborate further on what you actually do have? Is that the question to the witness?

Senator Kenny: Yes, what have they got?

The Chair: Senator, could you please ask your question?

Senator Kenny: I would like a summary of what's in the documents, please.

Ms. Hawara: We were asked three questions, and so we've provided an answer to the three questions. In addition, we are providing the letters that were sent to charities confirming their revocation of registration. They are the actual letters we sent to the organizations indicating the grounds for revoking their registered status.

To be clear — and we had this discussion last time — while I had mentioned that there were eight, in some instances we don't always make note with the charity of the terrorism link, the concerns we might have from a terrorism perspective. Our role, to go back to my opening remarks, is an administrative role. Our role is not to prove that a terrorism offence has taken place. Our role is to protect the registration system for charities by applying the provisions of the Income Tax Act.

Senator Kenny: Mr. Chair, the witness is providing an index, not a summary. A summary would tell us what the substance is in a brief form, and instead we are just getting a list of documents she's sending.

The Chair: In fairness to you, you are a witness here, but you can understand the frustration from this side because what we want to do is to find out, in a very general way, how much money was involved in the financing of terrorism through these charitable organizations, how many people were involved, and what has happened and transpired since this was identified. This is illegal activity.

Le président : Un résumé verbal, ici et maintenant?

Le sénateur Kenny : Non, un bref résumé du contenu du document. Vous avez parlé d'une liste de trois pages, en plus du document qu'elle va nous transmettre. Vous n'avez pas obtenu d'engagement ferme à l'égard du délai d'une semaine, alors cela va lui prendre un certain temps. Donnez-nous un résumé et...

Le président : Non, je suis désolé; vous avez mal interprété mes propos, monsieur le sénateur. Tout ce que je m'attendais à recevoir de nos témoins, c'était un bref résumé expliquant qui sont les huit organismes de bienfaisance et présentant une ventilation. Voilà ce que je m'attendais à recevoir et que nous n'avons pas reçu. Je n'ai rien reçu, si c'est que vous...

Le sénateur Kenny : Non, ce que je dis, c'est que d'autres documents s'en viennent. Obtenons aussi ce à quoi vous vous attendiez.

Le président : Vous voudrez peut-être nous donner plus de détails sur les renseignements dont vous disposez. Est-ce la question que vous adressez au témoin?

Le sénateur Kenny : Oui, quels renseignements a-t-elle obtenus?

Le président : Monsieur le sénateur, pourriez-vous poser votre question?

Le sénateur Kenny : Je voudrais obtenir un résumé de ce qui figure dans les documents, s'il vous plaît.

Mme Hawara : Trois questions nous ont été posées; nous avons donc donné une réponse aux trois questions. De plus, nous fournissons les lettres qui ont été envoyées aux organismes de bienfaisance pour confirmer la révocation de leur enregistrement. Il s'agit des lettres qui ont réellement été envoyées aux organisations, indiquant les motifs de la révocation de leur enregistrement.

Pour être claire — et nous avons eu cette discussion la dernière fois —, bien que j'aie mentionné qu'il y en avait huit, dans certains cas, nous n'avisons pas toujours l'organisme de bienfaisance du lien avec le terrorisme, des préoccupations que nous pourrions avoir du point de vue du terrorisme. Pour en revenir à ma déclaration préliminaire, notre rôle est administratif. Il ne s'agit pas de prouver qu'une infraction liée au terrorisme a été commise. Notre rôle consiste à protéger le système d'enregistrement des organismes de bienfaisance en faisant appliquer les dispositions de la Loi de l'impôt sur le revenu.

Le sénateur Kenny : Monsieur le président, le témoin fournit un index, pas un résumé. Un résumé nous exposerait la substance sous une forme abrégée; au lieu de cela, nous obtenons simplement une liste des documents qu'elle nous envoie.

Le président : En toute équité envers vous, vous êtes ici à titre de témoin, mais vous pouvez comprendre la frustration ressentie de notre côté, parce que nous voulons découvrir, de façon très générale, combien d'argent a servi au financement du terrorisme par l'intermédiaire de ces organismes de bienfaisance, combien de gens y ont pris part et ce qui est arrivé et ce qui s'est passé depuis que ce problème a été cerné. Il s'agit d'activités illégales.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Alastair Bland, Director, Review and Analysis Division, Charities Directorate, Legislative Policy and Regulatory Affairs Branch, Canada Revenue Agency: If I may, we're doing our best to strike the appropriate balance here. As was mentioned, we do not have a mandate to conduct criminal inquiries. Terrorist financing is a criminal offence.

What we do have the mandate to do is to protect the integrity of the registration system against the threat of terrorism. So where there is unacceptable risk or concern that an organization, through its activities, may lead to financing terrorism in one way, shape or form, we have certain powers available to us to deal with that.

What we're going to be providing, I think, is six of the eight letters outlining our grounds, under the Income Tax Act provisions, as to why they were revoked.

Now, the reasons for their revocation are likely to be things like they funded non-qualified donees. Now, in those letters, we do raise the concerns that we have that because they may not be operating purely for charitable purposes, there is an opportunity there for that money to be unaccounted for. Because of the context around the situation, one of those potential areas would be to end up in the hands of a terrorist organization. But we don't go down there. We do not prove that these funds were raised and will therefore be used for terrorist financing. That's not our mandate. Our mandate is to enforce the regulations. That's why we have those regulations under the Income Tax Act, to be able to protect the sector and the assets that are in it.

I don't think you're going to get a handle on the amount of terrorist financing through charities by looking at those letters, but it will give you an indication of the type of regulatory work we're doing.

It's a bit of a nuanced question. We did our best to answer the question, but it's not as simple as how many charities are funding terrorism.

Senator Beyak: Supplemental to the chair's question, is there a step that should be taken after you, somewhere you can send things to? I understand exactly what you're saying. It's not your agency's job. Everyone says, "It's not my job," but it isn't. What could we recommend, as a Senate committee, to make this easier?

Ms. Hawara: So we view ourselves as being a piece of the larger government effort to tackle terrorism and terrorist financing, and information sharing is critical to that. So, in the work that we do, there's a lot that we can share with our partners, and then they

Alastair Bland, directeur, Division de l'examen et de l'analyse, Direction des organismes de bienfaisance, Direction générale de la politique législative et des affaires réglementaires, Agence du revenu du Canada : Si je puis me permettre, nous faisons de notre mieux pour établir un juste équilibre. Comme cela a été mentionné, nous n'avons pas pour mandat de mener des enquêtes criminelles. Le financement du terrorisme est une infraction criminelle.

Le mandat que nous avons consiste à protéger l'intégrité du système d'enregistrement contre la menace de terrorisme. Alors, s'il y a un risque ou une crainte inacceptable que les activités d'une organisation puissent mener au financement du terrorisme d'une manière ou d'une autre, nous disposerons de certains pouvoirs qui nous permettent de nous en occuper.

Nous allons fournir, selon moi, six des huit lettres décrivant nos motifs, en vertu des dispositions de la Loi de l'impôt sur le revenu, de la révocation des enregistrements.

Les motifs de révocation des enregistrements sont probablement des choses comme le financement d'organismes bénéficiaires non qualifiés. Dans ces lettres, nous soulevons les préoccupations que nous avons à l'égard de la possibilité que les organismes ne soient pas exploités purement à des fins de bienfaisance et que les sommes d'argent en question ne soient pas comptabilisées. En raison du contexte entourant la situation, l'une des possibilités serait que l'argent aboutisse entre les mains d'une organisation terroriste. Mais nous n'allons pas jusque-là. Nous ne prouvons pas que ces fonds ont été récoltés et que, par conséquent, ils serviront à financer le terrorisme. Ça n'est pas notre mandat. Notre mandat consiste à faire appliquer la réglementation. C'est pourquoi nous avons établi ces règlements sous le régime de la Loi de l'impôt sur le revenu : pour être capable de protéger le secteur et les actifs qui s'y trouvent.

Je ne pense pas que vous pourrez vous faire une idée des sommes ayant servi à financer le terrorisme par l'intermédiaire d'organismes de bienfaisance en regardant ces lettres, mais elles vous donneront une indication du type de travail réglementaire que nous faisons.

C'est une question un peu nuancée. Nous avons fait de notre mieux pour y répondre, mais ça n'est pas aussi simple que de dire combien d'organismes de bienfaisance financent le terrorisme.

La sénatrice Beyak : En complément à la question du président, y a-t-il une étape qui devrait suivre votre intervention, un endroit où envoyer les choses? Je comprends tout à fait ce que vous dites. Ça n'est pas du ressort de votre agence. Tout le monde dit : « Ça n'est pas mon travail », mais c'est vrai. Que pourrions-nous recommander, en tant que comité sénatorial, pour faciliter ce processus?

Mme Hawara : Alors, nous nous considérons comme un élément du vaste effort gouvernemental visant à s'attaquer au terrorisme et à son financement, et l'échange de renseignements est essentiel à cet effort. Ainsi, dans le cadre du travail que nous

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

can consider it as part of their responsibilities and accountabilities to determine whether there is something more that they can do.

I think the mechanisms are in place for that to happen, and we are actively sharing information, within the confines of the Income Tax Act, in order to enable others to do their work.

You're right: There is a limit to what we can do. Our role is very much a preventative one in terms of protecting the charities themselves and the charitable sector, but we are dealing with those organizations, not the individuals involved with them. There are others in government who need access to our information, and we're there to provide it.

The Chair: Colleagues, I just want to follow up. They always say, "Follow the money," and you people, in your responsibilities, are following the money. I don't quite understand this: If a charitable organization has been identified, in one manner or another, as being involved with terrorist activity, why wouldn't you know the amount of money involved within that charity, because you've revoked their charitable status? What happened to the money? Who gets the money, and how much money was involved? It would seem to me to be very important to the general public that is watching this meeting. They would want to know how much money was involved in these charitable organizations. Now we've gone from eight to six, and you haven't explained why we went from eight to six organizations. How much money was involved? Because I think Canadians have the right to know. If you can't tell us, who can?

Ms. Hawara: If I may, chair, in each of the letters, as I was mentioning earlier, there's a full accounting of what we found. So if we audited over a period of two or three years and we found that money went overseas or money was used improperly in whatever way, all of that information is in the letter. The letters are available to the public upon request. A summary is published on the CRA's website. Usually in the summary we also include what the most significant findings were, and if there is money attached to that, we will highlight it.

I take your point, and we certainly do —

The Chair: Just to conclude, and then we'll get on to other questions, it will take us to look at the letters, and we're going to get six letters out of eight. We can add or subtract, and then we'll get the amount of money that was involved with respect to these charitable organizations. Is that correct?

Ms. Hawara: That's right.

The Chair: Okay, just so I have that clear.

faisons, nous pouvons communiquer beaucoup d'informations à nos partenaires, puis ils peuvent considérer que cela fait partie de leurs responsabilités et déterminer s'ils peuvent faire quelque chose de plus.

Je pense que les mécanismes nécessaires sont en place pour que cela se produise, et nous communiquons activement les renseignements, dans les limites prévues par la Loi de l'impôt sur le revenu, afin de permettre à d'autres intervenants de faire leur travail.

Vous avez raison : nos capacités sont limitées. Notre rôle est très préventif et consiste à protéger les organismes de bienfaisance et le secteur de la bienfaisance, mais nous faisons affaire avec ces organisations, pas avec les personnes qui en font partie. D'autres intervenants du gouvernement ont besoin d'accéder à nos renseignements, et nous sommes là pour les leur fournir.

Le président : Chers collègues, je veux seulement faire le suivi. On dit toujours : « Suivez l'argent » et, dans le cadre de vos responsabilités, c'est ce que vous faites. Je ne comprends pas très bien ceci : si un organisme de bienfaisance a été détecté, d'une manière ou d'une autre, comme étant impliqué dans une activité terroriste, pourquoi ne connaîtriez-vous pas la somme d'argent en cause au sein de cet organisme, puisque vous avez révoqué son statut d'organisme de bienfaisance? Qu'est-il arrivé à l'argent? Qui le reçoit, et quelles sommes étaient en cause? Il me semble que cela doit être très important pour le grand public qui regarde la séance. Il veut probablement savoir combien d'argent était en cause dans ces organismes de bienfaisance. Nous sommes passés de huit à six organisations, et vous n'avez pas expliqué pourquoi. Combien d'argent était en cause? Parce que je pense que les Canadiens ont le droit de savoir. Si vous ne pouvez pas nous le dire, qui le peut?

Mme Hawara : Si je puis me permettre, monsieur le président, chacune des lettres que j'ai mentionnées plus tôt contient un compte rendu complet de ce que nous avons découvert. Ainsi, si nous avons procédé à un audit sur une période de deux ou trois ans et que nous découvrons que des sommes d'argent sont allées à l'étranger ou que de l'argent est utilisé de façon inappropriée, de quelque manière que ce soit, toute cette information figure dans la lettre. Les lettres sont accessibles au public, sur demande. Un résumé est publié sur le site web de l'ARC. Habituellement, dans le résumé, nous précisons également quelles ont été les constatations les plus importantes, et, si des sommes d'argent s'y rattachent, nous le soulignons.

Je comprends votre point de vue, et il est certain que nous...

Le président : Simplement pour conclure, puis nous allons passer à d'autres questions : il faudra que nous jetions un coup d'œil aux lettres, et nous allons en recevoir six sur huit. Nous pourrons faire les additions ou les soustractions nécessaires, et nous obtiendrons les sommes d'argent qui étaient en cause relativement à ces organismes de bienfaisance. Est-ce exact?

Mme Hawara : C'est exact.

Le président : D'accord, je voulais seulement que ce soit clair.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*Translation*]

Senator Dagenais: I would like to come back to the issue of charities whose charter has been revoked. Obviously, you revoked their charter because, as administrators, you suspected that sums might have been sent to organizations that were not necessarily "terrorists" but of which the objectives were somewhat suspicious.

When you revoke the charter of certain organizations because you have doubts about the destination of sums of money, do you notify the Royal Canadian Mounted Police so that it can conduct an investigation? I imagine that, the moment you have any doubts, as administrators, you notify the RCMP?

Ms. Hawara: Yes. We have a very good relationship with the RCMP. We send it the information that we obtain through our audits. An agreement exists between the two organizations.

Under the Income Tax Act, we have the authority to share this type of information and we do so regularly, because we all have a role to play in this file. However, there is a limit to our authority and, by sending the RCMP information to which we have access, we help it fulfil its mandate.

Senator Dagenais: I understand that you have revoked the charter of eight organizations. You are not obliged to tell me how many you have in your crosshairs. However, I imagine that, in your work as administrators, it is possible that you are monitoring other organizations, that you have your eye on them. I will not ask you how many, but is it possible that there could be other organizations that are being closely examined by your administration?

Ms. Hawara: Yes, certainly. We have many responsibilities. We do not just conduct audits, we also conduct surveillance. On an ad hoc basis, we examine the activities of various charitable organizations. The sector is vulnerable, but not all charitable organizations interest us with respect to this particular concern. The number is still quite small. In the context of our work, we are constantly gathering information and examining the activities and annual statements of organizations to determine where we need to concentrate our efforts in this respect.

Senator Carignan: You say that eight charters were revoked. I also read in January, in a publication, that five organizations were subject to revocation following an investigation of political activities. There is no doubt some overlap. Are some of these five organizations also found in the eight previously mentioned?

Ms. Hawara: No, they do not overlap. To be more specific, the five organizations you mentioned have not yet had their status revoked. We have stated our intention to revoke them, but the organizations in question have rights to an appeal, and we have

[*Français*]

Le sénateur Dagenais : J'aimerais revenir à la question des organismes de charité dont la charte a été révoquée. Évidemment, vous avez révoqué leur charte parce que, en tant qu'administrateurs, vous soupçonniez que des sommes pouvaient être envoyées à des organismes pas nécessairement « terroristes », mais dont les buts étaient plutôt suspects.

Lorsque vous révoquez la charte de certains organismes parce que vous avez des doutes quant à la destination des sommes d'argent, est-ce que vous en avisez la Gendarmerie royale du Canada afin qu'elle puisse faire enquête? J'imagine que, à partir du moment où vous avez des doutes, en tant qu'administrateurs, vous en avisez la GRC?

Mme Hawara : Oui. Nous avons une très bonne relation avec la GRC. Nous lui communiquons les renseignements que nous obtenons dans le cadre de nos vérifications. Il existe une entente entre les deux organisations.

En vertu de la Loi de l'impôt sur le revenu, nous avons l'autorité de partager ce genre d'information et nous le faisons de façon régulière, parce que, justement, nous avons tous un rôle à jouer dans le cadre de ce dossier. Cependant, il y a une limite à notre autorité et, en transmettant à la GRC l'information à laquelle nous avons accès, nous l'aidons à remplir son mandat.

Le sénateur Dagenais : Je comprends que vous avez révoqué la charte de huit organismes. Vous n'êtes pas obligée de me dire combien vous en avez dans la mire. Toutefois, j'imagine que, dans le cadre de votre travail d'administrateurs, il se pourrait que vous en surveilliez d'autres, que vous avez à l'œil. Je ne vous demande pas combien, mais est-ce qu'il pourrait y en avoir d'autres qui sont sous la loupe de votre administration?

Mme Hawara : Oui, certainement. Nous exerçons une panoplie de responsabilités. Il ne s'agit pas seulement de vérifications comme telles, nous faisons également de la surveillance. De façon ponctuelle, nous examinons les activités des différents organismes de bienfaisance. Il y a une vulnérabilité dans le secteur, mais ce ne sont pas tous les organismes de bienfaisance qui nous intéressent par rapport à cette inquiétude en particulier. Il s'agit tout de même d'un petit nombre. Dans le cadre de notre travail, il s'agit d'amasser constamment de l'information et d'examiner les activités et les déclarations annuelles des organismes afin de déterminer où nous devons concentrer nos efforts à cet égard.

Le sénateur Carignan : Vous dites que huit chartes ont été révoquées. J'ai lu également en janvier, dans une publication, que la révocation de cinq organismes avait été effectuée à la suite d'enquêtes de vérification d'activités politiques. Il y en a sans doute qui se recoupent. Est-ce que, parmi les cinq, on en retrouve dans les huit?

Mme Hawara : Non, ils ne se recoupent pas. Pour préciser, les cinq dont vous parlez n'ont pas encore été révoqués. Nous avons signalé notre intention de les révoquer, mais les organismes en question ont des droits d'appel, et nous avons décidé de les laisser

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

decided to allow them to exhaust their appeal rights before making a decision. We have not yet revoked the charters of the five organizations you mentioned but more specifically, there is no overlap between the eight and the five.

Senator Carignan: In the context of your prevention process or your detection methods, I assume that you have a team or a special division responsible for conducting research to identify organizations susceptible of funding terrorist activities. Other than this division within your department, are there other detection methods in place? I would like to suggest one: the online publication of data. I know that data is transmitted and accessible to the general public on the Web. In another life, I used it myself to find the transactions that I deemed inappropriate. The information that I used on the site was extremely useful to me, but I had to combine it with other information.

Have you considered publishing more information on charities, for example, on the donors and the individuals or organizations who receive money, by the size of the donation? You understand that 40 million people could consult this information, which would increase your detection ability.

Ms. Hawara: That is one of the main reasons why we publish this information. We do it not only to allow donors to make informed decisions about the organizations they want to support, but also, as you say, to bolster our efforts to ensure compliance.

We are currently conducting a review of our system with a view to making improvements. We think that we can improve the information that is posted on the website. Will we go as far as publishing the names of donors? I do not believe that we will go that far, mostly because we currently do not ask charities to provide us with this information, except in certain specific circumstances involving overseas donors.

A balance must be struck between the administrative burden imposed on charities and the information that must be gathered, both for the public and for us. Certainly, one of the important sources of information is what we receive from our partners. This information is undoubtedly examined through the work of the division you mentioned.

Senator Carignan: When do you aim to change the rules or increase transparency?

Ms. Hawara: We are nearly at the midway point in our process. We should have a new statement and a new process for submitting information in electronic format by the end of 2018.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

épuiser ces droits d'appel avant de prendre une décision. Nous n'avons pas révoqué les cinq dont vous parlez, mais plus précisément, il n'y a aucun recoupement entre les huit et les cinq.

Le sénateur Carignan : Dans le cadre de votre processus de prévention ou de votre méthode de détection, je présume que vous avez une équipe ou une division spéciale chargée de faire ces recherches afin de déceler les organisations susceptibles de faire du financement à des fins d'activités terroristes. Outre cette division au sein de votre département, y a-t-il d'autres méthodes de détection qui sont en place? Je vous en suggère une : la publication sur Internet des données. Je sais que des données sont transmises et accessibles au grand public sur le Web. Dans une autre vie, je m'en suis moi-même servi pour détecter des transactions que je jugeais inappropriées. L'information que j'ai utilisée sur le site m'a été extrêmement utile, mais j'ai dû la combiner à d'autres renseignements.

Avez-vous pensé à publier davantage d'information sur les organismes de charité, par exemple les donateurs et les gens ou organisations qui reçoivent de l'argent, selon l'ampleur du don? Vous comprenez que 40 millions de personnes pourraient consulter cette information, ce qui augmente la capacité de détection.

Mme Hawara : C'est l'une des raisons principales pour laquelle nous publions cette information. Nous le faisons non seulement pour permettre aux donateurs de prendre des décisions éclairées par rapport aux organismes qu'ils veulent appuyer, mais aussi, comme vous dites, pour appuyer nos efforts en termes de respect de la loi.

Nous menons présentement un examen de notre système dans la perspective d'y apporter des améliorations. Nous pensons pouvoir améliorer les renseignements qui sont affichés sur le site web. Ira-t-on jusqu'à publier le nom des donateurs? Je crois que nous n'irons pas jusque-là, principalement parce que nous ne demandons pas aux organismes de bienfaisance de nous fournir cette information en ce moment, sauf dans certaines circonstances précises lorsqu'il s'agit de donateurs étrangers.

Il faut trouver un juste équilibre entre le fardeau administratif que l'on impose aux organismes de bienfaisance et les renseignements que l'on doit recueillir, tant pour le public que pour nous. Certainement, l'une des sources importantes d'information est celle que l'on reçoit de nos partenaires. Cette information est certainement examinée dans le cadre du travail de la division dont vous parlez.

Le sénateur Carignan : À quel moment prévoyez-vous changer les règles ou augmenter les éléments de transparence?

Mme Hawara : Nous sommes presque à mi-chemin dans notre processus. Nous devrions avoir une nouvelle déclaration et un nouveau processus pour la soumettre sous forme électronique vers la fin de 2018.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*English*]

Senator Day: I want to get an understanding as to your relationship with other security agencies in Canada. I guess that would be Mr. Bland, but from a statistical point of view, how many revocations have you had as a result of a court finding that a terrorist activity has taken place by one of these registered charities using charitable money?

Mr. Bland: I don't know of any that resulted as a result of a court finding.

Senator Day: So they're all based on your forensic audit looking at a risk analysis of various registered charities, and then your dialogue; that is, all this writing back and forth asking, "Why did you use the money for that purpose; so explain to us?" We will find all of that in the correspondence that you will be sending to us in due course. Is that correct?

Ms. Hawara: Yes.

Senator Day: We will get a good flavour for that side of your activity.

Mr. Bland, as head of analysis doing the audits and the risk-based analysis, do you take a look at those particular areas — not the ones where you've decided and gone all the way down the line and suspended, but there are others in between. Do you look at who is on the board of directors, which lawyers were involved, all of that activity, and do you make that information available to other security agencies in Canada?

Mr. Bland: Yes. This question came up with Senator Dagenais as well.

Since 2008-09, there have been 110 occasions where we saw fit to share information about either an applicant or a registered charity with the RCMP. In almost all the situations — in fact, the numbers are the same — we saw fit to share similar information with CSIS as well.

There are occasions where we would share or solicit information from FINTRAC with respect to either a charitable applicant or one of the existing organizations.

Senator Day: Do you share that to get some information back? Is that why you are doing this?

Mr. Bland: There are a number of reasons why we share information. Primarily, in order to ask their assistance on a matter and to get proper context around what it is that we're asking, we have to divulge the information about the taxpayer to them so that would be considered a disclosure. There are other times where we're perfectly comfortable in dealing with the

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*Traduction*]

Le sénateur Day : Je veux arriver à comprendre votre relation avec les autres organismes de sécurité du Canada. Je suppose que cette question s'adresse à M. Bland, mais, d'un point de vue statistique, à combien de révocations avez-vous procédé après qu'un tribunal a conclu qu'une activité terroriste avait été commise par l'un de ces organismes de bienfaisance enregistrés au moyen de fonds destinés à des œuvres caritatives?

M. Bland : Je n'en connais aucune qui a découlé de la conclusion d'un tribunal.

Le sénateur Day : Alors, les révocations sont toutes fondées sur votre vérification médico-légale fondée sur une analyse des risques posés par divers organismes de bienfaisance enregistrés, puis votre dialogue, c'est-à-dire toute cette correspondance où vous demandez : « Pourquoi avez-vous utilisé l'argent à cette fin; expliquez-le-nous donc? » Nous découvrirons tout cela dans le dossier que vous allez nous envoyer en temps et lieu. Est-ce exact?

Mme Hawara : Oui.

Le sénateur Day : Nous obtiendrons un bon aperçu de ce volet de vos activités.

Monsieur Bland, en tant que chef de l'analyse qui effectue les audits et les analyses fondés sur les risques, étudiez-vous les aspects particuliers — pas ceux à l'égard desquels vous avez pris une décision et êtes allé jusqu'à la suspension, mais il y en a d'autres au milieu. Tenez-vous compte des personnes qui siègent au conseil d'administration, des avocats qui ont participé, de toute cette activité, et mettez-vous ces renseignements à la disposition d'autres organismes de sécurité du Canada?

M. Bland : Oui. La question a également été posée par le sénateur Dagenais.

Depuis 2008-2009, il y a eu 110 occasions où nous avons jugé qu'il convenait de communiquer à la GRC de l'information au sujet d'un demandeur ou d'un organisme de bienfaisance enregistré. Dans presque toutes les situations — de fait, les chiffres sont les mêmes —, nous avons cru bon communiquer des renseignements semblables au SCRS également.

Il y a eu des occasions où nous avons communiqué ou demandé de l'information au CANAFE concernant un demandeur souhaitant être enregistré à titre d'organisme de bienfaisance ou l'une des organisations existantes.

Le sénateur Day : Communiquez-vous ces renseignements dans le but d'en obtenir en retour? Est-ce la raison pour laquelle vous le faites?

M. Bland : Nous communiquons cette information pour un certain nombre de raisons. Principalement, si nous voulons demander l'aide de ces organismes à l'égard d'une affaire et obtenir des renseignements appropriés sur le contexte qui l'entoure, nous devons leur communiquer l'information au sujet du contribuable, alors c'est considéré comme une communication.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

situation ourselves through our own mandate, but we feel an obligation to share with them because there might be something here that they may want to pick up on. I would call that proactive.

There are other occasions where they will actually ask us about a particular ongoing investigation and whether there are connections to the charitable sector or any registered charity in Canada. We will look through that and determine whether or not there are connections to their existing, ongoing investigation.

Senator Day: Following that forward, you determine the relevancy. In your submission you said the CRA may disclose information when it is relevant. So you determine relevancy. Do you have a memorandum of understanding with any of the 16 other government institutions with which you share this information to make sure that it's not then misused by them in any manner?

Mr. Bland: We have existing memorandums of understanding with the RCMP and with CSIS. Our primary reason for dealing with FINTRAC would be to share information. Their primary function is to share with intelligence services, so sharing with them automatically makes information — or the purpose of doing so is to make the information available to CSIS and the RCMP.

With respect to the other organizations identified, we haven't developed them as yet because we hadn't, until August, had the express authority to share specifically with them. Now that we do, if there's regular sharing that isn't just one-off, we'll certainly look at the necessity of having a memorandum of understanding.

But it's clear in our letters, when we articulate why we're sharing the information and under what authority we do so, the limits of that authority and their ability to use that information.

Senator Day: My concern is that it's gone up from 3 or 4 agencies that you could deal with and keep your arms around to 16 agencies under the new legislation. That's a lot of personal information that was with Canada Revenue Agency now being shared with 16 different agencies, all of which have relationships with other international organizations.

If I were a lawyer and happened to have been involved initially in helping to incorporate this agency, this could impact very seriously on my credibility later on, perhaps without my knowing anything about this until it's down the road quite a ways. So there has to be some sensitivity to the sharing that you're doing. I'm looking for some reassurance from you that such sensitivity is there.

D'autres fois, nous sommes parfaitement à l'aise de régler la situation nous-mêmes dans le cadre de notre propre mandat, mais nous nous sentons obligés de communiquer avec eux parce qu'il pourrait y avoir quelque chose sur quoi ils pourraient vouloir revenir. J'appellerais cela de la communication proactive.

À d'autres occasions, ils nous posent des questions au sujet d'une enquête particulière en cours et nous demandent s'il y a des liens avec le secteur de la bienfaisance ou avec tout organisme de bienfaisance enregistré au Canada. Nous étudions la question et déterminons s'il y a ou non des liens avec leur enquête en cours.

Le sénateur Day : Après cela, vous déterminez la pertinence. Dans votre mémoire, vous dites que l'ARC pourrait communiquer des renseignements s'il est pertinent de le faire. Ainsi, vous déterminez la pertinence. Avez-vous signé un protocole d'entente avec l'une des 16 autres institutions gouvernementales auxquelles vous communiquez ces informations pour vous assurer qu'elles ne les utilisent pas ensuite de façon inappropriée?

M. Bland : Nous avons conclu des protocoles d'entente avec la GRC et avec le SCRS. La principale raison pour laquelle nous faisons affaire avec le CANAFE est pour échanger des renseignements. La fonction principale de cet organisme est d'échanger des services de renseignement, alors la communication à cet organisme rend automatiquement les renseignements... ou le but de cette communication est de rendre les renseignements accessibles au SCRS et à la GRC.

En ce qui a trait aux autres organisations mentionnées, nous n'avons encore rien conclu avec elles parce que, avant le mois d'août, nous n'avions pas l'autorisation expresse d'échanger des renseignements avec elles précisément. Maintenant que nous l'avons, s'il y a des échanges réguliers qui ne sont pas des cas isolés, nous allons certainement étudier la nécessité de conclure un protocole d'entente.

Mais nos lettres expliquent clairement pourquoi nous communiquons l'information et en vertu de quelle autorité nous le faisons, les limites de cette autorité et la capacité de l'organisme d'utiliser cette information.

Le sénateur Day : Ma préoccupation tient au fait que vous êtes passé de trois ou quatre organismes avec lesquels vous pouviez faire affaire et entretenir des relations à 16 organismes sous le régime de la nouvelle loi. Cela fait beaucoup de renseignements personnels qui étaient à l'Agence du revenu du Canada et qui sont maintenant communiqués à 16 organismes différents, qui sont tous en relation avec d'autres organisations internationales.

Si j'étais avocat et que j'avais contribué, au départ, à aider un organisme à se constituer en société, cela pourrait avoir des conséquences très graves sur ma crédibilité, plus tard, peut-être sans que je le sache, jusqu'à ce que le processus soit bien avancé. Alors, il doit y avoir une certaine sensibilité quant aux renseignements que vous communiquez. Je veux que vous me rassuriez quant à l'existence de cette sensibilité.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Mr. Bland: Yes, certainly. As Ms. Hawara mentioned, there are limitations on our ability to share. First and foremost, it's at our discretion whether we share or not.

Senator Day: You determine whether it's relevant.

Mr. Bland: We will look at it and determine whether it's relevant to that organization's national security responsibilities. We document as to why we feel it is relevant.

Also, it must be relevant to a terrorism offence or a threat to the security of Canada as defined under the CSIS Act. It still needs to meet those two tests as well.

Senator Day: But you're applying the test. You're not going to a judge. You're not going to an independent third party. You're reading the CSIS Act and determining whether you should provide this information.

Mr. Bland: That's correct.

Senator Beyak: Do you proactively review and critically examine charities operating in zones of radicalization such as Syria, Pakistan and Libya? Can you tell us if you've found anything in the past few years? It may be out of your reach, but I wanted to ask.

Mr. Bland: We receive between 3,000 and 4,000 applications a year for registered charitable status. We use risk indicators to help be efficient and effective in only focusing on those particular applicants that may pose a threat or a risk in this area. An area where there are conflicts, such as the ones you mentioned, certainly is an indicator that we would need to take a closer look at that particular application to ensure that there are no concerns that the organization's activities would fall afoul.

We deny applications based on unacceptable risk. Some of those applications have come from organizations proposing to operate in those areas, yes. I'm afraid I don't have the numbers on me, though. Sorry.

Senator Mitchell: You've been talking about information that you had the prerogative of giving to some other organization. What about if one of those organizations, like CSIS or the RCMP, came to you for information? Would they need a warrant?

Ms. Hawara: If they're looking for our information in terms of their activities?

Senator Mitchell: Yes.

Ms. Hawara: In the context of information related to national security, there is now a mechanism through the Security of Canada Information Sharing Act. It's the process that Mr. Bland was describing, where you have to meet two thresholds. You need to either demonstrate that the information would be relevant to

M. Bland : Oui, certainement. l'a mentionné Mme Hawara, notre capacité de communication a des limites. Nous le faisons ou pas d'abord et avant tout à notre discrétion.

Le sénateur Day : Vous déterminez si c'est pertinent.

M. Bland : Nous étudions la situation et déterminons si c'est pertinent par rapport à la responsabilité de l'organisation en question en ce qui a trait à la sécurité nationale. Nous documentons les raisons pour lesquelles nous estimons que c'est pertinent.

En outre, il faut que ce soit pertinent par rapport à une infraction terroriste ou à une menace pour la sécurité du Canada au sens de la Loi sur le SCRS. Il faut tout de même que la situation réponde à ces deux critères également.

Le sénateur Day : Mais c'est vous qui appliquez les critères. Vous ne vous adressez pas à un juge. Vous ne vous adressez pas non plus à un tiers indépendant. Vous lisez la Loi sur le SCRS et déterminez si vous devriez fournir les renseignements en question.

M. Bland : C'est exact.

La sénatrice Beyak : Examinez-vous de façon proactive et critique les organismes de bienfaisance qui sont exploités dans les zones de radicalisation comme la Syrie, le Pakistan et la Libye? Pouvez-vous nous dire si vous avez découvert quoi que ce soit au cours des dernières années? C'est peut-être hors de votre compétence, mais je voulais poser la question.

M. Bland : Nous recevons entre 3 000 et 4 000 demandes d'enregistrement à titre d'organisme de bienfaisance par année. Nous utilisons des indicateurs de risque pour nous aider à être efficients et efficaces en ne nous concentrant que sur des demandeurs particuliers qui pourraient poser une menace ou un risque dans cette région. La présence de conflits dans des régions comme celles que vous avez mentionnées constitue certes un indicateur du fait que nous devons étudier de plus près la demande en question pour nous assurer que les activités de l'organisation ne suscitent aucune préoccupation.

Nous refusons les demandes lorsque le risque est inacceptable. Certaines de ces demandes proviennent d'organisations qui proposent de mener leurs activités dans ces régions, oui. J'ai bien peur de ne pas avoir apporté les chiffres, par contre. Désolé.

Le sénateur Mitchell : Vous parlez de renseignements que vous aviez la prérogative de donner à une autre organisation. Qu'arriverait-il si l'une de ces organisations, comme le SCRS ou la GRC, venait vous demander des renseignements? Auraient-elles besoin d'un mandat?

Mme Hawara : Si elles sont à la recherche de renseignements concernant les activités d'un organisme?

Le sénateur Mitchell : Oui.

Mme Hawara : Dans le contexte de renseignements relatifs à la sécurité nationale, un mécanisme est maintenant prévu dans la Loi sur la communication d'information ayant trait à la sécurité du Canada. Il s'agit du processus que décrivait M. Bland, alors qu'il faut répondre à deux critères. Il faut montrer ou bien que les

an investigation of a threat to the security of Canada under the CSIS Act or a terrorism-related offence. If we are satisfied that the information would meet that threshold, then we ask ourselves whether it would be relevant, in your example, to CSIS's or the RCMP's mandate. If those thresholds are met, we could share that national security information with CSIS or the RCMP.

This does not displace, though, the processes that are in place in terms of seeking warrants to obtain information from the agency. It is strictly limited to information-sharing for the purposes of national security.

Senator Mitchell: So in terms of information shared for any other reason, they would need a warrant, but with information for the purposes of national security, they wouldn't need a warrant?

Ms. Hawara: There's a mechanism now looking at the Income Tax Act and looking at the Security of Canada Information Sharing Act specifically to allow for more information-sharing in relation to national security.

Senator Mitchell: If a group is deregistered, are they told explicitly — and maybe we'll see it in this documentation that you'll show us —why they have been deregistered? If it's based, on the other hand, on secret information, in the process of an appeal, are they entitled to a special advocate to be their representative?

Ms. Hawara: In all of the cases we've handled up until now, we've exercised our authority under the Income Tax Act and applied the usual principles of administrative fairness. We share our concerns and the grounds upon which we believe the charities should be sanctioned or revoked, and they have an opportunity to provide representations to us. Then we make a decision. It's transparent to the charity in terms of our concerns and the grounds upon which we will rely in terms of our action.

There is another piece of legislation called the Charity Registration (Security Information) Act. We see it as a reserve power. If the information we needed to rely upon was intelligence or secret information, there is a process outlined in that piece of legislation for proceeding using a certificate process and putting the certificate in front of the court. But we see that as a reserve power, a sort of last resort. We prefer to operate under the Income Tax Act and fully explain to the charity the grounds for revocation and provide them an opportunity to respond.

The reserve power is important. We have not used it, but it is on the statute books.

renseignements sont pertinents par rapport à une enquête sur une menace pour la sécurité du Canada au titre de la Loi sur le SCRS ou sur une infraction liée au terrorisme. Si nous sommes convaincus que les renseignements répondraient à ce critère, nous nous demandons s'ils seraient pertinents — pour utiliser votre exemple — par rapport au mandat du SCRS ou de la GRC. Si ces critères sont respectés, nous pouvons communiquer ces renseignements relatifs à la sécurité nationale au SCRS ou à la GRC.

Toutefois, cela ne supplante pas les processus qui sont établis pour ce qui est de demander des mandats pour obtenir de l'information auprès de l'agence. C'est strictement limité à la communication d'information aux fins de la sécurité nationale.

Le sénateur Mitchell : Alors, dans le cas de renseignements communiqués pour toute autre raison, il leur faudrait un mandat, mais dans celui de l'information communiquée aux fins de la sécurité nationale, ils n'en auraient pas besoin?

Mme Hawara : Un mécanisme est maintenant prévu dans la Loi de l'impôt sur le revenu et dans la Loi sur la communication d'information ayant trait à la sécurité du Canada précisément pour permettre la communication d'une plus grande quantité d'information relativement à la sécurité nationale.

Le sénateur Mitchell : Si un groupe est désinscrit, lui dit-on explicitement — et peut-être que nous allons le voir dans les documents que vous allez nous montrer — pourquoi il l'a été? Si, par contre, la révocation est fondée sur des renseignements secrets, dans le processus d'un appel, a-t-il le droit d'être représenté par un avocat spécial?

Mme Hawara : Dans tous les cas dont nous nous sommes occupés jusqu'à présent, nous avons exercé notre autorité sous le régime de la Loi de l'impôt sur le revenu et avons appliqué les principes habituels de l'équité administrative. Nous communiquons nos préoccupations et les motifs pour lesquels nous croyons que les organismes de bienfaisance devraient être sanctionnés ou voir leur enregistrement révoqué, et ils ont la possibilité de nous présenter des observations. Nous prenons ensuite une décision. Le processus est transparent pour l'organisme de bienfaisance en ce qui a trait à nos préoccupations et aux motifs sur lesquels sont fondées les mesures que nous prenons.

Il existe une autre loi appelée la Loi sur l'enregistrement des organismes de bienfaisance (renseignements de sécurité). Nous la considérons comme un pouvoir de réserve. Si l'information sur laquelle nous devions nous fier consistait en des renseignements ou de l'information secrète, cette loi décrit un processus mené au moyen d'un certificat, où le certificat est présenté au tribunal. Mais nous considérons ce processus comme un pouvoir de réserve, un genre de dernier recours. Nous préférons mener nos activités sous le régime de la Loi de l'impôt sur le revenu et expliquer pleinement les motifs de la révocation aux organismes de bienfaisance et leur donner la possibilité de répondre.

Le pouvoir de réserve est important. Nous ne l'avons pas utilisé, mais il est prévu dans les textes de loi.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Senator Mitchell: I know that it is against the law for registered charities to receive funds from state sponsors of terrorism. There were two, I think, the last time you presented here in June 2015: Iran and Syria. Are there any others now?

Ms. Hawara: Not as far as I'm aware. I believe it's still the two.

Mr. Bland: To my knowledge.

Ms. Hawara: To my knowledge, yes.

Senator Mitchell: If it were to anybody's knowledge, who would that be if not you?

Ms. Hawara: I believe there's a process for amending that piece of legislation in the annex that lists those countries. I believe it would be my colleagues at Public Safety, but to be honest, I'm not 100 per cent sure.

It could potentially be Global Affairs Canada.

Senator Mitchell: And they would tell you?

Ms. Hawara: Yes.

[*Translation*]

Senator Dagenais: I would like to come back to the organizations whose charters you revoked. What were the arguments of these organizations following this revocation? Did they contest your decision? Did they present arguments to change your mind?

Ms. Hawara: Some organizations presented arguments and others did not. In one of two cases, the organization was no longer active, and there was therefore no one to make arguments.

Other organizations told us that they thought they were doing good work, but their submissions were not convincing. The letters that we will provide give an overview of the submissions that we received.

Senator Dagenais: They thought they were doing good work when they were collecting funds for organizations that were possibly financing terrorism? They did not go any further in their arguments? Normally, when a defense is presented, I imagine that it must go a bit further. They did not go further, and just claimed that they thought they were doing good work?

Ms. Hawara: I am giving you a very general summary because I do not remember the cases exactly. I hope you will forgive me.

Senator Carignan: I would like to come back to the question asked earlier about the revocation of the status of the five organizations linked to political activity. In the release, it was stated that there were some 30 audits underway that led to five revocations. So this is fairly high revocation rate. I imagine that it is not the same rate in the case of activities linked to terrorism; at least, I hope not.

Le sénateur Mitchell : Je sais que la loi interdit aux organismes de bienfaisance enregistrés de recevoir des fonds d'États qui soutiennent le terrorisme. Je pense que, la dernière fois que vous vous êtes présentée ici, en juin 2015, il y en avait deux : l'Iran et la Syrie. Y en a-t-il d'autres maintenant?

Mme Hawara : Pas pour autant que je sache. Je crois que c'est encore ces deux-là.

M. Bland : À ma connaissance.

Mme Hawara : À ma connaissance, oui.

Le sénateur Mitchell : Si quelqu'un d'autre devait le savoir, de qui s'agirait-il, sinon vous?

Mme Hawara : Je crois qu'un processus de modification de cette loi prévu dans l'annexe dresse la liste de ces pays. Selon moi, il s'agirait de mes collègues de Sécurité publique, mais, pour être honnête, je n'en suis pas entièrement certaine.

Il pourrait s'agir d'Affaires mondiales Canada.

Le sénateur Mitchell : Et ils vous le diraient?

Mme Hawara : Oui.

[*Français*]

Le sénateur Dagenais : J'aimerais revenir aux organismes dont vous avez révoqué la charte. Quels ont été les arguments de ces organismes à la suite de cette révocation? Ont-ils contesté votre décision? Ont-ils présenté des arguments pour vous faire changer d'avis?

Mme Hawara : Certains organismes ont présenté des arguments et d'autres, non. Dans un ou deux cas, l'organisation était inactive, et il n'y avait donc plus personne pour présenter des arguments.

D'autres organismes nous ont dit qu'ils croyaient bien faire, mais leurs représentations n'étaient pas convaincantes. Les lettres que nous allons fournir font état des représentations que nous avons reçues.

Le sénateur Dagenais : Ils croyaient bien faire lorsqu'ils collectaient des fonds pour des organismes qui finançaient éventuellement du terrorisme? Ils n'allaient pas plus loin dans leur argumentation? Normalement, lorsqu'on présente une défense, j'imagine qu'on doit aller un peu plus loin. Ils n'allaient pas plus loin, en disant qu'ils croyaient bien faire?

Mme Hawara : Je vous donne un résumé très général, parce que je ne me souviens pas des cas précis, alors vous me le pardonnerez.

Le sénateur Carignan : J'aimerais revenir à la question posée tout à l'heure au sujet de la révocation des cinq organismes liés à des activités politiques. Dans le communiqué, on parlait d'une trentaine de vérifications en cours qui auraient mené à cinq révocations. Il s'agit donc d'un taux de révocation assez élevé. J'imagine que ce n'est pas le même taux dans le cas d'activités liées au terrorisme; j'espère qu'il y en a moins.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Can you give us an idea of the selection criteria for the organizations that are being audited and of the number of audits that allowed you to identify eight cases?

Ms. Hawara: I think you are right. There is a high rate with regard to political activity. This is partly because the audits are not random. They are audits that we selected ourselves because we had concerns. We were quite sure that we would find something, that is, non-compliance. It is the same thing for audits that we perform in the case of terrorist activities; these audits are not random either. The Charities Directorate has a general auditing program that includes different types of auditing, which includes random audits. When we look at the auditing program as a whole and we look at the number of revocations, the figure is much smaller. However, and I do not want to compare them because we are talking about two different things, with regard to both political activity and terrorism-related activities, we target the most sensitive cases that could be problematic. That is why the rate is higher.

Senator Carignan: What about the selection criteria and the number?

Ms. Hawara: Concerning selection criteria, we have risk indicators. We have an array of information sources concerning the returns that the organizations themselves fill out: yearly returns, information from our partners, our own research, et cetera. Based on that, we apply risk indicator criteria that we have developed according to the type of activity the organizations carry out and the regions in which they work.

Senator Carignan: With only those two criteria, it remains quite broad.

Ms. Hawara: Yes.

[*English*]

Mr. Bland: It gives you an idea of the types of things we look at, without giving a public playbook of exactly how we select files. It's fair to say that with regard to the regions in which an organization proposes to operate, people can accept that it may or may not pose a risk. The amount of money they propose to expend in that area in relation to activities they may be conducting domestically may play into that as well. If there are some concerns around certain people associated with the charity or suspected of being associated with the charity, and concerns around their linkages, that is certainly relevant as well.

[*Translation*]

Senator Carignan: Are religious leanings taken into account?

Pouvez-vous nous donner une idée des critères de sélection des organismes pour lesquels vous effectuez une vérification et du nombre de vérifications qui ont permis d'arriver au nombre de huit?

Mme Hawara : Je pense que vous avez raison; le taux est élevé quant aux activités politiques. C'est en partie lié au fait qu'il ne s'agit pas de vérifications aléatoires. Il s'agit de vérifications que nous avons sélectionnées, parce que nous avions des inquiétudes. Nous étions tout de même sûrs de trouver quelque chose, comme de l'inobservation. C'est un peu la même chose dans le cadre des vérifications que nous effectuons dans le cas d'activités terroristes; ce ne sont pas des vérifications aléatoires. La Direction des organismes de bienfaisance a un programme général de vérification dans le cadre duquel se retrouve une panoplie de différents types de vérification, y compris des vérifications aléatoires. Donc, lorsqu'on prend le programme de vérification dans son ensemble et qu'on observe le nombre de révocations, le nombre est beaucoup plus petit. Toutefois, sans vouloir faire une comparaison, parce qu'il s'agit de deux choses complètement différentes, dans le cadre des activités politiques et dans le cadre du programme de vérification des activités liées au financement du terrorisme, nous cernons les cas les plus délicats qui pourraient receler des problèmes. Le taux est donc plus élevé pour cette raison.

Le sénateur Carignan : Qu'en est-il des critères de sélection et du nombre?

Mme Hawara : Nous disposons d'indicateurs de risques. Nous avons toute une panoplie de sources d'information quant aux déclarations que font les organismes eux-mêmes : les déclarations annuelles, l'information de nos partenaires, nos propres recherches, et cetera. De là, nous appliquons des indicateurs de risques que nous avons développés selon le type d'activités des organismes et les régions dans lesquelles ils travaillent.

Le sénateur Carignan : Avec seulement ces deux critères, c'est large, tout de même.

Mme Hawara : Oui.

[*Traduction*]

M. Bland : Cela vous donne une idée des types d'éléments que nous étudions, sans révéler au public exactement comment nous sélectionnons les dossiers. Il est juste de dire que, en ce qui a trait aux régions dans lesquelles une organisation propose de mener ses activités, les gens peuvent considérer que cela pourrait ou non poser un risque. La somme d'argent que les organismes proposent de dépenser dans la région en question relativement aux activités qu'ils pourraient mener au pays peut également entrer en ligne de compte. Si l'association — réelle ou soupçonnée — de certaines personnes avec l'organisme de bienfaisance et leurs liens suscitent des préoccupations, il est certain que c'est également pertinent.

[*Français*]

Le sénateur Carignan : Les éléments religieux sont-ils pris en compte?

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*English*]

Mr. Bland: In what context?

[*Translation*]

Senator Carignan: You could perform fewer audits on Catholic charities as compared to other charities that are more closely linked to groups such as Sunnis, as compared to Shiites who may be closer to the source of terrorist activities?

Ms. Hawara: We look more at the type of activity and other indicators. Religion is less of a factor. You must understand the context in which these activities occur. That is why the work is so complex, because we have to understand the dynamics and the context in which the charities operate. Mr. Bland gave you some examples of risk indicators that we use to guide our work.

Senator Carignan: I have one last question, because I did not receive an answer to my previous question.

How many organizations were audited in order to allow you to identify eight?

[*English*]

Mr. Bland: It's difficult to put a specific number on that because of the way we used to operate and the way we would triage the audits we would undertake.

Now that we have the capacity to do so, there are certain organizations for which our division will conduct the audit. The context in which those organizations are operating is crucial to fully comprehend the context in order to get an appropriate finding or outcome of the audit. There may be other occasions where we'll have a look at the organization. There may be concerns around linkages to terrorism, but there are glaring and obvious violations of the provisions under the Income Tax Act, and in all likelihood you could have a simple audit on those areas and revocation would be the net result of something like that. There's no need to use these specialized resources within my division to conduct such an audit because in all likelihood they will be revoked anyway. So it's very difficult to say exactly how many audits were done in order to come to that number of eight.

I can tell you that in the period of 2008 until last year, we concluded 16 audits ourselves. We revoked the organization on eight occasions.

We have the capacity now to conduct or keep an inventory of approximately 10 ongoing audits in any one year. Some audits take two, three years to conclude. We don't start and finish in the same year, but we have the capacity to have an inventory of 10.

[*Traduction*]

M. Bland : Dans quel contexte?

[*Français*]

Le sénateur Carignan : Vous pourriez effectuer moins de vérifications auprès d'une organisation catholique par rapport à une autre qui est davantage liée à des groupes, comme les sunnites, par opposition aux chiites qui risquent de travailler plus en amont dans le secteur du terrorisme?

Mme Hawara : Il s'agit plutôt des activités et d'autres indicateurs; le point de départ n'est pas la religion. Cependant, il faut tout de même que l'on comprenne le contexte dans lequel ces activités se déroulent. C'est pourquoi le travail est assez complexe, parce qu'il faut comprendre la dynamique et le contexte selon lesquels ils opèrent. Ce sont plutôt les exemples d'indicateurs de risques que M. Bland a énoncés qui dirigent notre travail.

Le sénateur Carignan : J'aurais une dernière question, puisque je n'ai pas eu de réponse à ma dernière question.

Combien d'organismes ont fait l'objet de vérifications pour que vous arriviez à un résultat de huit?

[*Traduction*]

M. Bland : Il est difficile de mettre un chiffre précis là-dessus en raison de la façon dont nous fonctionnions et dont nous procédions au triage des audits que nous entreprenions.

Maintenant que nous avons la capacité de le faire, il y a certainement des organisations pour lesquelles notre division mènera l'audit. Le contexte dans lequel ces organisations mènent leurs activités est crucial pour qui veut comprendre pleinement la situation afin d'arriver à une conclusion ou à un résultat approprié pour l'audit. Il pourrait y avoir d'autres occasions où nous allons examiner l'organisation. On pourrait être préoccupé par des liens avec le terrorisme, mais il y a des infractions flagrantes et évidentes aux dispositions de la Loi de l'impôt sur le revenu, et il est fort probable que l'on puisse procéder à un simple audit de ces questions et que la révocation soit le résultat net de quelque chose du genre. Au sein de ma division, il y est inutile d'avoir recours à ces ressources spécialisées pour procéder à un tel audit parce qu'il est fort probable que l'enregistrement sera révoqué de toute manière. Il est donc très difficile de dire exactement combien d'audits ont été effectués pour en arriver au nombre de huit.

Je peux vous dire que, pendant la période qui s'est étendue de 2008 à l'an dernier, nous avons conclu 16 audits par nous-mêmes. Nous avons révoqué l'enregistrement de l'organisation à huit occasions.

Nous avons maintenant la capacité de tenir ou de poursuivre environ 10 audits en cours durant une même année. Certains audits sont conclus en deux ou trois ans. Nous ne pouvons pas les commencer et les terminer durant la même année, mais nous avons la capacité d'en mener 10 de front.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Senator Carignan: That's enough.

Mr. Bland: It's really hard to determine how much is enough. We could audit all 86,000 if you want. It's getting the right balance and taking a risk-based approach. We'll pick the top 10, yes.

Senator Ngo: Thank you, Ms. Hawara and Mr. Bland.

A previous witness to this committee recommended that the CRA limits cash donations to charities to prevent such funds being misused or being used to fund radical terror-linked purposes. Has this been considered by the CRA, and what actions have been taken to move such an idea forward?

Ms. Hawara: I just want to make sure I understand. The idea is to limit the amount of cash donations?

Senator Ngo: That's correct.

Ms. Hawara: Writ large or coming in from foreign sources?

Senator Ngo: From foreign sources.

Ms. Hawara: The Canada Revenue Agency is responsible for administering the Income Tax Act as it's currently drafted. Something like that particular idea would likely require an amendment to the Income Tax Act, and that would fall to our colleagues at the Department of Finance. It wouldn't be something that the CRA itself could impose.

Currently there are no particular restrictions, with the exception of the donations from state sponsors of terrorism. The limitations or the requirements apply to the resources of the charity, not where they come from.

Senator Ngo: So you have no authority to prevent them from outside. How about inside of Canada?

Ms. Hawara: A registered charity, regardless of where the funds have come from, has to operate in a certain way and within certain requirements. That's our role: ensuring that they're operating for exclusively charitable purposes, that they maintain direction and control over their assets and resources, whether it's here or abroad. The requirements apply to the assets once they've been amassed.

Senator Mitchell: Are you stuck at eight? Are there no more since you last reported to us?

Ms. Hawara: Not since we were here last.

Senator Mitchell: I guess it's conceivable that once they lose their charitable status, an organization can continue to collect money and just not give a charitable deduction. Then, if there were a problem, it would become a police problem.

Le sénateur Carignan : C'est suffisant.

M. Bland : Il est vraiment difficile de déterminer combien est suffisant. Nous pourrions soumettre les 86 000 organismes à un audit, si vous voulez. Il s'agit d'établir le bon équilibre et d'adopter une approche fondée sur les risques. Nous choisissons les 10 plus importants, oui.

Le sénateur Ngo : Merci, madame Hawara et monsieur Bland.

Un témoin précédent du comité a recommandé que l'ARC limite les dons en espèces versés aux organismes de bienfaisance afin d'empêcher ces fonds d'être mal utilisés ou utilisés pour financer des activités liées au terrorisme radical. Cette recommandation a-t-elle été prise en compte par l'ARC, et quelles mesures ont été prises pour faire avancer cette idée?

Mme Hawara : Je veux seulement m'assurer de comprendre. L'idée est de limiter le montant des dons en espèces?

Le sénateur Ngo : C'est exact.

Mme Hawara : De façon générale ou les dons provenant de sources étrangères?

Le sénateur Ngo : De sources étrangères.

Mme Hawara : L'Agence du revenu du Canada est responsable d'administrer la Loi de l'impôt sur le revenu selon son libellé actuel. Une idée comme celle-là exigerait probablement la modification de cette loi et serait du ressort de nos collègues du ministère des Finances. L'ARC ne pourrait pas l'imposer par elle-même.

Actuellement, il n'y a aucune limite particulière, à l'exception des dons provenant d'États qui soutiennent le terrorisme. Les limites ou les exigences s'appliquent aux ressources de l'organisme de bienfaisance, pas à leur provenance.

Le sénateur Ngo : Alors, vous n'avez aucun pouvoir pour les empêcher de l'extérieur. Qu'en est-il de l'intérieur du Canada?

Mme Hawara : Un organisme de bienfaisance enregistré, quelle que soit la provenance des fonds, doit mener ses activités d'une certaine manière et selon certaines exigences. Voilà notre rôle : nous assurer qu'ils mènent leurs activités à des fins exclusivement caritatives, qu'ils conservent la direction et gardent le contrôle de leurs actifs et de leurs ressources, ici ou à l'étranger. Les exigences s'appliquent aux actifs une fois qu'ils ont été amassés.

Le sénateur Mitchell : Êtes-vous restés à huit? N'y en a-t-il eu aucun autre depuis la dernière fois que vous nous avez rendu des comptes?

Mme Hawara : Pas depuis notre dernière comparution.

Le sénateur Mitchell : Je suppose qu'il est concevable que, une fois qu'elle perd son statut caritatif, une organisation peut continuer de recueillir des fonds et simplement ne pas donner de déduction pour don de charité. Ensuite, s'il y a un problème, il devient un problème pour la police.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Ms. Hawara: Essentially, that's correct. There are requirements in terms of winding down the charity. A charity that's been revoked has to wind down within a year and give up all of its assets. The assets have been allowed to grow within the charitable sector and they must stay in the charitable sector, so a charity would need to demonstrate to us that they have spent all of their assets or donated all of their assets.

That is correct: There is nothing preventing them from continuing on as a non-profit organization or in some other form, but they would no longer be registered with the CRA and they would no longer have the ability to issue tax receipts.

The Chair: Could I follow up on Senator Mitchell and get this clear for the record? An organization that has had its charitable status revoked for terrorism activities, which has accrued a great deal of money, has the ability to pass that money on to whomever they wish?

Ms. Hawara: Not to whomever they wish. They must either spend their assets themselves or make gifts to what are called eligible donees: registered charities in good standing with the CRA and at arm's length from the organization that's been revoked.

The Chair: And you monitor that and you ensure that happens?

Ms. Hawara: We have a team within the directorate that looks after what we call the revocation tax.

The Chair: Colleagues, we're coming to the end of the hour here.

Senator Dagenais, do you have another question?

[*Translation*]

Senator Dagenais: Thank you, Mr. Chair. I have two short questions to ask our witness.

Ms. Hawara, you mentioned charities whose status had been revoked and who came back with very few arguments. It was impossible for two of them because they had already ceased their operations. Is it because your investigations took so long that these two charities were forced to cease operating?

Ms. Hawara: I do not believe that it was because of the time it took. I would have to look at the details of those two cases again. However, from time to time, we find certain organizations that are inactive and in our opinion, as a rule these organizations must operate solely for charitable purposes. So when we realize that a charity is inactive, that raises concerns.

Mme Hawara : Essentiellement, c'est exact. Des exigences s'appliquent à la réduction progressive des activités de l'organisme de bienfaisance. Un organisme dont l'enregistrement a été révoqué doit procéder à la réduction progressive de ses activités dans l'année qui suit et abandonner tous ses actifs. Les actifs ont pu croître à l'intérieur du secteur caritatif, et ils doivent demeurer dans ce secteur, alors les organismes de bienfaisance doivent nous prouver qu'ils ont dépensé tous leurs actifs ou qu'ils en ont fait don.

C'est exact : rien ne les empêche de continuer à mener leurs activités en tant qu'organisme sans but lucratif ou sous une autre forme, mais ils ne sont plus enregistrés auprès de l'ARC et n'ont plus la capacité de délivrer des reçus d'impôt.

Le président : Pourrais-je faire le suivi de la question du sénateur Mitchell et la préciser aux fins du compte rendu? Une organisation dont le statut d'organisme de bienfaisance a été révoqué en raison d'activités terroristes et qui a accumulé beaucoup d'argent a la capacité de transférer cet argent à qui elle le souhaite?

Mme Hawara : Pas à qui elle le souhaite. Elle doit dépenser elle-même ses actifs ou faire des dons à ce que nous appelons des organismes bénéficiaires admissibles : des organismes de bienfaisance en règle auprès de l'ARC et indépendants de l'organisation dont le statut a été révoqué.

Le président : Et vous surveillez ce processus et vous vous assurez que cela se produit?

Mme Hawara : Notre direction compte une équipe chargée de s'occuper de ce que nous appelons l'impôt de révocation.

Le président : Chers collègues, nous arrivons à la fin de l'heure.

Monsieur le sénateur Dagenais, avez-vous une autre question?

[*Français*]

Le sénateur Dagenais : Je vous remercie, monsieur le président, j'aurais deux courtes questions à poser à notre témoin.

Madame Hawara, vous avez mentionné des organismes dont la charte avait été retirée et qui ne vous ont pas donné beaucoup d'arguments. Cela avait été impossible pour deux d'entre eux, car ils avaient déjà cessé leurs opérations. Or, les délais de vos enquêtes sont-ils la cause de la cessation des opérations de ces deux organismes?

Mme Hawara : Je ne crois pas que c'était à cause de délais. Il faudrait que je regarde à nouveau les détails de ces deux cas. Cependant, de temps en temps, nous trouvons que les organisations sont inactives et, la règle générale, selon nous, est qu'un organisme doit fonctionner à des fins exclusivement charitables. Donc, lorsque nous trouvons une organisation qui est inactive, cela soulève des inquiétudes.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Senator Dagenais: Please correct me if I am wrong, but didn't the minister recently receive a mandate not to investigate charities that devote themselves to political activities? If that is the case, has this influenced how you work?

Ms. Hawara: Senator Carignan already mentioned this. Minister Lebouthillier made an announcement, I believe on January 20, concerning the program that we implemented further to the 2012 budget concerning the political activities of charities. That is completely separate from the issue of terrorist financing.

Therefore, the 2012 budget gave us the mandate to increase our monitoring activities, and for this purpose, we planned 60 audits focusing on political activity in particular, because there are specific rules that apply to the political activities of charities. When the minister made her announcement we had completed 30 such audits, 24 were underway and 6 had not yet begun. Given that the results were largely acceptable, we decided to end the program. In short, the 24 audits that were underway will be completed because that is the appropriate thing to do given the arm's length role of the Charities Directorate, but the 6 that had not yet begun will not be part of this program on political activity.

That was the announcement made by the minister on January 20 of this year. We are continuing our work on the 24 audits that were already underway.

[*English*]

Senator Day: Are all of your decisions to revoke final? Is there a "Clean your act up, we'll give you a year, and then we'll come back," kind of situation?

Ms. Hawara: I really appreciate this question, because we have been very focused on revocation, but there are other tools at the directorate's disposal, and the Review and Analysis Division uses them as well. We do take an education-first approach.

We have other tools: If at the conclusion of an audit we find minor issues of non-compliance, we send the charity an education letter. If it's something more troubling and we want a written undertaking on the part of the charity, we negotiate a compliance agreement with them, outlining the corrective measures. Oftentimes we will go back and verify that they have indeed done what they said they were going to do. We also have the ability to impose sanctions: either financial penalties or the authority to suspend the receipting privilege of the organization, and then, of course, there's revocation.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Le sénateur Dagenais : Vous me corrigerez si je me trompe, mais le ministre n'aurait-il pas reçu le mandat dernièrement de ne pas enquêter sur les organismes caritatifs qui se consacrent à des activités politiques? Si c'est le cas, cela a-t-il influencé votre façon de travailler?

Mme Hawara : Justement, le sénateur Carignan en a fait mention. Notre ministre, Mme Lebouthillier, a fait une annonce — le 20 janvier, je crois — concernant le programme que nous avions mis en place à la suite du budget de 2012, quant aux activités politiques des organismes de bienfaisance. C'est tout à fait distinct de la question du financement du terrorisme.

Donc, dans le cadre du budget de 2012, on nous a donné le mandat d'augmenter nos activités d'observation et, à cette fin, nous avions planifié de faire 60 vérifications mettant l'accent sur les activités politiques en particulier, parce qu'il y a des règles spécifiques qui s'appliquent aux activités politiques des organismes de bienfaisance. Lorsque la ministre a fait son annonce, nous avions terminé 30 vérifications, 24 étaient en cours et 6 n'avaient pas encore été entamées. Étant donné que les résultats obtenus étaient largement acceptables, nous avons décidé de commencer à mettre fin au programme. Bref, les 24 vérifications qui étaient en cours seront terminées — parce que c'est ce qui est approprié par rapport au rôle indépendant de la Direction des organismes de bienfaisance —, mais les 6 qui n'avaient pas été entamées ne le seront pas dans le cadre de ce projet sur les activités politiques.

Voilà l'annonce qui a été faite par la ministre le 20 janvier dernier. Nous poursuivons notre travail par rapport aux 24 vérifications qui étaient déjà en cours.

[*Traduction*]

Le sénateur Day : Vos décisions de révocation sont-elles toutes finales? Y a-t-il des genres de situations où vous dites : « Mettez-vous en règle; nous vous accordons un an, puis nous réévaluerons votre situation »?

Mme Hawara : Je suis vraiment heureuse que vous posiez cette question, car nous nous sommes beaucoup concentrés sur la révocation, mais la direction dispose d'autres outils, et la Division de la revue et de l'analyse les utilise également. Nous adoptons une approche axée sur l'éducation d'abord.

Nous possédons d'autres outils : si, à la conclusion d'un audit, nous trouvons des problèmes de non-conformité mineurs, nous envoyons une lettre d'éducation à l'organisme de bienfaisance. S'il s'agit de quelque chose de plus troublant et que nous voulons un engagement écrit de la part de l'organisme de bienfaisance, nous négocions avec lui un accord de conformité décrivant les mesures correctives à prendre. Souvent, nous revenons vérifier si l'organisme a bel et bien fait ce qu'il avait dit qu'il allait faire. Nous avons également la capacité d'imposer des sanctions financières et le pouvoir de suspendre le privilège de perception de l'organisation; ensuite, bien entendu, il y a la révocation.

In the case of the Review and Analysis Division, we've used all of those tools. We have focused today on revocation, but we have also found instances where other approaches were more appropriate given the circumstances.

Senator Day: Thank you. I didn't realize my question would take that long.

Mr. Bland, how many auditors do you have? How many analysts do you have that are working on determining whether you should or should not do an audit?

Mr. Bland: There are approximately 40 staff in my division.

The Chair: Is that 40 auditors?

Mr. Bland: It's 40 staff. Investigative analysts and auditors and geopolitical analysts all work together on audits, as well as research analysts and risk analysts.

With all due respect, I don't think it's a question of how many auditors there are. Depending on how complex the audit is, it may be just an auditor and a research analyst, but in all likelihood, if we're taking the audit on, it's a team approach. We would have a geopolitical analyst, an intelligence analyst, a research analyst, a risk analyst and an auditor.

Senator Day: I'd be interested in following through on that, but I wanted to make sure that I have all the legislation that you're operating under.

I was making a note as you were answering various questions. The Charities Registration (Security Information) Act is one you don't like that much. You prefer to use the Income Tax Act in the process as opposed to the other.

Then there's the recent Security of Canada Information Sharing Act, outlining the 16 agencies that you can share with.

The Anti-terrorism Act amendments last year — you're involved there.

In the CSIS Act, you have to interpret certain sections to determine whether something is relevant for disclosing.

Are there other pieces of legislation that you need as well that are pertinent to your work?

Ms. Hawara: The primary one is the Income Tax Act. That's the act that sets out the requirements for how charities must operate. We have to read it in conjunction with the common law. So a lot about charity law is actually outside of the Income Tax Act. We rely quite heavily on the decisions of tribunals, which have helped form charity law in Canada.

Dans le cas de la Division de la revue et de l'analyse, tous ces outils ont été utilisés. Aujourd'hui, nous nous sommes concentrés sur la révocation, mais nous avons également connu des situations où d'autres approches étaient plus appropriées, compte tenu des circonstances.

Le sénateur Day : Merci. Je n'avais pas pensé que la réponse à ma question serait si longue.

Monsieur Bland, combien d'auditeurs avez-vous? Combien de vos analystes travaillent à déterminer si vous devriez ou ne devriez pas procéder à un audit?

M. Bland : Ma division compte environ 40 employés.

Le président : S'agit-il de 40 auditeurs?

M. Bland : C'est 40 membres du personnel. Des analystes enquêteurs, des auditeurs et des analystes géopolitiques qui travaillent tous ensemble sur les audits, de même que des analystes de la recherche et des analystes des risques.

Avec tout le respect que je vous dois, je ne pense pas que la question soit liée au nombre d'auditeurs. Selon la complexité de l'audit, il ne pourrait y avoir qu'un auditeur et un analyste de la recherche, mais il est fort probable que, si nous entreprenons l'audit, ce sera un travail d'équipe. Nous aurons un analyste géopolitique, un analyste du renseignement, un analyste de la recherche, un analyste des risques et un auditeur.

Le sénateur Day : Je souhaiterais donner suite à cette question, mais je voulais m'assurer de connaître toutes les lois qui régissent vos activités.

J'ai pris une chose en note pendant que vous répondiez aux diverses questions qui vous ont été posées. Vous n'êtes pas vraiment un chaud partisan de la Loi sur l'enregistrement des organismes de bienfaisance (renseignements de sécurité). Vous préférez recourir à la Loi de l'impôt sur le revenu plutôt qu'à l'autre aux fins du processus.

Il y a aussi la Loi sur la communication de l'information ayant trait à la sécurité du Canada qui est récemment entrée en vigueur et qui énumère les 16 organismes avec lesquels vous pouvez échanger des renseignements.

Les modifications apportées l'année dernière à la Loi antiterroriste vous concernent également.

Vous devez interpréter certains articles de la Loi sur le SCRS afin de déterminer s'il est pertinent de divulguer quelque chose.

Y a-t-il d'autres instruments législatifs pertinents qui s'appliquent à vos activités?

Mme Hawara : La Loi de l'impôt sur le revenu est la plus importante, puisqu'elle établit les exigences relatives au fonctionnement des organismes de bienfaisance. Il faut l'interpréter à la lumière de la common law, car une grande partie du droit régissant les organismes de bienfaisance se trouve en marge de la Loi de l'impôt sur le revenu. Nous nous appuyons beaucoup sur les décisions des tribunaux, qui ont aidé à façonner le droit régissant les organismes de bienfaisance au Canada.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Senator Day: Have I mentioned all of the pertinent pieces of legislation under which you operate?

Ms. Hawara: I would think so.

The Chair: I want to clarify a couple of things for the record.

When do you expect the 24 audits, which Senator Dagenais referred to and you brought to the fore, to be done? The audits date back to 2012, when they began.

Ms. Hawara: They didn't all begin in 2012. They were launched over a period of four years, between 2012 and now. I'm hoping to have them done as quickly as possible. Some are more complex than others and will take a bit more time. I don't have any specific timelines that I can share, unfortunately.

[*Translation*]

Senator Carignan: Do you intend to transfer the budget of the section that audited political activity to the section that audits terrorist activity?

Ms. Hawara: Not necessarily. The people on the team that focused on auditing political activity came from different teams within the directorate. Gradually, as we complete the audits, I expect these employees to return to the directorate but not necessarily on one team rather than on another. We are also going to determine where the employees would like to work.

[*English*]

The Chair: I want to make a clarification. I don't think the committee is satisfied with respect to the information on the terrorism files that you were involved with. In view of the fact that you will be corresponding with us, and I'm expecting that to be within the week because the letters are available, I would assume that if you're called upon you would come back to us to answer any questions the committee has in respect of those particular files.

Ms. Hawara: Yes, of course. We are always at the committee's disposal.

The only thing I would mention is that we are somewhat limited in terms of how much we can say about individual charities. The Income Tax Act allows us to disclose the grounds upon which we make decisions; so we will provide that to the committee.

It will depend, perhaps, on the nature of the questions.

The Chair: If you have to plead the "fifth amendment," then you have to do so. I want to know that you will make yourself available to the committee because, quite frankly, the information we were looking for wasn't provided.

Ms. Hawara: Yes.

Le sénateur Day : Ai-je mentionné tous les instruments législatifs s'appliquant à vos activités?

Mme Hawara : Je crois.

Le président : Il y a deux ou trois choses que j'aimerais faire clarifier aux fins du compte rendu.

Le sénateur Dagenais a mentionné 24 vérifications, et vous en avez parlé plus en détail. Selon vous, quand seront-elles terminées? Ces vérifications ont débuté en 2012.

Mme Hawara : Les vérifications n'ont pas toutes commencé en 2012. Elles ont été amorcées sur une période de quatre ans, entre 2012 et aujourd'hui, et j'espère qu'elles seront achevées le plus rapidement possible. Certaines sont plus complexes que d'autres et prendront un peu plus de temps. Malheureusement, je ne dispose d'aucun calendrier précis.

[*Français*]

Le sénateur Carignan : Avez-vous l'intention de transférer le budget du département qui examinait les activités politiques au département qui vise les activités terroristes?

Mme Hawara : Pas nécessairement. Les gens qui forment l'équipe qui s'est concentrée sur les vérifications des activités politiques provenaient de différentes équipes au sein de la direction dans son ensemble. Tranquillement, au fur et à mesure que nous terminons les vérifications, je m'attends à ce que ces employés soient réintégrés au sein de la direction, mais pas nécessairement dans une équipe plutôt qu'une autre. Nous tentons de voir également où les employés aimeraient travailler.

[*Traduction*]

Le président : J'aimerais apporter une précision. Je ne crois pas que le comité a obtenu les renseignements qu'il souhaitait par rapport aux affaires de terrorisme où vous êtes intervenus. Puisque vous allez correspondre avec nous — et je m'attends à ce que cela se produise d'ici une semaine, vu que les lettres peuvent être obtenues —, je tiens pour acquis que vous vous représenteriez ici pour répondre à toute question que le comité pourrait avoir par rapport à ces dossiers en particulier, si nous vous convoquions.

Mme Hawara : Oui, bien sûr. Nous sommes toujours à la disposition du comité.

Je veux tout de même préciser que les renseignements que nous pouvons communiquer par rapport à un organisme de bienfaisance donnée sont limités. En vertu de la Loi de l'impôt sur le revenu, nous pouvons divulguer les motifs d'une décision, et c'est ce que nous présenterons au comité.

Je crois que tout dépendra de la nature des questions posées.

Le président : Si vous ne pouvez pas divulguer certains renseignements, ainsi soit-il. Je veux m'assurer que vous vous mettez à la disposition du comité, car, pour être parfaitement honnête, nous n'avons pas obtenu les renseignements souhaités.

Mme Hawara : Oui.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

The Chair: In terms of the Internet and access to the CRA, I want to reiterate that trying to find four or five files in here out of 32,000 is not an easy task. I would suggest that somebody who understands how to put a website together and make it easy for the general public to find, like me, would be very advisable, and then perhaps you wouldn't get some of the questions you get.

With that, I want to say thank you very much. We appreciate your coming. I'm looking forward to seeing you again.

Joining us on panel 4 today are a number of witnesses from Public Safety Canada, as we begin to look at threats to Canada's critical infrastructure. We are pleased to have with us today Ms. Monik Beauregard, Senior Assistant Deputy Minister, National and Cybersecurity Branch; Mr. Patrick Boucher, Acting Director General, Critical Infrastructure and Strategic Coordination Directorate; Ms. Suki Wong, Director General, National Security Operations Directorate; and Ms. Colleen Merchant, Director General, National Cyber Security Directorate.

Welcome. I understand that you have an opening statement. Please proceed.

[*Translation*]

Monik Beauregard, Senior Assistant Deputy Minister, National and Cybersecurity Branch, Public Safety Canada: Thank you, Mr. Chair and members of the committee, for the opportunity to discuss the resilience of Canada's critical infrastructure.

By way of context, critical infrastructure consists of the physical assets, information technology systems, networks and services essential to the health, safety, security, and economic well-being of Canadians.

Canada has 10 critical infrastructure sectors including: finance; food; transportation; government; information and communication technology; health; water; safety; and manufacturing.

Our critical infrastructure sectors are confronted by a complex mix of risks and threats, such as natural disasters, terrorist attacks and cyber incidents. The risk environment is continuously evolving. For example, natural disasters and severe weather events are striking with greater frequency and severity.

Le président : Pour ce qui est d'Internet et de l'accès en ligne à l'ARC, je tiens à répéter qu'il est difficile de trouver quatre ou cinq fichiers précis parmi 32 000. Je vous suggère de demander à une personne qui s'y connaît en création de sites web et qui sait comment faciliter la recherche pour des gens du grand public comme moi. Ce serait très judicieux, et cela vous éviterait peut-être d'avoir à répondre à certaines questions.

Sur ce, je vous remercie beaucoup. Nous vous sommes reconnaissants d'avoir comparu aujourd'hui, et nous serons heureux de vous revoir une prochaine fois.

Pour la quatrième table ronde d'aujourd'hui, nous recevons des témoins de Sécurité publique Canada afin d'aborder le sujet des menaces qui pèsent sur les infrastructures essentielles du Canada. Nous sommes heureux d'accueillir aujourd'hui Mme Monik Beauregard, sous-ministre adjointe principale, Secteur de la sécurité et de la cybersécurité nationale; M. Patrick Boucher, directeur général par intérim, Direction des infrastructures essentielles et de la coordination stratégique; Mme Suki Wong, directrice générale, Direction des opérations de la sécurité nationale; et Mme Colleen Merchant, directrice générale, Direction de la cybersécurité nationale.

Bienvenue à vous. Je crois que vous avez préparé une déclaration préliminaire. Nous vous écoutons.

[*Français*]

Monik Beauregard, sous-ministre adjointe principale, Secteur de la sécurité et de la cybersécurité nationale, Sécurité publique Canada : Bonjour, monsieur le président et membres du comité. Je vous remercie de me donner l'occasion de discuter avec vous de la résilience des infrastructures essentielles du Canada.

À titre d'information, les infrastructures essentielles regroupent les installations matérielles, les systèmes de technologie de l'information, ainsi que les réseaux et services qui se révèlent fondamentaux pour la santé, la sécurité et le bien-être économique des Canadiens.

Le Canada compte 10 secteurs d'infrastructures essentielles, notamment les finances, l'alimentation, le transport, le gouvernement, les technologies de l'information et de la communication, la santé, l'eau, la sécurité et le secteur manufacturier.

Nos secteurs d'infrastructures essentielles doivent faire face à un amalgame complexe de risques et de menaces, y compris les catastrophes naturelles, les attaques terroristes et les incidents cybernétiques. L'environnement du risque est en constante évolution. Par exemple, les catastrophes naturelles et les phénomènes météorologiques violents frappent avec une fréquence et une gravité accrues.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*English*]

While severe weather events are becoming more destructive, the terrorist threat is taking on new and evolving forms. The most recent public report on terrorist threats to Canada highlighted the threat posed by citizens who travel abroad to commit acts of terror and who subsequently return home to Canada.

Not all extremist travellers who return to Canada represent a terrorist threat. However, some have gained credibility from their time abroad to encourage and recruit aspiring violent extremists in Canada, and it is possible that some returnees could plan and carry out terrorist attacks in Canada. The government is actively dealing with this issue and is seeking to limit travel abroad by violent extremists through the Combating Terrorism Act.

[*Translation*]

The threat environment facing Canada's critical infrastructure sectors is compounded by their reliance on secure cyber systems. Increasingly, hostile actors, such as foreign intelligence agencies, terrorists or "hacktivists," are able to attack Canada's critical infrastructure without actually having to set foot on Canadian soil.

Public Safety Canada and our portfolio agencies are aware of a wide range of targeting against the private sector in Canada, including attacks against the telecommunications sector, the oil and gas industry and other elements of the natural resource sector.

Ultimately, the challenge of protecting our vital assets and systems from these risks and threats demands a cooperative approach to ensure resilience. To this end, Canada's National Strategy and Action Plan for Critical Infrastructure established a collaborative, federal, provincial, territorial and critical infrastructure sector approach to mitigate the full range of risks and threats facing our vital assets and systems.

Building on the strategy's central themes of partnerships, information sharing, and all-hazards risk management, sector networks were established for each of the 10 critical infrastructure sectors, which are led by a responsible federal department or agency, such as Natural Resources Canada in the case of the energy sector and the Public Health Agency of Canada in the case of the health sector.

[*Traduction*]

Alors que les phénomènes météorologiques violents deviennent de plus en plus dévastateurs, la menace terroriste revêt de nouvelles formes en pleine évolution. Le dernier Rapport public sur la menace terroriste pour le Canada souligne la menace que présentent les citoyens qui voyagent à l'étranger pour commettre des actes terroristes, et qui reviennent ensuite au Canada.

Les voyageurs extrémistes qui reviennent au Canada ne représentent pas tous une menace terroriste. Toutefois, certains ont suffisamment de crédibilité pour encourager et recruter des aspirants extrémistes violents au Canada, et il est possible que des voyageurs extrémistes revenus au pays planifient et mettent à exécution des attaques terroristes au Canada. Le gouvernement travaille activement à remédier à ce problème, et s'efforce de limiter les voyages à l'étranger d'extrémistes violents au moyen de la Loi sur la lutte contre le terrorisme.

[*Français*]

Le contexte de la menace à laquelle fait face le secteur des infrastructures essentielles du Canada est compliqué par le fait que ces secteurs dépendent de systèmes cybernétiques sécurisés. De plus en plus, des adversaires, comme des services du renseignement étrangers, des terroristes ou des cyberactivistes, réussissent à attaquer les infrastructures essentielles du Canada sans jamais même avoir mis le pied en territoire canadien.

Sécurité publique Canada et les organismes de notre portefeuille sont au courant de diverses attaques qui ont été perpétrées contre le secteur privé au Canada, notamment contre le secteur des télécommunications, contre l'industrie pétrolière et gazière, et contre d'autres éléments du secteur des ressources naturelles.

La difficulté liée à la protection de nos biens et systèmes fondamentaux contre ces risques et menaces exige une approche concertée pour garantir la résilience. Par conséquent, une approche favorisant la collaboration des gouvernements fédéral, provinciaux et territoriaux ainsi que des secteurs des infrastructures essentielles a été établie dans le cadre de la Stratégie nationale sur les infrastructures essentielles et du Plan d'action sur les infrastructures essentielles du Canada en vue d'atténuer l'éventail complet de risques et de menaces auxquels sont exposés nos biens et systèmes fondamentaux.

Tirant parti des thèmes centraux de la stratégie qui mettent l'accent sur les partenariats, l'échange de renseignements et la gestion des risques, des réseaux sectoriels ont été mis sur pied pour chacun des 10 secteurs d'infrastructures essentielles, lesquels sont dirigés par un responsable d'un organisme ou ministère fédéral, notamment Ressources naturelles Canada dans le cas du secteur de l'énergie, ou encore l'Agence de la santé publique du Canada dans le cas du secteur de la santé.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*English*]

Public Safety Canada is responsible for leading the overall federal effort to strengthen the resilience of critical infrastructure. In particular, we bring value to the public-private sector partnership by bringing stakeholders together to address risks, by providing regular threat briefings, hosting cross-sector exercises and developing risk management tools and guides designed to mitigate the impact of disruptions.

It is important to note that critical infrastructure owners and operators bear the primary responsibility for protecting their assets and systems. They are also responsible for emergency response planning and implementation along with the provinces and territories and municipalities within their respective jurisdictions, given that the majority of disasters occur at the local level.

Public Safety Canada's leadership role is reflected through our shared work with federal departments and agencies which are responsible for their respective sector networks, provinces and territories responsible for leading critical infrastructure protection activities within their jurisdictions, industry partners who own the majority of Canada's critical infrastructure, first responders and international allies.

Recognizing that our prosperity and security as Canadians depend on the complex array of interconnected networks, systems and facilities, Public Safety Canada has established a number of public and private sector engagement initiatives and developed tools to manage risks, reduce vulnerabilities and strengthen the resilience of critical infrastructure.

For example, we have established the National Cross-Sector Forum to bring together senior representatives from all 10 sectors to help set priorities and determine action items and to strengthen our collective resilience. It serves as the centerpiece for partnership and engagement to address cross-sector issues such as interdependencies and cybersecurity.

We've also developed a critical infrastructure information sharing framework to support collaborative efforts among critical infrastructure sectors and all levels of government. As part of this framework, Public Safety Canada has created a secure, web-based platform to make it easier to exchange best practices and information among critical infrastructure sectors and jurisdictions. This online gateway is where we have posted a number our risk management products, including a tabletop exercise or "TTX in a Box," which helps owners and operators develop and test measures to enhance their resilience against a full range of risk and threats.

[*Traduction*]

Sécurité publique Canada est chargée d'orienter l'ensemble des efforts déployés par le gouvernement fédéral pour accroître la résilience des infrastructures essentielles. Plus particulièrement, nous contribuons au partenariat entre les secteurs public et privé en réunissant les intervenants afin d'éliminer les risques, en offrant régulièrement des séances d'information sur les menaces, en animant des exercices intersectoriels, et en élaborant des outils et des guides de gestion des risques conçus pour atténuer l'incidence des perturbations.

Il importe de noter que les propriétaires et les exploitants des infrastructures essentielles sont les principaux responsables de la protection de leurs biens et systèmes. En outre, ils sont chargés de la planification et de la mise en œuvre des interventions d'urgence, au même titre que les provinces, les territoires et les municipalités au sein de leurs administrations respectives, étant donné que la plupart des catastrophes se produisent à l'échelon local.

Le rôle de chef de file de Sécurité publique Canada transparaît dans notre collaboration avec les acteurs suivants : les ministères et organismes fédéraux qui sont responsables de leurs réseaux sectoriels respectifs; les provinces et les territoires qui sont chargés de diriger les activités relatives à la protection des infrastructures essentielles dans leur administration; les partenaires de l'industrie qui détiennent la plupart des infrastructures essentielles au Canada; les premiers intervenants; et les alliés internationaux.

Reconnaissant que notre prospérité et notre sécurité en tant que Canadiens reposent sur l'éventail complexe de réseaux, de systèmes et d'installations interconnectés, Sécurité publique Canada a établi de nombreuses initiatives pour la mobilisation des secteurs privé et public, et a élaboré des outils visant à gérer les risques, à réduire les vulnérabilités et à renforcer la résilience des infrastructures essentielles.

Par exemple, nous avons mis sur pied le Forum national intersectoriel afin de réunir les principaux représentants des 10 secteurs pour contribuer à l'établissement des priorités et déterminer les mesures à prendre en vue d'accroître notre résilience collective. Ce forum constitue la pièce maîtresse en matière de partenariat et de mobilisation pour régler les problèmes intersectoriels, notamment les interdépendances et la cybersécurité.

En outre, nous avons élaboré un cadre d'échange d'information sur les infrastructures essentielles visant à appuyer les efforts de collaboration parmi les secteurs des infrastructures essentielles et tous les ordres de gouvernement. Par l'entremise de ce cadre, Sécurité publique Canada a créé une plateforme web sécurisée pour faciliter l'échange des pratiques exemplaires et des renseignements entre les secteurs des infrastructures essentielles et les administrations. Nous avons affiché de nombreux produits de gestion du risque sur cette passerelle virtuelle, y compris un exercice sur table dans une boîte, qui permet aux propriétaires et aux exploitants d'élaborer des mesures et de mettre celles-ci à l'essai en vue d'accroître leur résilience envers un éventail complet de risques et de menaces.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Recognizing that critical infrastructure is connected across the border, we have several joint initiatives under way with the Department of Homeland Security. For example, we have launched the Regional Resiliency Assessment Program, or RRAP, which is a tangible, boots-on-the-ground way for governments and industry to work together to examine vulnerabilities and threats and implement corrective measures.

The RRAP features site assessments, which culminate in a dashboard for owners and operators of critical infrastructure to evaluate their own resilience to both physical and cyber-threats. The products our clients receive include benchmarking against other facilities in the sector and region, and recommendations for enhancing resilience. We have conducted site assessments of critical infrastructure across Canada, including electricity grids, water treatment facilities and major transit hubs.

[*Translation*]

Keeping our cyber networks secure and resilient is one of the most challenging issues facing the government, private businesses and citizens, and our allies. This is why collaboration has been central to our cyber security efforts. These collaborative efforts are guided by Canada's Cyber Security Strategy, which is founded on three pillars that complement the efforts of our partners at home and abroad — securing government systems; partnering to secure vital cyber systems outside the federal government; and helping Canadians to be secure online.

We have made great progress in all of these areas. For example, we are working to upgrade and streamline federal government information and technology systems. These efforts are improving the security of our systems while enhancing the integrity of the supply chain throughout our supporting infrastructure. We are working to secure the vital systems outside of the federal government, which includes increasing the capacity of the Canadian Cyber Incident Response Centre, or CCIRC.

The CCIRC is mandated to help the provinces, territories, municipalities and the private sector organizations to secure their networks. It acts as a central hub for information sharing about cyber threats in Canada, and coordinates the national response to major cyber incidents.

Reconnaissant que les infrastructures essentielles sont reliées de part et d'autre de la frontière, nous avons entrepris plusieurs initiatives communes avec le département de la Sécurité intérieure. Ainsi, nous avons lancé le Programme d'évaluation de la résilience régionale, ou PERR, qui permet aux gouvernements et à l'industrie de disposer d'un moyen tangible sur le terrain pour travailler de concert et se pencher sur les vulnérabilités et les menaces, et mettre en œuvre les mesures correctives.

Le PERR comprend des évaluations de site, qui donnent lieu à des tableaux de bord permettant aux propriétaires et aux exploitants d'infrastructures essentielles d'évaluer leur propre résilience face à des menaces physiques et cybernétiques. Au nombre des produits que les clients obtiennent figurent, notamment, une évaluation comparative par rapport aux autres installations du secteur et de la région, et des recommandations visant à renforcer la résilience. Nous avons mené des évaluations de site relatives aux infrastructures essentielles partout au pays, y compris en ce qui touche les réseaux de distribution de l'électricité, les usines de traitement de l'eau, et les principaux centres de transit.

[*Français*]

Assurer la sécurité et la résilience des réseaux informatiques constitue l'un des défis les plus importants qui se posent pour notre gouvernement, les entreprises privées, les citoyens et nos alliés. C'est la raison pour laquelle la collaboration se révèle cruciale à nos efforts en matière de cybersécurité. Cette collaboration est orientée par la Stratégie de cybersécurité du Canada, laquelle repose sur trois piliers qui viennent renforcer les efforts déployés par nos partenaires au pays et à l'étranger, c'est-à-dire protéger les systèmes gouvernementaux, nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement fédéral, et aider les Canadiens à se protéger en ligne.

Nous avons accompli de grands progrès dans tous ces domaines. Ainsi, nous nous affairons à mettre à niveau et à rationaliser les systèmes de technologie de l'information du gouvernement fédéral. Ces efforts contribuent à accroître la sécurité de nos systèmes, tout en améliorant l'intégrité de la chaîne d'approvisionnement au sein de toutes nos infrastructures de soutien. Nous nous efforçons de protéger les principaux systèmes à l'extérieur du gouvernement fédéral, ce qui suppose d'accroître la capacité du Centre canadien de réponse aux incidents cybernétiques (CCRIC).

Le CCRIC est chargé d'aider les provinces, les territoires, les municipalités et les organismes du secteur privé à protéger leurs réseaux. Il agit à titre de plateforme centrale pour l'échange de renseignements sur les cybermenaces au Canada et il coordonne les interventions nationales mises en place lorsque surviennent des cyberincidents d'envergure.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Canadian firms and institutions are encouraged to alert CCIRC when they experience a cyber attack. In return, CCIRC provides information and guidance to registered firms to help them protect their systems from complex cyber threats.

[*English*]

Cyber-threats are constantly evolving and Canada needs to work to stay ahead of those risks. As a result, the department is leading a review of existing measures to protect Canadians and critical infrastructure from cyber-threats. The review will inform policy and program decisions that will make critical infrastructure more resilient to cyberattacks and help keep Canadians safe online.

I will conclude by noting that Public Safety Canada remains committed to working with public and private sector critical infrastructure partners to enhance resilience. To meet this goal, we need active participation from all levels of government and the private sector to drive meaningful risk-management action such as risk assessments, contingency planning and exercises.

[*Translation*]

Thank you for your time.

[*English*]

The Chair: Thank you very much. I know it's late in the day and we really appreciate you coming here to present to us.

Before I go to my colleagues, I will ask a question. There was a study done by the Standing Senate Committee on National Security and Defence back in 2004. The report was entitled *National Emergencies: Canada's Fragile Front Lines, An Upgrade Strategy*. Are you familiar with this report?

Ms. Beauregard: We'd have to look at that.

The Chair: Could you undertake to have someone go through that report and give us, in writing, as best you can, an update on the recommendations and if anything has been done with the recommendations?

Ms. Beauregard: Okay.

The Chair: I would ask if it could be done fairly soon because we are going into our study, and this will serve as the basis to some degree.

Ms. Beauregard: We'll definitely follow up on that.

The Chair: Thank you very much; I appreciate that.

On encourage les entreprises et les institutions canadiennes à alerter le CCRIC lorsqu'elles sont victimes d'une cyberattaque. En contrepartie, le CCRIC fournit des renseignements et une orientation aux entreprises inscrites afin de les aider à protéger leur système des cybermenaces complexes.

[*Traduction*]

Les cybermenaces évoluent sans cesse, et le Canada ne doit pas ménager ses efforts pour conserver une longueur d'avance face à ces risques. Par conséquent, le ministère mène à l'heure actuelle un examen sur les mesures existantes visant à protéger les Canadiens et les infrastructures essentielles contre les cybermenaces. Cet examen permettra d'éclairer les décisions en matière de politiques et de programmes qui amélioreront la résilience de nos infrastructures à l'égard des cyberattaques et aideront les Canadiens à assurer leur protection en ligne.

Je termine en mentionnant que le ministère demeure résolu à collaborer avec les partenaires des infrastructures essentielles des secteurs public et privé en vue d'accroître la résilience. Afin d'atteindre cet objectif, la participation active de tous les ordres de gouvernement et du secteur privé est nécessaire pour gérer les importantes mesures associées à la gestion du risque, notamment les évaluations de risque, la planification de mesures d'urgence et les exercices.

[*Français*]

Je vous remercie de m'avoir accordé de votre temps.

[*Traduction*]

Le président : Merci beaucoup. Je sais qu'il se fait tard, et nous vous sommes reconnaissants d'être parmi nous aujourd'hui.

Avant de donner la parole à mes collègues, j'aimerais poser une question. En 2004, le Comité sénatorial permanent de la sécurité nationale et de la défense a mené une enquête et produit un rapport intitulé *Les urgences nationales : le Canada, fragile en première ligne — Stratégie de renforcement*. Connaissez-vous le contenu de ce rapport?

Mme Beauregard : Il faudrait voir.

Le président : Pourriez-vous charger quelqu'un de parcourir le rapport afin de nous faire parvenir, par écrit, au meilleur de vos connaissances, une mise au point concernant les mesures éventuelles que vous avez prises à la lumière des recommandations?

Mme Beauregard : D'accord.

Le président : Cela peut-il être fait assez rapidement? Nous allons procéder à l'étude bientôt, et cela nous servira de base dans une certaine mesure.

Mme Beauregard : Nous allons donner suite à votre demande, c'est certain.

Le président : Merci beaucoup, c'est très apprécié.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*Translation*]

Senator Dagenais: Thank you to our guests. My question is about critical infrastructure security. Could you make a comparison with what is being done in the United States or in Great Britain, if you can, in terms of critical infrastructure security?

Ms. Beauregard: As I mentioned in my statement, we work very closely with our closest allies, the so-called "Five Eyes." We also work very closely with the Americans. When it comes to critical infrastructure, there are not necessarily any borders, particularly given the way that things work from east to west. I will ask Patrick to continue.

[*English*]

Patrick Boucher, Acting Director General, Critical Infrastructure and Strategic Coordination Directorate, Public Safety Canada: Thank you for the question. As Monik indicated, we work very closely with not only our American colleagues to the south but also the Five Eyes community. Related to critical infrastructure specifically, we have what's called the "Critical Five." This is a forum of our Five Eyes allies that we convene on a regular basis to discuss issues very specific to critical infrastructure and critical infrastructure resilience.

As Monik indicated, we work very closely with those partners on various initiatives. A good example is the RRAP program. It's an American methodology, and we've worked in very close collaboration with them to not only employ that here domestically in Canada but also to conduct joint border RRAP assessments with them as well.

[*Translation*]

Senator Dagenais: We are also talking about cyber attacks to which we could fall victim. Could you give us an idea of the profile of those who commit these cyber attacks and of the countries from which they might originate?

Ms. Beauregard: Cyber attacks can come from a large number of actors. They may be nation-states who are simply looking to pursue espionage activities or to seek a certain economic advantage. The government may be targeted for espionage reasons, while the private sector might be targeted for economic reasons. Terrorist groups might also choose to undertake cyber attacks. There are various motives. In the case of nation-states, the motives will be different from those of "hacktivists", as they are known, who are often seeking no other gain than the prestige of having successfully pirated a government system.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*Français*]

Le sénateur Dagenais : Merci à nos invités. Ma question concerne la sécurité des infrastructures essentielles. Pourriez-vous nous faire une comparaison par rapport à ce qui se fait aux États-Unis ou en Grande-Bretagne, si vous en avez une idée, en ce qui a trait à la sécurité des infrastructures essentielles?

Mme Beauregard : Comme je le mentionnais dans mes remarques, nous travaillons de très près avec nos alliés les plus proches, comme on les appelle en anglais, les « Five Eyes ». Nous travaillons aussi étroitement avec les Américains. Lorsqu'on parle d'infrastructures essentielles, il n'y a pas nécessairement de frontières, surtout compte tenu de la façon dont les choses fonctionnent d'est en ouest. Je demanderai à Patrick de poursuivre.

[*Traduction*]

Patrick Boucher, directeur général par intérim, Direction des infrastructures essentielles et de la coordination stratégique, Sécurité publique Canada : Je vous remercie de la question. Comme l'a mentionné Monik, nous travaillons en collaboration très étroite non seulement avec nos collègues américains au sud, mais également avec la collectivité des cinq. En ce qui concerne les infrastructures essentielles en particulier, nous avons le « Groupe Critical 5 ». Il s'agit d'une tribune où la collectivité des cinq se réunit régulièrement afin de discuter de questions très précises sur les infrastructures essentielles et leur résilience.

Comme l'a dit Monik, nous travaillons en collaboration très étroite avec nos partenaires sur diverses initiatives. Le PERR en est un bon exemple. Il s'agit d'une méthodologie américaine, et nous avons travaillé en très étroite collaboration avec nos partenaires américains afin de l'appliquer ici au Canada et de mener des évaluations frontalières conjuguées dans le cadre du PERR.

[*Français*]

Le sénateur Dagenais : On parle aussi des cyberattaques dont nous pourrions être victimes. Pourriez-vous nous donner une idée du profil de ceux qui commettent ces cyberattaques et des pays desquels elles peuvent provenir?

Mme Beauregard : Les cyberattaques peuvent venir d'un grand nombre d'acteurs. Il peut s'agir d'États-nations qui cherchent tout simplement à continuer des activités d'espionnage ou qui recherchent un avantage économique quelconque. Le gouvernement peut être ciblé pour des questions d'espionnage, le secteur privé peut l'être pour des questions économiques. Des groupes terroristes peuvent choisir de mener des cyberattaques également. Les motifs varient. Si on parle d'États-nations, les motifs seront différents des *hacktivists*, comme on dit, qui n'ont parfois aucun gain recherché sinon le prestige d'avoir réussi à pirater un système du gouvernement.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

There are many actors. There are also many motives. Unfortunately, we must focus on the impact. When it comes to our infrastructure resilience, it is the result that is the most important aspect for us, and not necessarily the origin of the threat. The result will be the same.

[*English*]

Senator Mitchell: This is a huge area of responsibility and coordination. Are you the person who wakes up every morning with that responsibility or can't sleep with it?

Ms. Beauregard: For the last six weeks, sir, yes. I do report. I have a deputy minister and a minister for Public Safety, but it's a whole-of-government concern, of course. We look at cybersecurity. We look at the security of critical infrastructure. As I indicated in my opening remarks, we have sector working groups, and, depending on what that sector is, we have a different government department that will be the chair of that working group. As I indicated, for example, Health will chair the working group that is looking at critical infrastructure in the domain of health.

At the end of the day, public safety is as much about coordination. It's a whole-of-government approach. We have to work with all of our government partners, federal or provincial or territorial.

Senator Mitchell: One of the areas that is of particular concern — and you emphasized it in your presentation — is the private sector. The bulk of our vulnerable infrastructure, cyber-wise, might well be in the private sector. I think you made that point.

When you do the RRAP feature site assessment and you find something lacking and the private sector entity doesn't seem to take it as intensely as you do, what recourse do you have?

Ms. Beauregard: It's a collaboration. When we do the RRAPs, it's either at our suggestion or their request. It's not "you must implement the recommendations." It's a collaborative effort.

Do you want to speak to the RRAP specifically?

Mr. Boucher: Sure.

Senator Mitchell: What if they must? What if it's that critical?

Mr. Boucher: As Monik indicated, this is very much a collaborative approach. So we go in there. It's boots on the ground where we do our assessment. We're in there for about three to four days with various experts that we have. We conduct the assessment in close collaboration with the owner and operator. We often also have a representative from the provincial government who participates in those assessments. At the end of the day we give them a dashboard of sorts that identifies possible vulnerabilities and also how that stacks up to other critical infrastructure that's comparable to their infrastructure so that they could gauge how they stack up compared to other entities as well.

Les acteurs sont nombreux. Les motifs le sont également. Malheureusement, on doit se concentrer sur l'impact. C'est le résultat qui est le plus important pour nous en ce qui concerne la résilience de nos infrastructures, et non pas nécessairement d'où provient la menace. Le résultat sera le même.

[*Traduction*]

Le sénateur Mitchell : C'est un énorme secteur de responsabilité et de coordination. Êtes-vous la personne qui se lève chaque matin avec cette responsabilité ou alors qui passe des nuits blanches à cause d'elle?

Mme Beauregard : Depuis six semaines, monsieur, oui. Je rends des comptes au sous-ministre et au ministre de la Sécurité publique, mais, bien sûr, c'est une préoccupation pour l'ensemble du gouvernement. Nous étudions la cybersécurité et la sécurité des infrastructures essentielles. Comme je l'ai dit dans ma déclaration préliminaire, nous avons des groupes de travail sectoriels, et, en fonction du secteur, un ministère différent présidera le groupe de travail. Par exemple, comme je l'ai mentionné, Santé Canada présidera le groupe de travail qui se penche sur les infrastructures essentielles liées au domaine de la santé.

Au bout du compte, la sécurité publique est tout autant une affaire de coordination : c'est une approche pangouvernementale. Il faut travailler avec tous nos partenaires au sein des gouvernements provinciaux, territoriaux et fédéral.

Le sénateur Mitchell : Vous l'avez souligné dans votre exposé : le secteur privé est particulièrement préoccupant. Le gros de nos infrastructures cybernétiques pourrait bien appartenir au secteur privé. Je crois que vous avez dit cela.

Quel recours avez-vous si vous découvrez une lacune dans le cadre d'une évaluation de site en vertu du PERR et que l'entité privée ne semble pas y accorder autant d'importance que vous?

Mme Beauregard : Les évaluations en vertu du PERR sont collaboratives. Nous les suggérons, ou alors elles nous sont demandées. Nous ne forçons pas la mise en œuvre de nos recommandations. C'est un travail de collaboration.

Voulez-vous aborder le sujet du PERR en particulier?

M. Boucher : D'accord.

Le sénateur Mitchell : Et si c'est obligatoire? Et si c'est crucial?

M. Boucher : Comme l'a dit Monik, il s'agit d'une approche très axée sur la collaboration. Nous nous rendons sur place et menons notre évaluation sur le terrain pendant trois ou quatre jours avec les divers experts à notre disposition. L'évaluation est effectuée en collaboration étroite avec le propriétaire et l'exploitant. Bien souvent, un représentant du gouvernement provincial participe aussi aux évaluations. Quand tout est terminé, on remet aux intéressés une sorte de tableau de bord qui leur indique les vulnérabilités potentielles ainsi que la mesure dans laquelle leur infrastructure essentielle se compare à d'autres du même genre, ce qui leur permet de voir comment leur infrastructure se classe par rapport aux autres entités.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

At the end of the day, these are recommendations. The input that we've gathered from them, through the 70-odd assessments we've conducted over the last few years, is that it's very positive. The owners and operators appreciate the recommendations and are utilizing the information accordingly.

The Chair: Do you want to follow up on that?

Senator Mitchell: Yes.

I think you may have covered this earlier, but I'm not sure. I think you said you're kind of agnostic about what the source of the hack might be, but clearly there is a lot of suggestion, if not evidence, that we are vulnerable to cyber-espionage by China. Is that something you focus on in a certain way?

Ms. Beauregard: The work that we do in cyber is mostly done in the CCIRC, the Canadian Cyber Incident Response Centre. The work that we do is really working with the private sector, the provinces and the territories, sharing with them information about the kinds of hacks that we've received. Again, it's not that we're totally agnostic as to what the origin is, but what we're trying to understand is the actual hack itself. Why were we vulnerable to that hack, to that incident, and are there trends that we need to be conscious of? Can we share that information with the private sector so they can best protect themselves?

Other parts of the government are not so agnostic as to where the threat comes from, but our part is really to be in a position to understand the incident, how we are vulnerable, how we can fix that, how we can build our resilience and share that beyond the government.

Senator Day: Thank you all for being here. I appreciate your presentation, Ms. Beauregard.

I recall this committee visiting several first responders in the past, and I believe it was during the time that there was in existence this wonderful organization under the acronym OCIPEP, the Office of Critical Infrastructure Protection and Emergency Preparedness. That has disappeared in name, but is it now one of the divisions within Public Safety Canada?

Ms. Beauregard: It has morphed into Public Safety. The way that we're organized now at Public Safety, we have five major branches. So National Security and Cybersecurity sits with me and my DGs here. Emergency Preparedness would be another assistant deputy minister. It's another full branch, where they have search and rescue and they have the Government Operations Centre. That's another full branch in Public Safety. Then you have policing, et cetera.

Au bout du compte, nous formulons des recommandations. La rétroaction que nous avons obtenue, au fil des quelque 70 évaluations que nous avons réalisées au cours des quelques dernières années, s'est révélée très favorable. Les propriétaires et les exploitants apprécient nos recommandations et utilisent les renseignements que nous leur donnons en conséquence.

Le président : Voulez-vous ajouter quelque chose?

Le sénateur Mitchell : Oui.

Je crois que vous avez déjà abordé ce sujet plus tôt, mais je n'en suis pas sûr. Je crois que vous avez dit que vous ne pouviez pas vraiment cerner les sources de piratage. Toutefois, il est clair qu'il y a un grand nombre d'indices, sinon de preuves, que nous prêtons le flanc au cyberespionnage chinois. Avez-vous déployé des efforts à ce sujet?

Mme Beauregard : Notre travail à ce chapitre est effectué principalement par le Centre canadien de réponse aux incidents cybernétiques, ou CCRIC. Nos activités touchent surtout la collaboration et l'échange de renseignements avec le secteur privé, les provinces et les territoires à propos des différentes tentatives de piratage dont nous avons été victimes. Je le répète : nous ne croyons pas qu'il est impossible de déterminer l'origine d'une tentative de piratage, mais nos activités sont axées sur la compréhension de l'acte de pirate lui-même. Pourquoi étions-nous vulnérables à cet acte de piratage ou à cet incident? Devrions-nous prendre conscience de certaines tendances? Pouvons-nous communiquer l'information au secteur privé pour l'aider à mieux se protéger?

D'autres secteurs du gouvernement en savent davantage sur les origines des menaces, mais notre travail consiste surtout à comprendre l'incident, à cerner les vulnérabilités et à y remédier, à trouver des moyens de renforcer notre résilience et à communiquer ce que nous avons appris à l'extérieur du gouvernement.

Le sénateur Day : Merci à tous d'avoir comparu aujourd'hui. Votre exposé était intéressant, madame Beauregard.

Je me rappelle que le comité a rendu visite à plusieurs organisations de premiers répondants par le passé. Je crois qu'à cette époque, il existait une merveilleuse organisation connue sous le sigle BPIEPC, soit le Bureau de la protection des infrastructures essentielles et de la protection civile. L'organisation n'existe plus sous cette forme, mais a-t-elle été intégrée à Sécurité publique Canada?

Mme Beauregard : Cette organisation s'est transformée pour devenir Sécurité publique. Sous sa forme actuelle, Sécurité publique compte cinq secteurs principaux. Mes directeurs généraux ici présents et moi-même faisons partie du Secteur de la sécurité et de la cybersécurité nationale. Un autre sous-ministre adjoint s'occupe de la Protection civile, un autre secteur à part entière, qui est responsable des activités de recherche et sauvetage et du Centre des opérations du gouvernement. C'est un tout autre secteur de Sécurité publique. Il y a aussi le secteur qui s'occupe du maintien de l'ordre, et cetera.

Senator Day: So I can get all that information off the Internet, off the website.

Ms. Beauregard: Yes, the structure of Public Safety and who does what, absolutely.

Senator Day: My recollection is that in the past there was a jurisdictional issue. The provinces had major jurisdiction in this area, but the federal government was trying to show leadership. In order to do that, they had a program with a lot of money in it that encouraged cooperation.

Are there still significant funds available through the federal government for first responders across Canada for emergency preparedness purposes?

Ms. Beauregard: I would have to get back to you on that specific question because it does deal with another branch.

Senator Day: I would be interested in knowing how it's developing along the way.

The final question I have relates to another area that has come within your umbrella, and that is Shared Services Canada. We saw the creation of that, and we follow the media attention on Shared Services. Is that coordinated in some way with your activity? It is a separate agency?

Ms. Beauregard: Yes.

Senator Day: What role do you have to play in relation to Shared Services Canada, which provides, across-government, federal government assistance and coordination in relation to computers and all the information technology that exists in each of the departments?

Ms. Beauregard: Yes, you're absolutely right that it is a separate department. As a separate department, it's a partner with which we have to work on a daily basis on all of these issues. For example, as we launch into a cyber review, Shared Services will be one of the major partners that we consult and that we work with in conducting the cyber review.

Senator Day: From your point of view, does it make it easier to protect against cyberattacks to have a Shared Services Canada situation than each department looking after itself?

Ms. Beauregard: I don't know that it's any easier or any more complicated. I think we have a lot of departments and a wide array of systems throughout the government. CBSA has many of their own systems; so does DND. That's why we have to all work collectively.

I don't know if you want to weigh in on Shared Services, but I don't think it makes it any more or less complicated.

Le sénateur Day : Alors, je peux trouver tous ces renseignements sur votre site web.

Mme Beauregard : Oui, vous pouvez y trouver la structure de Sécurité publique ainsi que les responsabilités de chaque secteur, tout à fait.

Le sénateur Day : Selon mes souvenirs, il y a eu dans le passé un problème relativement à la compétence. Les provinces jouissaient d'un pouvoir important à ce sujet, mais le gouvernement fédéral essayait de faire preuve de leadership. À cette fin, il a consenti un important budget à un programme visant à encourager la coopération.

Le gouvernement fédéral offre-t-il toujours un financement important aux premiers répondants aux quatre coins du Canada aux fins de la protection civile?

Mme Beauregard : Je vais devoir vous répondre plus tard, parce que cette question concerne un autre secteur.

Le sénateur Day : J'aimerais savoir comment les choses évoluent.

Ma dernière question porte sur une autre organisation qui s'est greffée à la vôtre, à savoir Services partagés Canada. Nous avons assisté à sa création, et nous suivons l'attention médiatique suscitée par Services partagés. Ses activités sont-elles coordonnées d'une façon quelconque avec les vôtres? S'agit-il d'un organisme distinct?

Mme Beauregard : Oui.

Le sénateur Day : Services partagés Canada fournit de l'aide et une coordination fédérale à l'échelle du gouvernement relativement aux ordinateurs et à la technologie de l'information au sein de chaque ministère. Quel est votre rôle dans tout cela?

Mme Beauregard : Oui, vous avez tout à fait raison, il s'agit d'un ministère distinct. C'est un partenaire avec lequel nous devons travailler quotidiennement pour nous attaquer à tous ces enjeux. Par exemple, lorsque nous commençons un examen en matière de cybersécurité, Services partagés est l'un des principaux partenaires que nous consultons et avec qui nous travaillons pour mener l'examen.

Le sénateur Day : À votre avis, est-il plus simple de se protéger des cyberattaques grâce à Services partagés Canada, ou serait-il préférable que chaque ministère s'occupe de lui-même?

Mme Beauregard : Je ne sais pas si c'est plus simple ou plus compliqué. Je crois qu'il y a beaucoup de ministères et un large éventail de systèmes dans l'ensemble du gouvernement. L'ASFC a de nombreux systèmes, et le MDN aussi. C'est pourquoi nous devons tous travailler ensemble.

Je ne sais pas si vous voulez ajouter quelque chose au sujet de Services partagés... Mais je ne crois pas que cette organisation rend les choses plus simples ou plus compliquées.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

[*Translation*]

Senator Day: Senator Merchant, do you wish to make any comments?

[*English*]

Colleen Merchant, Director General, National Cyber Security Directorate, Public Safety Canada: From a security perspective, they've put some interesting things in place. In particular, they've reduced the number of connections to the Internet, which means there are fewer places that need to be protected, which is easier. Also, they've instituted some security standards across government, so you don't have a weaker link, in many cases.

I think that while Monik said it's not necessarily any more or less complicated, some benefits have accrued for cybersecurity.

Senator Day: Has that been implemented as a result of your encouragement and Public Safety Canada's encouragement, or are they taking the lead on that?

Ms. Merchant: Part of it was due to the cybersecurity strategy that was released five years ago. The first pillar of that is to protect government systems. That was one of the resulting activities that were undertaken.

Senator Beyak: I share Senator Mitchell's concerns about the massiveness of the tasks that you're undertaking.

I was more concerned with the mandate letter to the minister. It's filled with tasking even more collaboration. What has been your observation of the timeline that you've been given for that and the minister has been given? Is it going to work? Will it need to be extended? Can you bring all the partners in adequately in the timeline you've been given?

Ms. Beauregard: Can I just ask for clarification? You're only speaking about the cyber review, not the entire mandate letter?

Senator Beyak: Actually, the entire mandate letter was a concern to me. It's massive. I'm not sure where your part fits into it.

Ms. Beauregard: Thankfully, I don't have all the reviews in the mandate letter to carry out. There are other ADMs at Public Safety, and we share the burden of carrying out these reviews.

I think at this point we're all looking at the scope of the reviews and thinking about how to carry them out, putting the framework around it and thinking about how wide or narrow we want to go with these reviews. We're still in the preliminary stages. I think we're following some short timelines in terms of getting to cabinet and all that, but otherwise we're still scoping it out.

[*Français*]

Le sénateur Day : Madame Merchant, souhaitez-vous ajouter des commentaires?

[*Traduction*]

Colleen Merchant, directrice générale, Direction générale de la cybersécurité nationale, Sécurité publique Canada : Cette organisation a pris des mesures intéressantes du point de vue de la sécurité, en particulier la réduction du nombre de connexions à Internet, ce qui a réduit le nombre d'endroits à protéger et ainsi facilité les activités de protection. Elle a également instauré des normes de sécurité à l'échelle du gouvernement afin de renforcer, dans un grand nombre de cas, des maillons faibles.

Même si Monik a dit que les choses ne sont pas nécessairement plus ou moins compliquées, il y a tout de même des avantages relativement à la cybersécurité.

Le sénateur Day : Est-ce que ces mesures sont le fruit de votre encouragement et de celui de Sécurité publique Canada, ou est-ce que Services partagés Canada a pris l'initiative?

Mme Merchant : C'est attribuable en partie à la stratégie de cybersécurité d'il y a cinq ans, dont le premier pilier était la protection des systèmes gouvernementaux. C'était l'une des activités entreprises à cette fin.

La sénatrice Beyak : J'ai les mêmes préoccupations que le sénateur Mitchell à propos de l'ampleur des tâches que vous avez entreprises.

Je suis davantage préoccupée par la lettre de mandat adressée au ministre. Elle est remplie de tâches qui supposent encore plus de collaboration. Qu'avez-vous observé au chapitre de l'échéancier qui vous a été donné, à vous et au ministre? Pouvez-vous le respecter? Devra-t-il être assoupli? Pourrez-vous réunir tous les partenaires adéquatement dans les délais qui vous ont été donnés?

Mme Beauregard : Puis-je vous demander de clarifier votre question? Vous parlez uniquement des examens en matière de cybersécurité, et pas de la lettre de mandat en entier?

La sénatrice Beyak : En fait, j'étais préoccupée par la lettre de mandat au complet. Il s'agit d'un effort énorme, et je ne suis pas certaine de votre rôle dans tout ça.

Mme Beauregard : Heureusement, je n'ai pas à m'occuper de tous les examens mentionnés dans la lettre de mandat. Il y a d'autres SMA à Sécurité publique, et nous nous partageons le fardeau à l'égard de ces examens.

Actuellement, je crois que nous sommes tous en train d'étudier la portée des examens et la façon dont nous allons les mener. Nous établissons le cadre et nous nous demandons à quel point la portée des examens doit être large ou restreinte. Nous en sommes encore aux étapes préliminaires. Je crois que nous suivons un échéancier serré pour ce qui est de présenter cela au Cabinet, mais pour le reste, nous en sommes encore à déterminer la portée des examens.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT. RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Senator Beyak: It is the Minister of Public Safety, so I know you're just the cyber branch. But do you think I should read it into the record so that people watching these telecasts are aware?

Ms. Beauregard: You mean the portion of the mandate? Absolutely.

Senator Beyak: The whole mandate.

Senator Day: You're going to read the mandate letter?

Senator Beyak: No. There's quite a bit, actually. The Minister of Public Safety and Emergency Preparedness is expected to:

> Lead a review of existing measures to protect Canadians and our critical infrastructure from cyber-threats, in collaboration with the Minister of National Defence, the Minister of Innovation, Science and Economic Development, the Minister of Infrastructure and Communities, the Minister of Public Services and Procurement, and the President of the Treasury Board.

I'm just wondering, as I said, about the timeline and how you're going to coordinate all that.

Ms. Beauregard: As I mentioned, we are working with all of our partners that are mentioned in the mandate letter to work together to scope and then to make proposals to the minister.

Senator Beyak: All the very best to you.

Ms. Beauregard: Thank you.

[*Translation*]

Senator Carignan: In your definition of the term "critical infrastructure," you refer to that which is essential to health, safety, security and well-being. In the United States, there seems to be a broader definition, key assets, which include potential targets. I will say it in English —

[*English*]

— "potential targets whose destruction may not endanger vital systems but could create a local disaster or profoundly affect national morale."

[*Translation*]

Examples are given, such as sports stadiums and shopping centres. In France, the terrorists attacked a concert hall and a sports stadium. In Africa, shopping centres have been the target of attacks. Do you have a broader definition of critical infrastructure, and do you also take into account elements of these key assets in the context of your security concerns?

La sénatrice Beyak : Je sais que vous représentez seulement le Secteur de la cybersécurité du ministère de la Sécurité publique, mais selon vous, devrais-je lire la lettre pour qu'elle figure au compte rendu et que les gens qui nous regardent puissent en prendre connaissance?

Mme Beauregard : Vous voulez dire la partie pertinente du mandat? Absolument.

La sénatrice Beyak : Le mandat au complet.

Le sénateur Day : Vous allez lire la lettre de mandat?

La sénatrice Beyak : Non, elle est très longue, en fait. Le ministre de la Sécurité publique et de la Protection civile doit :

> Diriger un examen des mesures en place pour assurer la protection des Canadiens et des infrastructures critiques du Canada contre les cybermenaces, en collaboration avec le ministre de la Défense nationale, le ministre de l'Innovation, des Sciences et du Développement économique, le ministre de l'Infrastructure et des Collectivités, la ministre des Services publics et de l'Approvisionnement et le président du Conseil du Trésor.

Comme je l'ai dit, je m'interrogeais à propos de l'échéancier et de la façon dont vous allez coordonner tout cela.

Mme Beauregard : Comme je l'ai dit, nous travaillons avec l'ensemble de nos partenaires mentionnés dans la lettre de mandat pour établir la portée des activités afin de formuler des propositions à l'intention du ministre.

La sénatrice Beyak : Je vous souhaite la meilleure des chances.

Mme Beauregard : Merci.

[*Français*]

Le sénateur Carignan : Dans votre définition de l'expression « infrastructures essentielles », vous faites référence à ce qui est essentiel ou fondamental à la santé, à la sécurité et au bien-être. Aux États-Unis, il semble y avoir une définition plus large, soit les actifs clés, qui comprennent les cibles potentielles. Je vais le dire en anglais...

[*Traduction*]

... « les cibles potentielles dont la destruction ne met pas nécessairement en danger les systèmes essentiels, mais peut créer une catastrophe locale ou avoir une grande incidence sur le moral de la nation. »

[*Français*]

On en donne des exemples, notamment les stades sportifs et les centres commerciaux. Les terroristes en France ont attaqué un centre de spectacles et un centre sportif. En Afrique, ce sont des centres commerciaux qui ont fait l'objet d'attaques. Avez-vous une définition plus large des infrastructures essentielles et tenez-vous compte également des éléments de ces actifs clés dans le cadre de vos préoccupations en matière de sécurité?

Ms. Beauregard: This might be a long answer. We have set out 10 sectors of critical infrastructure according to a very specific definition. If one of those sectors is hit, there could be negative repercussions on the entire country.

When we examine terrorist threats, we look at them through the lens of critical infrastructure sectors, but we also look at terrorist threats through other lenses. We study foreign trends, particularly in the transportation sector, which directly affects these 10 areas. We also know that the tourism sector is a potential target for terrorist attacks.

We have witnessed attacks on vulnerable targets in foreign countries: stadiums, bars and hotels. We look at these targets more from the perspective of analysing terrorist threats that have an impact on the entire country, for example if there is a sector that is hit by a cyber incident or by a natural disaster.

So we use several different lenses to evaluate threats.

Senator Carignan: How do you look at threats from the point of view of prevention? In your brief you often refer to the provinces and territories. You did not often refer to municipalities. You mentioned them a few times while discussing cyber attacks. I did not hear the word "municipality" very often. You collaborate with the municipalities. They have local infrastructures and they must be particularly concerned about security and prevention.

When you speak with municipalities to determine which targets are vulnerable, are measures taken to support, educate, and equip them? Do you not think this would be important, given that all municipalities are not at the same level?

Ms. Beauregard: I would say that the work is essentially done when a threat appears and we have undertaken a fairly serious assessment of a possible threat. We primarily work with law enforcement, such as the RCMP or municipal police forces, because we can share certain sensitive information with them.

As for terrorist threats, we work closely with police forces, and it is they who decide in due course what to do with the information.

Senator Carignan: So we are in reaction mode, and not in prevention mode.

Ms. Beauregard: No, I am talking more about preparation. If indeed there are signs of a potential attack, we essentially work with law enforcement, whether that be to prepare or to respond.

Mme Beauregard : Cela pourrait être une longue réponse. Nous avons énoncé 10 secteurs d'infrastructures essentielles en fonction d'une définition très particulière. Si l'un de ces secteurs est touché, cela peut entraîner des répercussions néfastes sur tout le pays.

Lorsqu'on examine les menaces terroristes, c'est au moyen de la lentille des secteurs d'infrastructures essentielles, mais on examine aussi les menaces terroristes à travers d'autres lentilles. On étudie les tendances à l'étranger, notamment en ce qui concerne les transports, ce qui entre directement dans ces 10 domaines. On constate également que le domaine du tourisme est une cible potentielle d'attentats terroristes.

On en a été témoin à l'étranger lors d'attaques dirigées vers les stades, les bars et les hôtels, qui sont des cibles vulnérables. On examine ces cibles davantage dans la perspective de l'analyse des menaces terroristes que des répercussions sur l'ensemble du pays, à savoir s'il y a un secteur qui est touché soit par un cyberincident ou par une catastrophe naturelle.

Donc, nous utilisons plusieurs lentilles pour évaluer les menaces.

Le sénateur Carignan : Comment abordez-vous les menaces pour faire de la prévention? Dans votre exposé, vous faites souvent allusion aux provinces et aux territoires. Vous avez peu parlé des municipalités. Vous les avez mentionnées à quelques reprises lorsqu'il était question des cyberattaques. J'ai très peu entendu le mot « municipalité ». Vous travaillez en collaboration avec les municipalités. Elles ont des infrastructures locales qui doivent les préoccuper tout particulièrement du point de vue de la sécurité et de la prévention.

Dans le cadre de ces échanges avec les municipalités afin d'établir des cibles vulnérables, des mesures sont-elles prises pour les soutenir, les sensibiliser et les outiller? Ne croyez-vous pas que ce serait important, étant donné que les municipalités ne sont pas toutes au même niveau?

Mme Beauregard : Je vous dirais que le travail se fait essentiellement lorsqu'une menace se dessine et que nous avons effectué une évaluation assez robuste d'une éventuelle menace. Le travail se fait essentiellement avec les forces de l'ordre, donc avec la GRC ou les forces policières municipales, parce que nous pouvons partager avec eux certains renseignements de nature plus sensible.

En ce qui concerne les menaces terroristes, le travail est mené de concert avec les forces policières et, à ce moment-là, celles-ci prennent les décisions relativement à l'information reçue.

Le sénateur Carignan : Donc, nous sommes en mode réaction et non pas en mode prévention.

Mme Beauregard : Non, je parle davantage de préparation. Si, effectivement, il y a des signes d'une attaque potentielle, que ce soit en préparation ou en réponse, nous travaillons essentiellement avec les forces de l'ordre.

Senator Carignan: That is what I said, in reaction to signs. However, if there are not any, we do not have a plan, training, or direct communication with municipalities to inform them of the problems they might face and to give them the possibility to put preventive measures in place.

Ms. Beauregard: Work on the ground is largely undertaken with the sectors themselves through the Regional Resilience Assessment Program, that we discussed earlier, which includes a municipal lens for assessing a terrorist threat.

[*English*]

Mr. Boucher: I will take this opportunity to emphasize the interconnected nature of securing the critical infrastructure. We've touched upon a few of the different pillars. First of all, there are the owners and operators, and their crucial partners. They bear the primary responsibility to protect their assets.

Municipalities are also partners in this, and they have a role to play. We talked about first responders. That's the role they play in this, with the support of provinces and territories, if need be.

Provinces and territories are other very important partners and are responsible for leading critical infrastructure protection activities within their jurisdiction.

Then there is the federal government and the role that we play in terms of coordinating the overall national approach. If events do cascade into events of national significance, that's where we kick in.

But as Monik indicated, when it's localized events, you have municipalities working with the owners and operators to subdue the threat or to react.

Ms. Beauregard: We work with the provinces, and the provinces would then reach out to the municipalities. Through the GOC that I mentioned earlier, the Government Operations Centre, a lot of information is pushed out to the provinces, territories and municipalities.

The Chair: I want to go to an area that is becoming more and more debated publicly; namely, the question of the electromagnetic pulse. That is primarily in the United States, but now it's becoming a question for Canada as well. I understand our energy and cyberspace could be threatened by this. Could you give us your observation on how critical this particular issue is and what is being done in respect to addressing it?

Ms. Beauregard: In terms of our observations, it's a very serious issue that we're looking at closely, and we are looking at what's happening in other parts of the world. We're looking at how the Americans are reacting to this.

Le sénateur Carignan : C'est ce que je disais, en réaction à des signaux. Cependant, s'il n'y en a pas, nous n'avons pas de plan, de formation ou d'échange directement avec les municipalités pour les initier aux problèmes qu'elles pourraient rencontrer et pour leur donner la possibilité de prendre des mesures de prévention.

Mme Beauregard : Le travail sur le terrain se fait davantage avec les secteurs eux-mêmes dans le cadre du Programme d'évaluation de la résilience régionale, dont nous parlions plus tôt, qui prévoit une lentille axée sur l'évaluation de la menace terroriste par rapport aux municipalités.

[*Traduction*]

M. Boucher : Je vais saisir profiter de l'occasion de souligner la nature interreliée de la sécurité des infrastructures essentielles. Nous avons parlé de quelques-uns des différents piliers. Premièrement, il y a les propriétaires et les exploitants ainsi que leurs partenaires cruciaux. Ils sont les principaux responsables de la protection de leurs biens.

Les municipalités sont également des partenaires, et elles ont un rôle à jouer. Nous avons parlé des premiers répondants : c'est le rôle qu'elles jouent, avec le soutien des provinces et des territoires, au besoin.

Les provinces et les territoires sont également des partenaires très importants. Ils sont responsables de diriger les activités de protection des infrastructures essentielles qui relèvent de leur compétence.

Ensuite vient le gouvernement fédéral : nous coordonnons l'approche nationale dans son ensemble. Nous entrons en jeu quand des événements s'aggravent et prennent une ampleur nationale.

Mais comme Monik l'a mentionné, les municipalités vont travailler avec les propriétaires et les exploitants afin de réagir aux menaces et de les régler quand il s'agit d'événements locaux.

Mme Beauregard : Nous travaillons avec les provinces, et celles-ci vont ensuite communiquer avec les municipalités. Grâce au COG que j'ai mentionné plus tôt — le Centre des opérations du gouvernement — les provinces, les territoires et les municipalités produisent beaucoup de renseignements.

Le président : Je tiens à aborder un sujet qui est de plus en plus débattu sur la place publique, soit les impulsions électromagnétiques. La question concernait principalement les États-Unis, mais cela devient de plus en plus pertinent au Canada. Je crois comprendre que c'est une menace pour nos infrastructures énergétiques et cybernétiques. Pouvez-vous nous parler de l'importance de cette question ainsi que des mesures qui ont été prises pour nous protéger de cette menace?

Mme Beauregard : C'est un enjeu très grave que nous suivons de près. Nous observons ce qui se passe à ailleurs dans le monde, et nous suivons la réaction des Américains à ce chapitre.

In terms of how we're responding, however, it would be more of an NRCan lead on that rather than Public Safety. In that sense, we would invite you to direct your questions to our NRCan colleagues.

The Chair: But it is of grave concern, from what I understand you said; is that correct?

Mr. Boucher: We would refer to it as being part of high-impact but low-frequency or probability-type events — Black Swan events, as some people call them. They're rare but they could be devastating, so it does require special attention.

The critical infrastructure community as a whole has recognized the need to better address these issues, and NRCan is leading the charge from a federal perspective on that front.

There are things that we've done at Public Safety to help support owners and operators to better deal with those types of events. For example, we've put together guidance documents in working with partners, owners and operators, NRCan, the provinces and other important partners to talk about readiness for such events.

We've conducted that in three different areas for these high-impact, low-probability events. We've looked at space weather, or EMPs, as you referred to, senator; we've looked at catastrophic earthquakes; and also major cyberattacks. So there is work that Public Safety has done in terms of providing guidance and guideline documents to those owners and operators in order to better bolster their resistance.

The Chair: Obviously, it's an area where we will have to follow up.

Let us turn to one other issue here, the question of the foreign companies and the investment in critical infrastructure. For example, in the U.S. and the United Kingdom, parliamentary committees raised serious concerns about a foreign company. In this case, it was a Chinese telecommunications company that offered to sell equipment for use in critical infrastructure. There was a similar situation in Australia, where they blocked a commercial transaction for national security reasons.

Does Canada have a mechanism to stop a foreign company that is a security risk from participating in our critical infrastructure, do we have the power to use it, and who identifies that critical infrastructure for such an investment?

Ms. Beauregard: Yes, we do have tools in place. We have the Investment Canada Act that gives us the tools to look at investments in Canada and to conduct assessments in terms of the security of investments.

En ce qui concerne les mesures prises, toutefois, cela relève davantage de RNCan que de Sécurité publique. Je vous inviterais donc à adresser vos questions directement à nos collègues de RNCan.

Le président : Mais d'après ce que vous avez dit, il s'agit d'une question très préoccupante. C'est exact?

M. Boucher : Je dirais qu'il s'agit d'un événement aux impacts élevés, mais dont la fréquence ou la probabilité est faible; c'est ce que certaines personnes appellent un événement de type « cygne noir ». Ce genre d'événements est rare, mais pourrait s'avérer catastrophique, alors il faut y porter une attention particulière.

L'ensemble de la collectivité des infrastructures essentielles a reconnu le besoin de mieux contrer ces menaces, et RNCan est le fer de lance du gouvernement à ce chapitre.

Nous avons pris certaines mesures à Sécurité publique pour aider à soutenir les propriétaires et les exploitants pour qu'ils composent mieux avec ce genre d'événements. Par exemple, nous avons préparé des documents d'orientation qui touchent le travail avec les partenaires, les propriétaires et les exploitants, RNCan, les provinces et d'autres partenaires importants afin d'aborder la préparation face à ce genre d'événements.

Nous avons travaillé sur les événements à impacts élevés et à probabilité faible dans trois régions différentes. Nous nous sommes penchés sur la météorologie de l'espace — ou les impulsions électromagnétiques, comme vous l'avez dit, monsieur le sénateur — et sur les séismes catastrophiques ainsi que sur les cyberattaques importantes. Donc, Sécurité publique a déployé des efforts pour fournir des directives et des documents d'orientation afin d'aider les propriétaires et les exploitants à améliorer leur résistance.

Le président : Évidemment, nous allons devoir faire un suivi sur ce sujet.

Abordons à présent la question des entreprises étrangères et de l'investissement dans les infrastructures essentielles. Par exemple, des comités parlementaires aux États-Unis et au Royaume-Uni ont soulevé de graves préoccupations à propos d'une entreprise étrangère. Il s'agissait d'une entreprise de télécommunications chinoise qui avait offert de vendre de l'équipement pour utilisation dans une infrastructure essentielle. Une situation similaire s'est produite en Australie, où la transaction commerciale avait été bloquée pour des raisons de sécurité nationale.

Le Canada a-t-il en place un mécanisme visant à empêcher une entreprise étrangère qui pose un risque à la sécurité de participer dans nos infrastructures essentielles? Avons-nous le pouvoir de l'utiliser? Et qui cerne les infrastructures essentielles liées à ce genre d'investissement?

Mme Beauregard : Oui, il y a des outils en place. La Loi sur Investissement Canada nous habilite à examiner les investissements faits au Canada et à mener des évaluations sur leur sécurité.

Suki can delve into the details, if you wish.

Suki Wong, Director General, National Security Operations Directorate, Public Safety Canada: And we'd be happy to follow up, senator, with more detailed information for you.

In Canada, there is, under the Investment Canada Act, a national review process that allows our minister to provide counsel to the Minister of Innovation, Science and Economic Development in terms of a national security review process and whether the Public Safety minister should play an active role in terms of looking at the foreign investment's implications are for Canada. So, yes, there's a role for our minister.

Senator Ngo: To follow up on your question, can you tell us what is the percentage of Canada critical infrastructure currently owned and operated by private industry?

Ms. Beauregard: In Canada?

Senator Ngo: In Canada.

Ms. Beauregard: I believe it's about 90 per cent.

Senator Ngo: So what you asked is very relevant.

The Chair: Colleagues, I'd like to thank our witnesses for coming. We very much appreciate it. I know it's later in the day, so I'll excuse our witnesses.

If we could go in camera for just a few minutes, I'd appreciate it.

(The committee continued in camera.)

(The committee resumed.)

The Chair: I understand that Senator Mitchell has two motions with respect to the question of budgeting for the committee.

Senator Mitchell: Yes. Do you want me to do them one at a time?

The Chair: Yes, if you would.

Senator Mitchell: I move:

> That the following budget application as pertains to our order of reference dealing with the security threats facing Canada for $190,158 for the fiscal year ending March 31, 2017, be approved for submission to the Standing Committee on Internal Economy, Budgets and Administration following a final review by the Senate Administration that will be overseen by the Subcommittee on Agenda and Procedure.

The Chair: Can I put the question? Is everybody agreed?

Hon. Senators: Agreed.

Senator Mitchell: I further move:

Suki peut vous fournir plus de détails, si vous le souhaitez.

Suki Wong, directrice générale, Direction générale des opérations de la sécurité nationale, Sécurité publique Canada : Nous serions heureux de faire un suivi, monsieur le sénateur, et de vous fournir des renseignements plus détaillés.

Au Canada, sous le régime de la Loi sur Investissement Canada, il y a un processus d'examen national selon lequel notre ministre peut conseiller le ministre de l'Innovation, des Sciences et du Développement économique à propos d'un processus d'examen de la sécurité nationale et du rôle actif que le ministre de Sécurité publique devrait jouer par rapport à l'examen de l'incidence d'investissements étrangers au Canada. Alors, notre ministre joue bien un rôle à ce chapitre.

Le sénateur Ngo : Pour donner suite à votre question, pouvez-vous nous dire quel pourcentage des infrastructures essentielles du Canada appartiennent à des intérêts privés et sont exploitées par ceux-ci?

Mme Beauregard : Au Canada?

Le sénateur Ngo : Au Canada.

Mme Beauregard : Je dirais que c'est environ 90 p. 100.

Le sénateur Ngo : Ce que vous avez demandé est donc très pertinent.

Le président : Chers collègues, j'aimerais remercier nos témoins d'avoir comparu aujourd'hui. C'est très apprécié. Je sais qu'il se fait tard, alors je vais laisser nos témoins partir.

J'aimerais que la séance se poursuive à huis clos pendant quelques minutes.

(La séance se poursuit à huis clos.)

(La séance reprend.)

Le président : Je crois que le sénateur Mitchell veut présenter deux motions relatives au budget du comité.

Le sénateur Mitchell : Oui. Voulez-vous que je vous les présente une à la fois?

Le président : Oui, s'il vous plaît.

Le sénateur Mitchell : Je propose :

> Que la demande de budget suivante concernant notre ordre de renvoi relatif aux menaces à la sécurité qui pèsent sur le Canada, à savoir 190 158 $ pour l'exercice se terminant le 31 mars 2017, soit approuvée et présentée au Comité permanent de la régie interne, des budgets et de l'administration, après avoir été examinée une dernière fois par l'Administration du Sénat, sous la supervision du Sous-comité du programme et de la procédure.

Le président : Puis-je mettre la question aux voix?

Des voix : D'accord.

Le sénateur Mitchell : Je propose :

That the following budget application as pertains to our order of reference dealing with Canada's national security and defence policies, practices, circumstances and capabilities for $14,742 for the fiscal year ending March 31, 2017, be approved for submission to the Standing Committee on Internal Economy, Budgets and Administration following a final review by the Senate Administration that will be overseen by the Subcommittee on Agenda and Procedure.

The Chair: You have all heard the motion. Agreed?

Hon. Senators: Agreed.

Senator Ngo: In the budget, you put the year ending March 31, 2016. There is a typo.

The Chair: That will be corrected in both documents. Thank you, senator.

(The committee adjourned.)

OTTAWA, Monday, March 21, 2016

The Standing Senate Committee on National Security and Defence met this day at 1:01 p.m. to examine and report on Canada's national security and defence policies, practices, circumstances and capabilities; and to study security threats facing Canada.

Senator Daniel Lang (*Chair*) in the chair.

[*English*]

The Chair: Colleagues, welcome to the Standing Senate Committee on National Security and Defence for Monday, March 21, 2016. Before we begin, I would like to introduce the members around the table. My name is Dan Lang, senator for Yukon. On my immediate left is the clerk of the committee, Mark Palmer. I'd like to invite the senators to introduce themselves and state the region they represent, starting with Senator Wells.

Senator Wells: David Wells, Newfoundland and Labrador.

Senator Mitchell: Grant Mitchell, Alberta.

Senator Carignan: Claude Carignan, Quebec.

The Chair: Thank you, colleagues. Joining us for the first panel are representatives from the Canada Border Services Agency. Last June, this committee tabled a report on the Canada Border Services Agency entitled *Vigilance, Accountability and Security at Canada's Borders*. The report was unanimously adopted by the committee of the Senate and contained 10 specific recommendations which included, as follows: recommended oversight of Canada Border Services Agency; the establishment of a civilian review and complaints body; audio and video recording of interviews conducted by Border Services officers; and improved screening of visitors, immigrants and temporary visa holders, including students, temporary foreign workers, refugees

Que la demande de budget suivante concernant notre ordre de renvoi relatif aux menaces à la sécurité qui pèsent sur le Canada, à savoir 14 742 $ pour l'exercice se terminant le 31 mars 2017, soit approuvée et présentée au Comité permanent de la régie interne, des budgets et de l'administration, après avoir été examinée une dernière fois par l'Administration du Sénat, sous la supervision du Sous-comité du programme et de la procédure.

Le président : Puis-je mettre la question aux voix? Êtes-vous tous d'accord?

Des voix : D'accord.

Le sénateur Ngo : Dans le budget, vous avez indiqué que l'exercice se terminait le 31 mars 2016. Il y a une faute de frappe.

Le président : La faute sera corrigée dans les deux documents. Je vous remercie, monsieur le sénateur.

(La séance est levée.)

OTTAWA, le lundi 21 mars 2016

Le Comité sénatorial permanent de la sécurité nationale et de la défense se réunit aujourd'hui, à 13 h 1,pour étudier afin d'en faire rapport, les politiques, les pratiques, les circonstances et les capacités du Canada en matière de sécurité nationale et de défense et les menaces à la sécurité nationale.

Le sénateur Daniel Lang (*président*) occupe le fauteuil.

[*Traduction*]

Le président : Chers collègues, bienvenue à cette séance du Comité sénatorial permanent de la sécurité nationale et de la défense, en ce lundi 21 mars 2016. Avant de commencer, j'aimerais présenter les sénateurs ici présents. Je m'appelle Dan Lang, sénateur du Yukon. À ma gauche, le greffier du comité, Mark Palmer. J'invite donc les sénateurs à se présenter et à indiquer quelle région ils représentent, en commençant par le sénateur Wells.

Le sénateur Wells : David Wells, Terre-Neuve-et-Labrador.

Le sénateur Mitchell : Grant Mitchell, Alberta.

Le sénateur Carignan : Claude Carignan, Québec.

Le président : Merci, chers collègues. Pour notre premier groupe de témoins, nous recevons des représentants de l'Agence des services frontaliers du Canada. En juin dernier, notre comité a déposé un rapport sur l'Agence des services frontaliers du Canada intitulé *Vigilance, reddition de comptes et sécurité aux frontières du Canada*. Le rapport a été adopté à l'unanimité par le comité sénatorial et il contenait 10 recommandations précises, dont : l'établissement d'un organisme de surveillance de l'ASFC et d'un organisme civil et indépendant d'examen des plaintes et des questions liées à la sécurité nationale; l'enregistrement sur support audiovisuel des entrevues réalisées par les agents de l'ASFC; et le contrôle accru des visiteurs, des immigrants et des titulaires de

and permanent residents. It urged the implementation of an entry and exit registry of all travelers, Canadians and non-Canadians. It called for more resources to be made available to the front line for the Canada Border Services Agency officers, and it recommended biometrics be collected from all foreign nationals arriving in Canada subject to existing provisions and agreements with other governments.

Joining us on our first panel today to provide an update on what has been happening with the Canada Border Services Agency are Martin Bolduc, Vice President, Programs Branch; and Caroline Xavier, Vice President, Operations Branch. Welcome. I understand that you have an opening statement, so please begin.

[*Translation*]

Martin Bolduc, Vice President, Programs Branch, Canada Border Services Agency: Thank you. It is a pleasure to be here, and I thank the committee for the opportunity to discuss our work at the Canada Border Services Agency. I have with me today our vice-president of operations, Caroline Xavier.

[*English*]

I have a short opening statement, after which we would be pleased to respond to any questions from the committee.

The Canada Border Services Agency is the second-largest federal armed law enforcement organization. Our mission is as simple as it is complex: ensure the security and prosperity of Canada by managing the access of people and goods to and from Canada. Our job has been summed up in many ways, often in terms of keeping out the bad without impeding the flow of the good.

The CBSA's responsibilities in this regard range from customs and immigration enforcement to food, plant and animal inspection. To do this we administer and enforce the Customs Act, which outlines our responsibilities to collect duties and taxes on imported goods, interdict illegal goods and administer trade legislation and agreements.

[*Translation*]

With Immigration, Refugees and Citizenship Canada, we share responsibility for administering the Immigration and Refugee Protection Act, which governs both the admissibility of people into Canada, and the identification, detention and removal of those deemed to be inadmissible under the act.

visas temporaires, y compris les étudiants, les travailleurs étrangers temporaires, les réfugiés et les résidents permanents. Il appelait la mise en place d'un registre des entrées et des sorties de tous les voyageurs, canadiens et étrangers, de même que des ressources supplémentaires pour les agents de première ligne de l'ASFC, en plus de recommander la collecte de données biométriques auprès de tous les étrangers arrivant au Canada, sous réserve des dispositions des accords intervenus avec les autres gouvernements.

Le premier groupe de témoins à se joindre à nous aujourd'hui est ici pour faire le point sur l'Agence des services frontaliers du Canada. Il s'agit de Martin Bolduc, vice-président, Direction générale des programmes; et Caroline Xavier, vice-présidente, Direction générale des opérations. Bienvenue. Je crois que vous avez une déclaration préliminaire, alors je vous en prie.

[*Français*]

Martin Bolduc, vice-président, Direction générale des programmes, Agence des services frontaliers du Canada : Merci. Je suis heureux d'être ici parmi vous et je remercie le comité de nous donner l'occasion de discuter de notre travail à l'Agence des services frontaliers du Canada. Je suis accompagné aujourd'hui de la vice-présidente de la Direction générale des opérations, Mme Caroline Xavier.

[*Traduction*]

J'aimerais d'abord prononcer une courte déclaration préliminaire, après quoi je répondrai avec plaisir à toutes les questions du comité.

L'Agence des services frontaliers du Canada est le deuxième organisme armé d'exécution de la loi en importance au gouvernement fédéral. Sa mission est aussi simple que complexe : assurer la sécurité et la prospérité du Canada en gérant l'accès des personnes et des marchandises qui entrent au pays et qui en sortent. Nous pouvons résumer notre travail de nombreuses façons, mais souvent il s'agit d'empêcher l'entrée de ce qui est indésirable sans nuire à la circulation de ce qui est souhaitable.

Les responsabilités de l'ASFC à cet égard vont des mesures d'exécution des douanes et de l'immigration jusqu'à l'inspection des aliments, des végétaux et des animaux. Pour y arriver, nous assurons l'application et l'exécution de la Loi sur les douanes, qui définit nos responsabilités en matière de perception des droits et des taxes sur les marchandises importées, nous interceptons les marchandises illégales et nous appliquons les lois et les accords sur le commerce.

[*Français*]

Nous partageons la responsabilité de l'application de la Loi sur l'immigration et la protection des réfugiés avec Immigration, Réfugiés et Citoyenneté Canada. La Loi sur l'immigration et la protection des réfugiés régit l'admissibilité des personnes au Canada, ainsi que l'identification, la détention et le renvoi des personnes jugées interdites de territoire aux termes de la loi.

Finally, the agency enforces over 90 other statutes on behalf of federal departments and agencies. On an average business day, the CBSA processes more than a quarter-million people seeking to enter Canada by land, air and sea. That's close to 100 million people a year.

[*English*]

In the past year, we processed tens of millions of commercial shipments and collected some $29 billion in taxes and duties, or 10 per cent of all government revenue.

In the course of these activities, the CBSA made more than 8,000 drug seizures worth over $400 million, well over 7,000 seizures of weapons and firearms and 43,000 seizures of prohibited food, plants and animals. And, of course, we've been closely involved in the screening and admission of 25,000 refugees from Syria.

As an agency and in collaboration with our partners in Canada and internationally, we continue to seek out and implement new ways to enhance our capacity to carry out these crucial activities efficiently and effectively.

For example, as of last November, critical wants and warrants information is automatically queried at our primary inspection booths from the Canadian Police Information Centre database. We're now able to use this information at the point of arrival.

Just last week, an Electronic Travel Authorization requirement for visa-exempt foreign nationals flying to or transiting through Canada came into effect. These eTAs are issued by Immigration, Refugees and Citizenship Canada and add another level of pre-departure screening.

[*Translation*]

As announced by Prime Minister Justin Trudeau, we will move forward with the entry/exit initiative, building on our relationship with the United States to establish a coordinated and common approach to perimeter security.

As a next step, Canada and the U.S. have agreed to exchange routine biographical information — basically name, date of birth, and nationality/citizenship — for all travellers at land border ports of entry. With this exchange, a record of entry into one country would be considered a record of exit from the other.

Enfin, l'agence exécute plus de 90 autres lois pour le compte d'autres ministères et organismes fédéraux. Dans le cadre d'une journée ouvrable ordinaire, l'ASFC traite plus d'un quart de million de personnes qui souhaitent entrer au Canada par voie terrestre, aérienne et maritime. Cela représente près de 100 millions de personnes par année.

[*Traduction*]

Au cours de la dernière année, nous avons traité des dizaines de millions d'expéditions commerciales et perçu environ 29 milliards de dollars en taxes et en droits de douane, ce qui représente 10 p. 100 des recettes publiques.

Dans le cadre de ces activités, l'ASFC a effectué plus de 8 000 saisies de drogue d'une valeur dépassant les 400 millions de dollars, plus de 7 000 saisies d'armes et d'armes à feu et 43 000 saisies d'aliments, de végétaux et d'animaux prohibés. Bien entendu, nous avons participé étroitement au contrôle et à l'admission de 25 000 réfugiés syriens.

À titre d'organisme fédéral, et en collaboration avec nos partenaires au Canada et à l'étranger, nous continuons de chercher et de mettre en œuvre de nouveaux moyens de renforcer notre capacité à accomplir ces activités essentielles de façon efficace.

À titre d'exemple, depuis novembre dernier, l'information essentielle sur les mandats et les avis de recherche est automatiquement consultée à nos guérites d'inspection primaire à partir de la base de données du Centre d'information de la police canadienne. Nous pouvons maintenant utiliser cette information au point d'arrivée.

Il y a à peine une semaine, l'exigence relative à l'autorisation de voyage électronique est entrée en vigueur pour les étrangers originaires d'un pays dispensé de l'obligation de visa qui entrent au Canada par voie aérienne ou qui transitent par le Canada. Ces autorisations de voyage électroniques sont délivrées par Immigration, Réfugiés et Citoyenneté Canada et ajoutent un niveau supplémentaire de contrôle des voyageurs avant le départ.

[*Français*]

Comme l'a annoncé le premier ministre Justin Trudeau, nous allons de l'avant avec l'Initiative sur les entrées et les sorties, en prenant appui sur notre relation avec les États-Unis pour établir une approche coordonnée et commune de la sécurité du périmètre.

Comme prochaine étape, le Canada et les États-Unis ont convenu d'échanger des données biographiques courantes — essentiellement le nom, la date de naissance et la nationalité ou la citoyenneté — sur l'ensemble des voyageurs dans les postes frontaliers terrestres. Dans le cadre de cet échange, l'enregistrement de l'entrée dans un pays sera considéré comme l'enregistrement de sortie de l'autre pays.

[*English*]

Looking further ahead, within the next four years, with the exception of U.S. citizens, all foreign nationals applying for work or study permits, a visitor visa or permanent residency in Canada will be subject to biometric screening. This will ensure we keep pace with our partners, including the U.S., the U.K. and Europe. Partnership, as would be expected, is of fundamental importance to the CBSA.

[*Translation*]

It has a role in almost everything we do, including our work with domestic and international law enforcement partners to assess the risk of export shipments leaving Canada. In this regard, the CBSA agrees with the findings of the recent report from the Office of the Auditor General. We have developed action plans to respond to the recommendations of the Office of the Auditor General, and we are on track to address most of these by the end of the calendar year.

I am pleased to note that the Office of the Auditor General's report recognized the processes we have implemented to select high-risk shipments for counter-proliferation. The report also highlighted our success in blocking exports of property obtained by crime, such as stolen vehicles.

[*English*]

In many ways, targeting capacity is at the root of success in border management. Our targeting program allows us to perform pre-arrival risk assessments of traveler, cargo and conveyance information with the goal of facilitating movement of low-risk cargo and people and identifying those which may pose a threat to security and safety in Canada. We've been continually improving this program since 2012 and will maintain this commitment going forward. The audit's recommendations and consulting action plan will help strengthen our efforts in this regard.

Where enforcement is concerned, the agency's responsibilities also include identifying and removing from Canada foreign nationals and permanent residents who may pose a threat to our security or may be inadmissible under the Immigration and Refugee Protection Act. Last year we removed more than 11,000 people deemed inadmissible to Canada, with the priority on those with criminality.

[*Translation*]

I would emphasize that the decision to remove someone from Canada is not taken lightly. Anyone ordered to be removed from Canada is entitled to due process before Canadian law. All

[*Traduction*]

Si l'on regarde plus loin, d'ici les quatre prochaines années, à l'exception des citoyens des États-Unis, tous les étrangers qui présenteront une demande de permis de travail ou d'études, de visa de visiteur ou de résidence permanente au Canada feront l'objet d'un contrôle biométrique. Grâce à cette mesure, nous suivrons le rythme de nos partenaires, dont les États-Unis, le Royaume-Uni et l'Europe. Comme on peut s'y attendre, les partenariats ont une importance fondamentale pour l'ASFC.

[*Français*]

Ils jouent un rôle dans presque toutes nos activités, y compris notre travail avec les partenaires nationaux et internationaux d'exécution de la loi pour évaluer le risque des expéditions à l'exportation qui quittent le Canada. À cet égard, l'ASFC souscrit aux constatations du rapport récent préparé par le Bureau du vérificateur général du Canada. Nous avons élaboré des plans d'action pour donner suite aux recommandations du Bureau du vérificateur général, et nous sommes sur la bonne voie de donner suite à la majorité d'entre elles d'ici la fin de l'année civile.

Je suis heureux de mentionner que le rapport du Bureau du vérificateur général reconnaît la valeur des processus que nous avons mis en œuvre pour sélectionner les expéditions à risque élevé afin de lutter contre la prolifération. Le rapport fait également ressortir notre succès lorsqu'il s'agit de bloquer l'exportation de biens criminellement obtenus, tels que les véhicules volés.

[*Traduction*]

À de nombreux égards, la capacité de ciblage est à la base de la réussite dans la gestion frontalière. Notre programme de ciblage nous permet d'effectuer des évaluations des risques avant l'arrivée des voyageurs, des marchandises et des moyens de transport dans le but de faciliter la circulation des marchandises et des personnes à faible risque et de repérer celles qui pourraient constituer une menace à la sécurité du Canada. Nous apportons des améliorations à ce programme sur une base continue depuis 2012 et nous respecterons cet engagement dans l'avenir. Les recommandations découlant de l'audit et le plan d'action qui a suivi contribueront à renforcer nos efforts à cet égard.

Une de nos responsabilités en matière d'exécution de la loi consiste à repérer les étrangers et les résidents permanents qui pourraient constituer une menace à notre sécurité ou qui pourraient être interdits de territoire en vertu de la Loi sur l'immigration et la protection des réfugiés, et à les renvoyer du Canada. L'année dernière, nous avons renvoyé plus de 11 000 personnes jugées interdites de territoire au Canada, en renvoyant en priorité les personnes ayant commis des actes criminels.

[*Français*]

Je tiens à insister sur le fait que la décision de renvoyer une personne du Canada n'est jamais prise à la légère. Toute personne visée par une mesure de renvoi du Canada a droit à l'application

removal orders are subject to various levels of appeal. There are also administrative review procedures that assess the potential risk to the person of returning to the country of origin.

We continue to work closely with our partners, including the Canadian Red Cross and the United Nations High Commissioner for Refugees.

Along with enhancing our capacity for enforcement, we continue to grow programs that help facilitate the legitimate movement of people and goods.

[*English*]

The NEXUS program, for example, which speeds the border process for low-risk, pre-approved travelers between Canada and the U.S., now has more than 1.2 million members. Programs and initiatives such as eManifest and Trusted Trader are helping commercial importers by streamlining and simplifying processes at the border. Here, again, partnership and collaboration are essential to success. For example, we consult frequently with marine, airport and bridge authorities, where there is a significant interest in working with us to modernize infrastructure and the process at the border.

[*Translation*]

We maintain close relationships with industry stakeholders through our commercial consultative committee, which is attended by 25 trade associations, including the Canadian Chamber of Commerce, the Canadian Federation of Independent Business, Canadian Manufacturers and Exporters, the Shipping Federation of Canada, the Canadian Society of Customs Brokers, and the Canadian/American Border Trade Alliance.

The importance of our cooperation and collaboration with the United States in terms of both trade and security cannot be overstated, and we are active participants and contributors in an intelligence alliance with Australia, New Zealand, the United Kingdom and the United States.

[*English*]

We also have a growing relationship with Mexico, which is important for strengthening North American cooperation in areas that improve border security while supporting trade and the facilitation of travelers.

Mr. Chair, I could go on and on, but I recognize that my time is limited. I would like to add that like everyone at the Canada Border Services Agency, I am proud of the role that the people of the CBSA play in protecting our country and our economic

régulière de la loi canadienne. Toutes les mesures de renvoi peuvent faire l'objet d'appels devant différentes instances judiciaires. Il existe aussi des examens administratifs qui évaluent le risque que pourrait courir une personne si elle est retournée dans son pays d'origine.

Nous continuons de travailler en étroite collaboration avec nos partenaires, notamment la Croix-Rouge canadienne et le Haut Commissariat des Nations Unies pour les réfugiés.

En plus de renforcer notre capacité d'exécution de la loi, nous continuons d'élaborer des programmes qui contribuent à faciliter la circulation légitime des personnes et des marchandises.

[*Traduction*]

À titre d'exemple, le programme NEXUS, qui accélère le traitement à la frontière des voyageurs préautorisés à faible risque entre le Canada et les États-Unis, compte maintenant plus de 1,2 million de membres. Des programmes et des initiatives comme le Manifeste électronique et les programmes des négociants dignes de confiance aident les importateurs commerciaux en rationalisant et en simplifiant les formalités à la frontière. Là encore, le partenariat et la collaboration sont la clé du succès. À titre d'exemple, nous consultons fréquemment les administrations des ports, des aéroports et des ponts, qui manifestent un intérêt marqué pour collaborer avec nous en vue de moderniser les infrastructures et les processus à la frontière.

[*Français*]

Nous entretenons des liens étroits avec les intervenants de l'industrie grâce à notre comité consultatif sur les activités commerciales à la frontière, auquel participent 25 associations de négociants, y compris la Chambre de commerce du Canada, la Fédération canadienne de l'entreprise indépendante, Manufacturiers et Exportateurs du Canada, la Fédération maritime du Canada, la Société canadienne des courtiers en douane et la Canadian-American Border Trade Alliance.

On ne saurait trop insister sur l'importance de notre collaboration avec les États-Unis au chapitre du commerce et de la sécurité. Nous participons activement à une alliance sur le renseignement avec l'Australie, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis.

[*Traduction*]

Nous avons également une relation grandissante avec le Mexique, ce qui est important pour renforcer la collaboration nord-américaine dans des domaines qui permettent d'améliorer la sécurité des frontières tout en facilitant les échanges commerciaux et les déplacements des voyageurs.

Monsieur le président, je pourrais continuer, mais je suis conscient que le temps qui m'est accordé est limité. J'aimerais ajouter que, comme tous les gens de l'Agence des services frontaliers du Canada, je suis fier du rôle que les employés de

prosperity, and of the commitment, dedication and professionalism they bring to the challenges they face every single day.

Thank you for this time, Mr. Chair. I look forward to any questions honourable senators may have.

The Chair: Thank you very much, sir.

I'd like to note for the record that Senator Day, Senator Ngo and Senator L. Smith are here as well.

Before we get into the recommendations of our report of last spring, I'd like to raise an issue that has come to our attention: the death, which was made public, in a detention centre in Ontario about a month ago. Perhaps you could clarify for the record exactly what happened. We also had a death in Vancouver, I believe two years ago. First, could you give us some background in respect of the detention by the CBSA? Second, could you also give us an indication of how many individuals have died in the custody of or in detention by CBSA over, say, the last 10 years?

Mr. Bolduc: I'll turn it over to my colleague, Ms. Xavier.

Caroline Xavier, Vice President, Operations Branch, Canada Border Services Agency: I will not be able to get into the details of the two recent deaths in the news. However, as you say, they happened at two provincial facilities, one at Maplehurst Correctional Complex and the other at the Toronto East Detention Centre. That's the extent of what I will be able to speak to with regard to those two recent deaths. We take seriously the matter of the care of individuals within our detention facilities or those within the provincial facilities on our behalf.

You asked about how many deaths have occurred over the last 10 years. Since the creation of the agency in 2003, we have had 11 deaths, two of them in the immigration holding centres of the CBSA and the remaining in provincial facilities where they were held on our behalf. Quite a bit has been done with regard to lessons learned every time an incident occurs within our facilities. The other death that you speak of happened in the British Columbia Immigration Holding Centre in Vancouver. There has been a coroner's inquest into that case and recommendations have come forth.

We have adhered to many of those recommendations, including the fact that on a national level we have looked at all of our immigration centres, policies and the way in which our programs are managed, including changes to physical infrastructure in our immigration holding centres to minimize any potential for self-harm. As well, we have ensured that

l'ASFC jouent dans la protection de notre pays et de notre prospérité économique, ainsi que de l'engagement, du dévouement et du professionnalisme dont ils font preuve pour relever les défis qui se présentent tous les jours.

Monsieur le président, je vous remercie du temps que vous m'avez accordé. C'est avec plaisir que je répondrai maintenant aux questions des honorables sénateurs.

Le président : Merci beaucoup, monsieur.

Je précise au passage que les sénateurs Day, Ngo et L. Smith sont aussi avec nous.

Avant d'examiner les recommandations formulées dans notre rapport du printemps dernier, j'aimerais faire mention d'un événement qui a été porté à notre attention : le décès d'une personne gardée dans un centre de détention de l'Ontario il y a environ un mois. Cela a été rendu public. Peut-être que vous pourriez nous indiquer précisément ce qui s'est passé aux fins du compte rendu. Il y a également eu un décès à Vancouver, il y a deux ans, je crois. Premièrement, pourriez-vous nous parler du contexte entourant la détention par l'ASFC? Deuxièmement, pourriez-vous aussi nous dire combien de personnes sont décédées alors qu'elles étaient détenues par l'ASFC au cours des 10 dernières années, disons?

M. Bolduc : Je vais renvoyer la question à ma collègue, Mme Xavier.

Caroline Xavier, vice-présidente, Direction générale des opérations, Agence des services frontaliers du Canada : Je ne pourrai pas entrer dans les détails en ce qui a trait aux deux décès rapportés récemment dans les médias. Je peux cependant vous confirmer qu'ils ont eu lieu, comme vous l'avez mentionné, dans deux établissements provinciaux : un au Centre correctionnel Maplehurst, et l'autre au Centre de détention de l'Est de Toronto. C'est tout ce que je peux vous dire à ce sujet. Nous prenons très au sérieux la façon dont sont traitées les personnes sous la garde de nos centres de détention ou détenues dans les installations provinciales en notre nom.

Vous vouliez savoir combien il y avait eu de décès au cours des 10 dernières années. Depuis la création de l'agence, en 2003, nous avons déploré 11 décès, dont deux dans les centres de surveillance de l'immigration de l'ASFC, et les autres dans des établissements provinciaux où ces personnes étaient détenues pour l'agence. Chaque incident nous a permis de tirer des leçons, et nous avons amélioré bien des choses dans nos installations depuis. L'autre décès auquel vous faites allusion s'est produit en Colombie-Britannique, au Centre de surveillance de l'Immigration de Vancouver. Des recommandations ont été formulées à la suite du rapport du coroner dans cette affaire.

Nous avons mis en œuvre bon nombre de ces recommandations. Nous avons notamment examiné tous les centres de surveillance de l'immigration du pays, toutes les politiques nationales, de même que la façon dont sont administrés nos programmes. Des modifications ont aussi été faites à l'infrastructure physique des centres de surveillance de

programs in our detention facilities are run to the appropriate standards. We work with entities such the Canadian Red Cross and the UNHCR, who come to our centres to review programs and make recommendations to us on a regular basis.

We've also continued to put in place such policies as medical forms, which are updated every 60 days, to ensure that we take good care of individuals in our facilities with regard to both their mental health and their physical health.

I could go on a bit more, but I think that gives you an overview.

The Chair: I'll pursue this a bit, colleagues, because it is important, current and of concern, obviously, to your organization and to the general public.

Is the Canada Border Services Agency doing their own investigation, or is an outside agency doing the investigation to ensure objectivity?

Ms. Xavier: I'd say both of the above. We always do our immediate fact-finding and investigation to ensure that policies were adhered to and find out what the incident is. We also work in collaboration with the province where the incident may have occurred, with the local police in the jurisdiction of the facility and with the coroner, in particular cases such as the B.C. incident. As well, a series of reviews and investigations are done with outsiders. On an annual basis and as part of our regular regime, there is also collaborative work with our colleagues in the Canadian Red Cross and the UNHCR, who come in and give us feedback on how well our programs are being managed.

The Chair: I want to hone in on what was said specifically. You talked about collaboration. It seems that you would call in a provincial authority to do their review and come out with their findings. For example, in the case of Ontario, you would call in Ontario's Special Investigations Unit so that you're made totally aware that things were done properly. If they weren't, then you'd be told so that you could take corrective action. Is that what would happen?

Ms. Xavier: Again, it depends where the incident occurs. In the case of provincial facilities, we work with them. Whatever mechanisms of review are done by those facilities, we adhere to that and work with those investigative organizations, including, as you said, some of the bodies you mentioned and the local coroner of the province. For any death, the majority of the time a coroner's inquest will occur, and from that, an independent review is also done.

The Chair: To conclude this, are they automatically called when there is a death?

l'immigration afin de réduire les risques d'automutilation. Nous travaillons avec la Croix-Rouge canadienne et l'UNHCR, qui dépêchent régulièrement des représentants dans nos centres pour évaluer les programmes et nous soumettre leurs recommandations.

Nous avons aussi continué à mettre en place des politiques comme celle sur les formulaires médicaux, qui sont actualisés tous les 60 jours, afin de veiller aux bons soins des personnes détenues dans nos établissements, tant pour ce qui est de leur santé mentale que de leur santé physique.

Je pourrais continuer, mais je crois que cela vous donne une idée.

Le président : Je vais poursuivre en ce sens, chers collègues, car c'est une question d'actualité importante et préoccupante, de toute évidence, pour votre organisation et pour le grand public.

Est-ce que l'Agence des services frontaliers du Canada mène ses propres enquêtes, ou est-ce qu'elle confie le mandat à une entité externe pour assurer l'objectivité du processus?

Mme Xavier : Je dirais les deux. Nous procédons toujours à la vérification immédiate des faits et menons notre propre enquête pour nous assurer que les politiques ont été respectées et vérifier ce qui s'est passé. Nous travaillons aussi en collaboration avec la province où s'est produit l'incident, avec le service de police local et avec le coroner, surtout dans les cas comme celui de la Colombie-Britannique. De plus, une série d'examens et d'enquêtes sont effectués par des entités externes. Chaque année, dans le cadre de notre processus régulier, nous travaillons également en collaboration avec nos collègues de la Croix-Rouge canadienne et de l'UNHCR, qui examinent pour nous comment nos programmes sont administrés.

Le président : Je veux revenir sur ce qui a été dit précisément. Vous avez parlé de collaboration. J'en déduis que vous feriez appel à une organisation provinciale pour qu'elle fasse sa propre enquête et en tire ses propres conclusions. Par exemple, pour ce qui est arrivé en Ontario, vous appelleriez l'Unité des enquêtes spéciales de l'Ontario, qui pourrait vous dire précisément si les choses ont été faites correctement. Sinon, elle vous recommanderait de prendre des mesures correctives. Est-ce ainsi que les choses se passent?

Mme Xavier : Encore là, tout dépend de l'endroit où s'est produit l'incident. Si c'est arrivé dans un établissement provincial, nous travaillons en collaboration avec la province. Peu importe les mécanismes d'examen assurés par ces installations, nous les respectons et travaillons avec les entités responsables des enquêtes, y compris celles que vous avez mentionnées, et le coroner local. Dans la majorité des cas de décès, il y aura enquête du coroner, et à partir de là, un examen indépendant est aussi effectué.

Le président : Pour clore le sujet, ils sont appelés automatiquement lorsqu'un décès survient?

Ms. Xavier: They are automatically called. Whether they choose to do an inquest for every investigation, you'd have to confirm that with the provinces' coroners.

The Chair: I'm not talking about that. I'm talking about, for example, the Ontario Special Investigations Unit. Are they called immediately or later?

Ms. Xavier: I can't say they're called automatically because it depends on where an incident takes place and the rules within that facility.

As I said, we work within the provincial facilities and whatever review mechanisms or bodies they may have with regard to their facilities. We work with all the various organizations and authorities of jurisdiction within each province where the facilities are held.

[*Translation*]

Senator Carignan: I would like to come back to the answer to a question I put to a representative of the Office of the Auditor General, Nancy Cheng, who said the following:

> Herein lies the problem with non-declared shipments, for example, because for those, the CBSA doesn't have authority to do random checks.

She says, at least in her statement, that you supposedly don't have the authority to do random checks for non-declared shipments. Can you tell me whether that is how you understand things, and why you cannot do random checks for shipments, considering that you do checks for individuals anyway? If random checks can be done for individuals, I feel that they should be fine for shipments. Right?

Mr. Bolduc: I don't have the context for the quote to know what she was referring to, but there are no legal provisions preventing us from doing random checks for commercial goods. Obviously, given the volumes we process, and depending on the mode of importation, it may prove to be difficult, but there are mechanisms in place. I would need some more details regarding the context of that statement.

Senator Carignan: Okay. My second question is about having an organization that would oversee the agency's activities or an inspector general. Are you comfortable with the idea of not having that kind of an organization for overseeing activities? Or do you think there should be one? If so, what are the steps you are currently taking to implement something like that?

Mr. Bolduc: The decision to provide the agency with an oversight organization will obviously belong to the government. There are a number of ways to review the decisions made by the agency. One of those has to do with our seizures, which can be

Mme Xavier : Ils sont appelés automatiquement. C'est à eux ensuite de décider si cela mérite un rapport, mais ce serait à confirmer avec les coroners provinciaux.

Le président : Ce n'est pas ce que je veux dire. Je parle, par exemple, de l'Unité des enquêtes spéciales de l'Ontario. Est-ce qu'on l'appelle immédiatement ou plus tard?

Mme Xavier : On ne l'appelle pas automatiquement, parce que cela dépend de l'endroit où s'est produit l'incident et des règles en place dans les installations en question.

Comme je le disais, nous travaillons avec les installations provinciales et nous suivons les mécanismes d'examen en place ou les entités désignées. Nous collaborons avec les différentes organisations et les autorités de chaque province où sont administrées les installations.

[*Français*]

Le sénateur Carignan : J'aimerais revenir à la réponse à une question que j'ai posée il y a quelques semaines à une représentante du Bureau du vérificateur général, Mme Nancy Cheng, qui a déclaré ce qui suit :

> Prenez, entre autres, le problème des envois non déclarés pour lesquels l'ASFC n'a pas le droit d'effectuer de contrôles aléatoires.

Elle soutient, du moins dans sa déclaration, que, dans le cas des envois non déclarés, vous n'auriez pas le pouvoir de faire des contrôles aléatoires. Pouvez-vous m'expliquer si c'est là votre compréhension, et pourquoi vous ne pouvez pas faire de contrôles aléatoires pour les colis, compte tenu du fait que, de toute façon, vous en faites pour les personnes? Si on fait des contrôles aléatoires pour les personnes, on devrait, à mon sens, pouvoir le faire pour les envois, n'est-ce pas?

M. Bolduc : Je n'ai pas le contexte de la citation pour savoir à quoi elle faisait référence, mais il n'y a aucune disposition légale qui nous empêche de faire des contrôles aléatoires de marchandises commerciales. Évidemment, compte tenu des volumes que nous traitons, et dépendamment du mode d'importation, cela peut s'avérer difficile, mais il y a des mécanismes en place. Il me faudrait un peu plus de détails quant au contexte de cette déclaration.

Le sénateur Carignan : Parfait. Ma deuxième question porte sur le fait d'avoir un organisme de surveillance, de supervision des activités de l'agence ou d'avoir un inspecteur général. Êtes-vous à l'aise avec l'idée de ne pas avoir ce type d'organisation de surveillance des activités? Ou pensez-vous qu'il devrait y en avoir une? Quelles sont les démarches que vous faites à l'heure actuelle, le cas échéant, pour les mettre en place?

M. Bolduc : La décision de doter l'agence d'un organisme de révision reviendra évidemment au gouvernement. Il existe plusieurs avenues possibles quant à la révision des décisions prises par l'agence. L'une de ces avenues est liée à nos saisies, qui

appealed to the minister. We refer to it as our recourse program, and it stems from a legal obligation.

As far as detention goes, each of our decisions to detain an individual is reviewed by the Immigration and Refugee Board of Canada, after 48 hours of detention, after 7 days, and over the next 30 days. So there are some neutral organizations that review the agency's decisions. We refer to the Office of the Auditor General, the reports on plans and priorities, and so on. Now, if the government wants to provide the agency with a different framework, the agency will collaborate on its implementation.

Senator Carignan: Don't you have any suggestions you could make to the government on oversight measures that should be implemented? You are waiting for the government's decision?

Mr. Bolduc: Like you, I read that the Minister of Public Safety told the media that he was thinking about a framework that could suit the agency. Of course, we will work with the department on providing suggestions, but the decision will rest with the government.

[*English*]

Senator Mitchell: Chair, if I had three questions it would make a difference to how I would start, rather than just two. Would you give me two? I should have asked for four; maybe I could have got three. Thanks.

Thanks to both of you for being here. I'm interested in following up a bit on the chair's questioning about imprisonment. There are reports — I think they're quite broadly known now — that many refugee-type arrivals end up being held without charges for many years. I think one is, in fact, now for 11 years.

That doesn't seem consistent with proper human rights. It doesn't seem consistent with the rule of law. How do you propose we deal with that in a fair, more just way?

Ms. Xavier: Just to be clear, are you looking for how we propose the way forward? That would be difficult for me to speak to. What I can tell you is consistent with what you heard from my colleague, that there are dialogues I expect this government may have as a result of some of the things they're hearing and the views that this government may have.

However, I can speak to what exactly we do currently. As Martin was saying earlier, when somebody is being detained they have a series of avenues available to them immediately, within the 48 hours, and then the seven and then every 30 days. Usually when we detain somebody, it is because they're a public safety, health or national security concern, for reasons of identity confirmation or for reasons that they could potentially be a flight risk, or it was a mass arrival, as we call it.

peuvent faire l'objet d'un appel auprès du ministre, et qu'on appelle notre Programme des recours, lequel découle d'une obligation légale.

En ce qui concerne la détention, chacune de nos décisions de détenir un individu est revue par la Commission de l'immigration et du statut de réfugié, et ce, après 48 heures de détention, après 7 jours, et pour les 30 jours subséquents. Il y a donc tout de même des organismes neutres qui révisent les décisions prises par l'agence. On fait référence au Bureau du vérificateur général, aux Rapports sur les plans et les priorités, ainsi de suite. Maintenant, si le gouvernement désire doter l'agence d'un cadre différent, l'agence collaborera à la mise en place de ce cadre.

Le sénateur Carignan : De votre côté, vous n'avez pas d'idées sur les mesures de surveillance qui devraient être mises en place, que vous pourriez suggérer au gouvernement? Vous attendez la décision du gouvernement?

M. Bolduc : Tout comme vous, j'ai lu que le ministre de la Sécurité publique a affirmé aux médias qu'il réfléchissait au cadre qui pourrait convenir à l'agence. Évidemment, nous travaillerons en collaboration avec le ministère pour émettre des suggestions à ce moment-là, mais la décision reviendra au gouvernement.

[*Traduction*]

Le sénateur Mitchell : Monsieur le président, si vous me permettiez de poser trois questions plutôt que deux, je commencerais différemment. Je peux en poser deux? J'aurais dû en demander quatre; peut-être que j'en aurais eu trois. Merci.

Merci à vous deux d'être ici. J'aimerais poursuivre un peu dans la même veine que le président et vous poser quelques questions sur les détentions. On a signalé — et je pense que c'est un fait bien connu maintenant — que beaucoup de réfugiés qui arrivent au pays sont détenus sans accusation pendant de nombreuses années. En fait, je crois qu'un de ces réfugiés est détenu depuis 11 ans.

Cela ne semble pas cadrer avec les principes pertinents en matière de droits de la personne. Cela ne semble pas cadrer non plus avec la primauté du droit. Comment proposez-vous que nous abordions la situation, pour que ce soit plus juste et équitable?

Mme Xavier : Je veux simplement m'assurer de bien comprendre votre question : vous voulez savoir ce que nous proposons pour l'avenir? Ce serait difficile pour moi de me prononcer là-dessus. Ce que je peux vous dire, et cela rejoint ce que mon collègue disait tout à l'heure, c'est que je présume que le gouvernement actuel, vu ses positions sur le sujet, voudra tenir des discussions à la lumière des choses qui ont été rapportées.

Je peux toutefois vous parler de la façon dont les choses se passent actuellement. Comme Martin l'indiquait plus tôt, quand une personne est mise sous garde, différentes options s'offrent à elle dans l'immédiat, dans les premières 48 heures, puis dans les sept qui suivent, et ensuite tous les 30 jours. Lorsque nous détenons une personne, c'est normalement parce qu'elle pose des risques pour la sécurité ou la santé publique ou pour la sécurité nationale. C'est peut-être que nous ne pouvons pas confirmer son

There are various reasons, but the ongoing detention of an individual is really under the remit of the Immigration and Refugee Board because that's where we go every 30 days to confirm whether that detention should be continued.

Again, it's not taken lightly. We take detaining somebody very seriously. We do look at various options other than detention before we get there, depending on the case before us.

Senator Mitchell: Specifically now to recommendations. One of our recommendations in the report that the chair referred to in his opening comments was that all interviews with prospective immigrants or people arriving at the border, visitors, should be videotaped. Have you given that some consideration? Can you give us an update as to where you might be in the implementation of that? Questions arise, sort of he said, she said.

Ms. Xavier: With regard to when we're doing interviews, for example, in our secondary examination centres, those are recorded, less so video, perhaps, but at least audio, depending.

In terms of the IRB hearings, those are held in a manner that is more or less — I'll use the term lightly — public. There are recordings of those proceedings, and they are made public depending on what the IRB members determine, because each case can be sensitive.

The information is in the public record when it's before the IRB. For other reasons when we're interviewing some individuals, they are recorded in some manner as well, whether it's audio or audiovisual.

Senator Mitchell: I'm going right back to the recommendations. On number 9, we were quite struck to find that there was a wall between central CBSA information, intelligence operations and the information that didn't get past that wall that could have been used by front-line border workers, which would be the Integrated Customs Enforcement System database. We were also struck that there wasn't a great deal of exchange with the Canadian Police Information Centre database information at the point of primary inspection, that is, the border. How can that be? Has it been corrected? Have you worked on it?

Mr. Bolduc: In fact, it's been corrected since November of last year.

Senator Mitchell: Is that because of our recommendation?

identité ou que nous avons des raisons de croire qu'elle présente un risque de fuite. Il arrive aussi que nous ayons des arrivées massives, comme on dit.

Il y a plusieurs raisons, mais la détention continue d'un individu relève de la Commission de l'immigration et du statut de réfugié, car c'est à elle que nous nous adressons tous les 30 jours pour confirmer que la détention doit être maintenue.

Encore là, nous ne prenons pas cela à la légère. Nous savons que la détention est une avenue très sérieuse. Avant d'en arriver là, nous examinons les options qui s'offrent à nous, autres que la détention, et c'est toujours en fonction du cas qui nous occupe.

Le sénateur Mitchell : Passons maintenant aux recommandations. Une des recommandations formulées dans le rapport auquel le président a fait référence dans son introduction visait à enregistrer sur support audiovisuel toutes les entrevues avec les immigrants éventuels ou les personnes se présentant à la frontière, les visiteurs. Avez-vous envisagé cette possibilité? Pouvez-vous nous dire où vous en êtes avec la mise en œuvre de cette recommandation? Quand des questions sont soulevées, c'est un peu votre parole contre la leur.

Mme Xavier : Lorsque nous menons des entrevues, par exemple dans nos centres d'examen secondaire, celles-ci sont enregistrées. Peut-être pas nécessairement sur support vidéo, mais au moins sur support audio.

Pour ce qui est des audiences de la CISR, le tout se déroule de façon publique, si je peux m'exprimer ainsi, même si ce n'est pas exactement le terme qui convient. Ces audiences sont enregistrées, et elles sont rendues publiques si les membres de la CISR déterminent que c'est justifié, car certains cas peuvent imposer une certaine discrétion.

Les renseignements sont du domaine public quand ils arrivent à la CISR. On en enregistre aussi, pour d'autres raisons, quand nous interrogeons des particuliers, par des moyens audio ou audiovisuels.

Le sénateur Mitchell : Je reviens aux recommandations. À la recommandation n° 9, nous avons été tout à fait secoués de constater l'existence d'un mur entre les services centraux d'information et de renseignement de l'ASFC, qui empêchait l'information de le franchir et de servir aux agents de première ligne des services frontaliers, à partir de la base de données du Système intégré de l'exécution des douanes. Nous avons aussi été étonnés d'apprendre qu'il n'y avait pas beaucoup d'échanges de renseignements avec la base de données du Centre d'information de la police canadienne, au point d'inspection primaire, c'est-à-dire à la frontière. Comment ça se fait? A-t-on corrigé cette lacune? Y avez-vous travaillé?

M. Bolduc : En fait, c'est corrigé depuis novembre dernier.

Le sénateur Mitchell : Grâce à notre recommandation?

Mr. Bolduc: I think your recommendations were the push that we needed to move, but the work with the RCMP had been started. So front-line officers now have access to warrants at primary, and we're already seeing the success of having that information available. We've been able to effect arrests and refer cases to the police who issued the arrest warrants. So it has been very successful.

As for your question vis-à-vis the intelligence, in fact, our intelligence program is there to support our front line. I would say that we have a very dynamic workforce that is spread out in all of our regions and, again, works in collaboration with other law enforcement because the day-to-day reality of our business is that you are as effective as your intelligence is good.

I think what might have been perceived as barriers are coming down. Again, as I said, often we will have intelligence officers right at the POE, the port of entry, who will then support the front line day-to-day.

Senator Wells: Thank you, Mr. Bolduc and Ms. Xavier, for appearing.

I have a question that is a follow-up from Senator Carignan's question. One of the recommendations was that the Auditor General called for the CBSA to take steps to ensure that gaps in coverage for export examinations aren't predictable.

First, why were they predictable? As you can appreciate, this kind of predictability can help those who wish to exploit our systems. And second, what actions have you taken to make them less predictable?

Mr. Bolduc: The predictability was derived where on some occasion we put a hold on a shipment to give us the ability to do an examination. When you don't act quickly on that examination, you open up your game book to the outside world. What we've been focusing on is that, as soon as there is a shipment of interest to the CBSA, we act upon that examination to either confirm or deny that there is a need for us to investigate further. So those corrective actions have been taken by the CBSA so that we're a little more action-oriented when it's time to inspect shipments for export.

As for the other recommendations that were made by the Office of the Auditor General, they speak to the timeliness of the information that we get and also that we be a little more structured in identifying what is of priority. If we do the ratio, we get about 1 million export declarations a year. If you look at the import side, we process over 15 million commercial imports. Again, a smaller team looks at exports, but I think the recommendation will help us to have a better-managed program that has demonstrated, according to the Office of the Auditor General, that it can be efficient and effective.

Senator Day: My apologies for being a wee bit late getting here. I'm caught up now.

M. Bolduc : Je pense qu'elle a donné le petit coup de pouce nécessaire pour nous faire bouger, mais la collaboration avec la GRC avait commencé. Les agents de première ligne ont maintenant accès aux mandats, à l'inspection primaire, et, déjà, nous constatons l'avantage de disposer de ces renseignements. Nous avons ainsi pu faire des arrestations et saisir la police de certains dossiers, ce qui lui a permis de délivrer les mandats d'arrestation. La mesure a donc été très efficace.

En ce qui concerne notre programme de renseignement, il existe, en fait, pour appuyer le travail de nos agents de première ligne. Notre personnel très dynamique, réparti dans toutes nos régions, collabore, encore une fois, avec d'autres polices, parce que le quotidien de notre activité rend notre efficacité proportionnelle à la qualité de notre renseignement.

Je pense que ce mur s'écroule. Comme je l'ai dit, nos agents du renseignement se trouveront précisément au point d'entrée, pour ensuite appuyer dans leur travail quotidien nos agents de première ligne.

Le sénateur Wells : Merci, madame Xavier, monsieur Bolduc, d'être ici.

Ma question fait suite à celle du sénateur Carignan. L'une des recommandations du vérificateur général était de réclamer de l'ASFC la prise de mesures pour empêcher la prévisibilité des lacunes dans son examen des exportations.

Pour commencer, pourquoi sont-elles prévisibles? Comme vous pouvez le constater, cette prévisibilité peut favoriser ceux qui veulent profiter de notre système. Ensuite, qu'avez-vous fait pour les rendre moins prévisibles?

M. Bolduc : Leur prévisibilité découle du fait qu'il arrive que nous retenions un chargement pour l'examiner. Quand l'examen tarde, on révèle en quelque sorte notre recueil de stratégies au monde extérieur. Nous nous sommes donc efforcés, dès qu'un chargement présente de l'intérêt pour notre agence, de l'examiner sans tarder, pour soit confirmer, soit nier la nécessité, pour nous, d'approfondir l'enquête. Ces mesures correctrices ont donc amené l'Agence à agir un peu plus rapidement lorsque vient le temps d'inspecter des chargements destinés à l'exportation.

Quant aux autres recommandations du Bureau du vérificateur général, elles concernent l'opportunité des renseignements que nous obtenons et la nécessité de nous organiser un peu mieux pour déterminer nos priorités. Voyez le rapport : nous examinons environ un million de déclarations d'exportations par année. Quant aux importations commerciales, nous en traitons plus de 15 millions. Encore une fois, l'équipe qui s'occupe des exportations est plus petite, mais je pense que la recommandation nous aidera à nous doter d'un programme mieux géré, qui a prouvé son efficacité, d'après le Bureau du vérificateur général.

Le sénateur Day : Veuillez m'excuser pour mon retard. Je me suis maintenant repris.

My first question goes to the relationship at the border. Do every one of your border crossing points — I'm thinking Canada-U.S. — now have an armed CBSA person in attendance?

Ms. Xavier: That's correct. So, as part of the initiative with regard to arming the Border Services officers, one the priorities was ensuring that at the land border port of entry, our officers be armed at the primary inspection line, and that indeed is the goal of the initiative. To this day, at this point, we're pretty much there with having armed all of our officers who are at the front primary inspection line with a firearm.

Senator Day: What percentage? You're almost there — 90 per cent?

Ms. Xavier: No, I'd say we're pretty much 100 per cent there. The only reason I had that hesitation — "pretty much there" — is that, for example, you may have the odd officer who is about to go back onto the primary inspection line who just came off of parental leave. They may have to get trained, recertified, and get back on the front line. All of the officers who are expected to be manning the front primary inspection booth are armed.

Senator Day: That's helpful for us to know that, chair.

My colleague Senator Mitchell was asking a question about the information at your primary inspection place. That's the first place that someone coming into Canada would stop at.

In the past, we have learned that you had difficulty with calling in if you felt you should call in the RCMP. They weren't always standing at the ready to come, and that posed a difficulty in the coordination to effect the action you wanted to effect.

Can I assume now that, with the armed personnel, that problem is less than it was? Do you have arrest and detention authority and facilities?

Ms. Xavier: We always had the authority to arrest and detain with regard to the CBSA mandate. The ability to have the side arm now is just an additional tool for us to use in the bailiwick of tools that we already had with regard to our posture.

We feel we have an excellent relationship with our RCMP colleagues, and they continue to be quite responsive to us on the calls that we make to them with regard to anything that goes beyond our mandate or that we're exercising on behalf of their mandate. As you know, the CBSA does a lot of work on behalf of others. Over 90 acts are managed by the CBSA on behalf of others. Although we may be that first point of intervention, if you want, we would potentially still need to call the RCMP, depending on the situation, because it's for them to take over that investigation from a particular point.

Senator Day: I have another line of questioning, but I wonder if I can go on second round.

The Chair: Fine, sir.

Senator Ngo: I would like to continue the questions asked by Senator Mitchell.

Ma première question concerne les rapports à la frontière. Est-ce qu'à chacun de vos points de passage — à la frontière canado-américaine — se trouve un agent armé de l'ASFC?

Mme Xavier : Oui. L'une des priorités de l'initiative visant à armer les agents de services frontaliers était justement de doter la ligne d'inspection primaire, au point d'entrée de la frontière terrestre, d'agents armés. C'est maintenant chose à peu près faite. Presque tous nos agents postés à la première ligne d'inspection primaire portent une arme à feu.

Le sénateur Day : Quel pourcentage? Presque tous : est-ce 90 p. 100?

Mme Xavier : Non, presque 100 p. 100. Si je n'ai pas dit tout, c'est seulement parce que, par exemple, il peut arriver qu'un agent à la veille de retourner sur la ligne d'inspection primaire vient de terminer un congé parental, qu'il n'a pas été formé, que son accréditation n'a pas été renouvelée. Tous les agents censés occuper la guérite de première inspection sont armés.

Le sénateur Day : C'est utile pour nous de le savoir, monsieur le président.

Mon collègue Mitchell a posé une question sur les renseignements accessibles sur votre ligne d'inspection primaire, le premier endroit où s'arrêterait quelqu'un qui arrive au Canada.

Dans le passé, nous avons appris qu'il n'allait pas toujours de soi pour vous d'appeler la GRC à la rescousse. Elle n'était pas toujours prête à se porter chez vous, et cela compliquait la coordination des mesures que vous vouliez appliquer.

Puis-je maintenant supposer que, vos agents étant désormais armés, ce problème a perdu de son acuité? Avez-vous des pouvoirs d'arrestation et de détention ainsi que les locaux voulus?

Mme Xavier : Notre mandat nous a toujours accordé le pouvoir d'arrêter et de détenir les contrevenants. Le fait d'être armés ne fait qu'ajouter un moyen de plus à l'arsenal dont nous disposions déjà.

Nous estimons entretenir d'excellents rapports avec nos collègues de la GRC, et ils continuent de réagir très rapidement à nos appels pour tout ce qui déborde notre mandat ou pour ce que nous faisons pour leur compte. Comme vous le savez, notre agence fait beaucoup de travail pour les autres. Nous administrons plus de 90 lois au nom d'autres organisations. Même si en étant les premiers intervenants, si vous voulez, nous aurions quand même besoin d'appeler la GRC, selon la situation, parce qu'il lui revient, passé un certain point, de s'occuper de l'enquête.

Le sénateur Day : J'ai une autre série de questions à poser, mais je me demande si je peux attendre mon prochain tour.

Le président : Très bien.

Le sénateur Ngo : Je voudrais suivre le filon prospecté par le sénateur Mitchell.

Of course, one of the mandates of the CBSA is to ensure that the free flow of export goods complies with Canada's laws. Does the CBSA have the necessary information, practices and authority to prevent the export of goods that contravene Canada's export laws?

Mr. Bolduc: Again, CBSA is sort of the *guichet unique*, the single window, if I can use the expression, for many departments when we're talking about exports. Our ability to get timely information to be able to make decisions relies on the cooperation we have with other government departments. I think there are 12 government departments that are involved or have a nexus when we talk about exports.

I think the Auditor General's report highlighted the fact that we are effective in addressing proliferation and that we are successful when it comes to goods acquired through criminal acts. We seize annually, on average, 450 stolen cars at the different ports we have.

As for the authorities, again, the Customs Act is built in such a fashion that a lot of focus is put on imports and a little less focus on exports. I think the Auditor General made six recommendations. We're following up on those six recommendations, and we believe that we'll be in good shape, as I said, by the end of 2016 to have addressed all of those recommendations.

Senator Ngo: The Auditor General's audit said about one third of the targets were not met because the CBSA came too late, or some other things prevented you from doing anything until after the shipment was gone, or the ship left the port, and so on. Could you explain those delays of one third of the targets not met?

Mr. Bolduc: Well, it speaks a bit to the point that I was making earlier. It's being less predictable. It's having a framework that is more rigorous about acting on those shipments that we have an interest in, but it's always the dilemma of competing priorities. As I said, it's about a ratio of 1 to 15, export versus import. We will always be challenged with priorities, but our commitment is to do a better job. The next time that the Auditor General comes and visits, it won't be one third.

Senator Ngo: What do you recommend to address the situation?

Mr. Bolduc: Again, it's having the right focus. In our day-to-day work, it's always a challenge to find the right thing to look at and to direct the right resources for those high-risk goods and high-risk people. It's a daily challenge.

I think we have a good program. I think the recommendations of the Auditor General will make our program better, and I am confident that we will meet the expectations and that we will be able to report to Canadians what is expected of us, that we deliver and protect Canada.

Bien sûr, l'un des mandats de l'ASFC est de s'assurer que la libre circulation des marchandises destinées à l'exportation se fasse conformément aux lois canadiennes. Est-ce que l'Agence possède les renseignements, les habitudes et les pouvoirs nécessaires pour empêcher l'exportation de marchandises qui contreviennent aux lois canadiennes?

M. Bolduc : Encore une fois, notre agence est une sorte de guichet unique pour beaucoup de ministères, quand il s'agit d'exportation. Notre capacité d'obtenir des renseignements opportuns pour la prise de décisions dépend de la collaboration d'autres ministères fédéraux. Je pense que douze de ces ministères sont impliqués ou ont un lien avec nous pour les exportations.

Je pense que le rapport du vérificateur général a souligné notre efficacité contre la prolifération et notre succès contre l'acquisition de marchandises à la faveur d'actes criminels. Chaque année, nous saisissons en moyenne, 450 voitures volées, dans les différents points où nous sommes postés.

Quant aux lois, encore une fois, celle sur les douanes est ainsi construite qu'elle insiste beaucoup plus sur les importations que sur les exportations. Je pense que le vérificateur général a formulé six recommandations. Nous y donnons suite et nous croyons être en bonne posture, d'ici la fin de 2016, comme je l'ai dit, d'avoir donné suite à toutes.

Le sénateur Ngo : D'après l'audit du vérificateur général, le tiers des objectifs de votre agence n'a pas été atteint parce qu'elle est arrivée trop tard, qu'un empêchement l'a paralysée jusqu'après le départ du chargement ou que le bateau a quitté le port et ainsi de suite. Pourriez-vous expliquer ce tiers d'objectifs non atteints?

M. Bolduc : Eh bien, ça revient un peu à ce que je disais : c'est moins prévisible. Malgré un cadre plus rigoureux pour l'intervention sur les chargements auxquels nous nous intéressons, le dilemme des priorités contraires se pose toujours. Comme je l'ai dit, le rapport des exportations aux importations est d'environ 1 à 15. Nous serons toujours sollicités par les priorités, mais nous sommes déterminés à faire un meilleur travail. Au prochain audit du vérificateur général, ce ne sera plus un tiers d'objectifs manqués.

Le sénateur Ngo : Que recommandez-vous pour corriger la situation?

M. Bolduc : Encore une fois, c'est de nous concentrer sur le vrai problème. Dans notre quotidien, il est toujours difficile de cerner le vrai problème et d'affecter les bonnes ressources aux marchandises et aux personnes qui présentent un risque élevé. C'est un problème de tous les jours.

Notre programme est excellent. Les recommandations du vérificateur général contribueront à l'améliorer. Je suis convaincu que nous répondrons aux attentes et que nous pourrons dire aux Canadiens ce qu'on attend de nous, que nous y répondons et que nous protégeons le Canada.

Senator White: I apologize for being late as well. Thanks to both of you for being here.

When I listen to the discussions around CBSA, I always end up with a fish or fowl discussion because really, in the past decade and a bit, CBSA has moved from being a revenue or taxation department to being a police agency in this country, protecting our borders, as you just said, and I do appreciate that. But really, we haven't moved to the level of being a true police agency. Firearms, from my perspective, being carried by uniformed personnel in every location, and the ability, when in pursuit, to actually pursue rather than have to hand off to another police agency — those pieces may sound like they don't matter much to some of the public. After October 22, I know Calgary airport became an issue even for us, even with our own union.

Do you see us getting to a point where you become a police agency, one of the largest in the country? If you do, then oversight is obvious. Every police agency, all 198 of them, give or take — whatever number we have — would have an oversight body. Do you see that being the end game for CBSA, becoming a large police agency protecting our borders?

Mr. Bolduc: Maybe I can start and then let my colleague weigh in. Thank you for the question.

The arming initiative for CBSA was introduced in 2006, following a decision made by the government. As Caroline mentioned, we are at the end of that 10-year period, having close to 6,400 officers armed out of close to 7,000. So the ratio is fairly significant.

The biggest change that came with the side arm was a change in the culture of the organization and, to your point, becoming a recognized law enforcement organization that is armed.

Right now we draw our authorities from the Customs Act and the Immigration and Refugee Protection Act, which stipulate that we have authorities at ports of entry, and on some occasions inland, when we're talking about our inland enforcement activities.

Do I see a future in five, six, seven years where CBSA will be recognized as having authorities at POEs but also outside of POEs? I would think that it would be the normal evolution of an organization. Again, there are certain challenges that come with that, but I'm pleased daily — and Caroline hears that from colleagues — that we hear feedback. I think we're a valued partner from the RCMP but also from other law enforcement organizations.

Maybe, Caroline, you want to add to that.

Ms. Xavier: I don't have much more to add. The bottom line is that although we may not have the series of authorities that you talked about, at this point in time we feel quite satisfied with the authorities that we have to be able to do the job that's been assigned to us by this government in terms of where we land with the Customs Act, the CBSA Act and IRPA.

Le sénateur White : Toutes mes excuses, moi aussi, pour mon retard. Je vous remercie tous les deux d'être ici.

Toutes ces discussions sur votre agence, elles se terminent toujours dans une espèce de flou, parce que, en vérité, depuis au moins une dizaine d'années, votre agence est passée de vache à lait, qui rapportait des recettes et des taxes, à chien de garde de nos frontières, comme vous venez de le dire, et je comprends. Mais, en réalité, elle n'est pas parvenue à devenir un véritable organisme policier. D'après moi, une partie du public ne semble pas faire grand cas de la présence, partout, d'agents armés en uniforme et de leur capacité de courir après les individus plutôt que de le faire faire par une autre police. Après le 22 octobre, je sais que l'aéroport de Calgary est devenu un problème même pour nous, même avec notre propre syndicat.

Nous voyez-vous parvenir au point où vous devenez un organisme policier, l'un des plus importants du pays? Si oui, la question de la surveillance est évidente. Toutes les polices, les 198, plus ou moins — quel qu'en soit le nombre — auraient un organisme de surveillance. Voyez-vous que la finalité, pour l'agence, est de devenir une grosse organisation policière chargée de protéger nos frontières?

M. Bolduc : Je vous donnerai un premier élément de réponse, puis ma collègue interviendra. Je vous remercie pour la question.

L'initiative visant à armer les agents de l'ASFC remonte à 2006, par décision du gouvernement. Comme Caroline l'a dit, nous arrivons à la fin de cette décennie, au cours de laquelle nous avons armé près de 6 400 agents sur près de 7 000. Il s'agit donc d'un rapport assez important.

Le changement concomitant le plus important a touché la culture de l'organisation qui, comme vous dites, est devenue une organisation policière reconnue, dont les agents sont armés.

Actuellement, nous tirons nos pouvoirs de la Loi sur les douanes ainsi que de la Loi sur l'immigration et la protection des réfugiés, qui nous accordent nos pouvoirs aux points d'entrée et, en certaines occasions, à l'intérieur du pays, quand il s'agit de nos activités d'exécution de la loi dans les bureaux intérieurs.

Est-ce que j'entrevois, d'ici sept ans, pour l'Agence, la reconnaissance de ses pouvoirs aux points d'entrée, mais, aussi, ailleurs? Je pense que ce serait une évolution normale. Encore une fois, cette évolution s'accompagne de certains défis, mais, chaque jour, je suis heureux d'entendre des réactions, et Caroline en reçoit des collègues. Je pense que nous sommes un partenaire estimé de la GRC, mais aussi des autres organisations chargées de l'application de la loi.

Peut-être, Caroline, que vous voulez en dire plus à ce sujet.

Mme Xavier : Il me suffira de dire que, en somme, même si nous n'avons pas la série de pouvoirs dont vous parlez, nous sommes actuellement tout à fait satisfaits de ceux que nous avons pour nous acquitter du travail qui nous a été confié par le gouvernement pour l'application de la Loi sur les douanes, celle qui régit notre agence et la Loi sur l'immigration et la protection des réfugiés.

We have, however, really progressed in terms of our reputation and our ability to add value with our law enforcement partners, at both the federal and the provincial levels. We are recognized as well internationally with regard to our international network and the role we play in continuing to manage the safety of our country.

Senator White: Thank you very much for that. I'm telling you that you actually have increased your credibility with police agencies as you've changed your role, for sure.

As we're moving to discussions around more pre-clearance, obviously there will need to be the ability to perform more functions or different functions in a pre-clearance perspective 500 kilometres from the border, for example, if we ever get into, at some point, sea containers or railway. Then you're not at a POE anymore. You will have to change some of those functions anyway. Would you agree, Mr. Bolduc?

Mr. Bolduc: I think we'll need to engage with the U.S. as to what will be the authorities, similar to what U.S. Customs and Border Protection has when they operate in Canada, as you know. With some of the enforcement activities that they take, they call in either CBSA or the local police jurisdiction. I see a model that could operate very similarly if one day we end up operating out of the U.S.

Senator L. Smith: Just looking at your report, could you give us a summary of what learnings you went through with the Syrian refugee program, especially in terms of your interpersonal relationships, the horizontal relationships within other departments of the government? What did you learn, if there are two or three things?

There was an earlier question to you, Ms. Xavier, about the deaths of people and what the learnings were. You never really told us any learnings. It would be helpful it you could tell us a couple of your key learning points that are not confidential to you but that are good for us to understand in terms of the government, in terms of value for money, making sure that we do the right thing, et cetera, with people who come into our country.

Ms. Xavier: As you know, the steering initiative was led by our colleagues at the Immigration Department. I would say one of the key learnings is the fact that we worked extremely well on a joint initiative in a horizontal manner and in a very collaborative manner.

Senator L. Smith: What was it? Be specific. What was your role?

Ms. Xavier: Our role was specifically ensuring that those who would be landing here as permanent residents were, first of all, cleared appropriately from the get-go overseas. We played a role there with our international network, providing support to our immigration visa officers, giving them guidance on the questions they were asking of the refugees, as well as facilitating them

Cependant, notre réputation et notre valeur ajoutée pour nos partenaires dans l'application de la loi, tant fédéraux que provinciaux ont réellement augmenté. Nous sommes aussi reconnus à l'étranger, à cause de notre réseau international, et pour notre rôle dans le maintien de la sécurité de notre pays.

Le sénateur White : Je vous en remercie énormément. Je vous le dis, vous avez vraiment augmenté votre crédibilité auprès des organisations policières, en modifiant votre rôle. C'est certain.

Alors que nous nous dirigeons vers des discussions sur le prédédouanement, il faudra, manifestement, pour cette opération, vous acquitter de plus de fonctions ou de fonctions différentes, à 500 kilomètres de la frontière, par exemple, si jamais, vous vous occupez, un jour, de conteneurs maritimes ou de chemins de fer. Dans ce cas-là, on n'est plus à un point d'entrée. De toute manière, vous devrez changer certaines de ces fonctions. N'êtes-vous pas d'accord, monsieur Bolduc?

M. Bolduc : Je pense que nous devrons, avec le concours des Américains, cerner les sources de nos pouvoirs, comme ceux que détiennent leurs services homologues lorsqu'ils sont en mission au Canada, comme vous le savez. Pour certaines de leurs activités d'exécution de la loi, ils appellent soit notre agence, soit les polices locales. Je vois un modèle qui pourrait fonctionner de manière très semblable si, un jour, nous nous retrouvons en mission aux États-Unis.

Le sénateur L. Smith : Pourriez-vous nous résumer les leçons que vous avez retenues, d'après votre rapport, à la faveur du programme pour les réfugiés syriens, particulièrement en ce qui concerne les relations interpersonnelles, les rapports horizontaux avec d'autres ministères fédéraux? Quelles sont les deux ou trois leçons que vous avez retenues?

Madame Xavier, on vous a posé une question, plus tôt, sur les mortalités et les leçons que vous en avez retenues. Vous ne nous avez jamais vraiment parlé de ces leçons. Il serait utile que vous en mentionniez quelques-unes, qui ne sont pas confidentielles, du genre de celles qu'il serait bon pour nous de comprendre, au niveau de l'État, pour l'optimisation des dépenses, l'assurance, pour nous, d'avoir pris la bonne décision, et cetera, pour les personnes que nous accueillons dans notre pays.

Mme Xavier : Comme vous le savez, l'élan est venu de nos collègues à l'Immigration. L'une des principales leçons retenues est celle de l'efficacité de notre excellente collaboration horizontale à une initiative commune.

Le sénateur L. Smith : De quoi s'agit-il? Soyez précise. Quel a été votre rôle?

Mme Xavier : Notre rôle précis était de nous assurer que ceux qui arriveraient ici étaient, dès le début, autorisés à l'étranger à venir ici. Nous avons joué un rôle, avec notre réseau international, en appuyant nos agents chargés des visas d'immigration, en les orientant sur les questions à poser aux réfugiés et en facilitant l'embarquement, dans les avions en partance pour le Canada, des

aboard airplanes, ensuring that those who started the process were exactly the same people who would be boarding the airplane to Canada. So from an identity management perspective, the whole multi-layered security screening apparatus was primarily managed through the CBSA, working in collaboration with our colleagues in the portfolio.

At the ports of entry, our role was ensuring their arrival and finalizing the screening process, just as we would with any other arriving passenger, and so completing the permanent residency application process at the ports of entry.

As you know, the process took place at two ports of entry, primarily: Montreal and Toronto. From that, we'll continue to have a role with any incidences with regard to post-arrival if any of those situations arise.

I'd say the primary learning is the fact that our role in being able to bring people from overseas and then managing the whole multi-layered approach of security screening was one that the CBSA did very well, and we were seen as working well with international partners and other government departments. We were seen as having a very good leadership role in that perspective.

We learned as well that there are ways in which we can continue to streamline our security screening process but in a manner to ensure that we're not compromising it. I can assure you that was not the case, and we took that role quite seriously.

Another lesson I would mention is just the fact that we were able to mobilize quickly by bringing people across the country, because we did have to add more assets in Toronto and Montreal to be able to continue to meet the day-to-day mandate we were performing in the normal business of those ports of entry, as well supplementing in order to be able to meet the magnitude of people we were bringing in. At a national level, we mobilized really quickly and worked again in collaboration with colleagues here in Canada as well as with those overseas.

Senator L. Smith: These are all your people that you moved from one part of the country to the other in order to handle this?

Ms. Xavier: Correct.

Senator L. Smith: President Obama said he felt better because Donald Trump in his speeches was saying he wouldn't allow Syrian refugees to come in. It was controversial. In the papers, the President said that he felt better with the implication of his border services people working with our people to make sure that whatever extra screening or work that was done gave confidence that the people we were allowing in were mostly good people. Could you comment on that? What was that all about?

Ms. Xavier: As part of the security screening process, one of the things we do is check against a variety of databases: immigration, law enforcement, national security screening databases. Those databases included some of our own as well as those of the U.S., for example.

mêmes personnes exactement que celles qui avaient entamé le processus. Pour le contrôle des identités, tout le dispositif de contrôle préliminaire de la sécurité à plusieurs niveaux était principalement géré par l'entremise de l'ASFC, en collaboration avec nos collègues du portefeuille.

Aux points d'entrée, notre rôle était de nous occuper de leur arrivée et de finaliser le processus d'enquête tout comme nous le faisons pour tout autre passager qui arrive. Il s'agissait donc de compléter le processus de demande de résidence permanente aux points d'entrée.

Comme vous le savez, cela s'est fait à deux points d'entrée, soit Montréal et Toronto. Nous allons continuer de jouer un rôle dans toutes les situations qui pourraient se présenter après l'arrivée.

Je dirais que la première chose à souligner, c'est que l'ASFC s'est très bien acquittée de son rôle qui est de recevoir des gens de l'étranger et de gérer toutes les dimensions des enquêtes de sécurité. L'ASFC a été perçue comme étant capable de bien travailler avec les partenaires étrangers et avec les autres ministères gouvernementaux. On a estimé qu'elle avait très bien joué son rôle de leader dans cette perspective.

Nous avons aussi appris que nous pouvons encore continuer de simplifier notre processus d'enquête de sécurité sans pour autant le compromettre. Je vous assure que nous ne l'avons pas compromis et que nous prenons ce rôle très au sérieux.

Je dirais que nous avons aussi appris que nous pouvons nous mobiliser rapidement en amenant des gens de partout au pays, car nous avons dû augmenter les ressources à Toronto et à Montréal pour pouvoir continuer de nous acquitter de notre mandat normal dans ces points d'entrée, en plus d'ajouter les ressources requises pour recevoir les très nombreuses personnes qui arrivaient. À l'échelle nationale, notre mobilisation a été rapide et nous avons encore là travaillé en collaboration avec nos collègues ici au Canada ainsi qu'à l'étranger.

Le sénateur L. Smith : Ce sont tous vos gens que vous avez déplacés d'une partie du pays à l'autre pour s'occuper de cela?

Mme Xavier : Oui.

Le sénateur L. Smith : Le président Obama a dit qu'il se sentait mieux, parce que Donald Trump disait dans ses discours qu'ils ne permettraient pas l'arrivée de réfugiés syriens. C'était matière à controverse. Dans les journaux, on a pu lire que le président avait dit se sentir soulagé à l'idée que les gens de ses services frontaliers coopéraient avec nos gens pour que le travail d'enquête supplémentaire donne aux gens l'assurance que nous ne laissions entrer que de bonnes personnes. Pouvez-vous me parler de cela? De quoi s'agissait-il au juste?

Mme Xavier : Dans le cadre du processus de contrôle, nous faisons entre autres des vérifications dans diverses bases de données visant notamment l'immigration, l'exécution de la loi et la sécurité nationale. Il s'agit de bases de données canadiennes ainsi que de bases de données américaines.

If we had any questions with regard to somebody we were processing, that case was either set aside because they required additional information; or, again, if we needed to get additional information, there was the possibility of working directly with the U.S., for example, on a particular case. But in most cases, anything that required additional information, with the amount of time we were working under, was exactly set aside and not processed at that point in time.

Senator L. Smith: What's the number one issue that came up during this process of screening that was a challenge to you? Was it the volume? Was it the time frame? What was the number one problem or challenge that you faced that you were able to successfully overcome?

Ms. Xavier: I would say it's the time aspect. To your point, it wasn't that it wasn't overcome. We found a strategy, which is basically that where it needed to take more time, we needed to set it aside to take the time it needs. I think that was a very valuable lesson learned, and the manner in which you can process things quickly, but at the end of the day, you need to go back to the case and do the due diligence. I think that would be the number one challenge.

Mr. Bolduc: You asked, senator, about lessons learned. I think if you put a task to the public service and you challenge them to deliver it, the public service can do extraordinary things. I think it was a real Team Canada effort from all departments that were involved.

The Chair: Colleagues, I just want to follow up on a couple of questions. I want to get back to the recommendations we had in the report that all interviews be done with audio and recordings and that recordings be retained for a period of 10 years.

If I'm not mistaken, Ms. Xavier, you responded that there was some audio and maybe some video. Could you tell me why you have objections to this particular recommendation? Because it would seem to me that this recommendation is very common sense that in this day of technology there be a recording of events so that there's no question, as we've had in the past, that what took place actually did take place. Can you tell me if you are looking at implementing this recommendation, and if you're not, can you tell us why?

Ms. Xavier: I want to start out by saying there is no objection to the recommendation. Audiovisual cameras are actually in place across all of our ports of entries.

The Chair: I know that.

Ms. Xavier: The issue isn't that the visual aspect is not going to be there. It's sometimes that the audio aspect isn't. We only do audio primarily in interviews, as you were recommending. Audio is not on, for example, in all ports of entry. In the airports, you're

Si nous avions des questions à propos d'une personne dont nous traitions le dossier, nous mettions le dossier de côté en vue d'obtenir de l'information supplémentaire, et nous avions la possibilité de nous adresser directement aux services américains pour obtenir l'information sur des cas particuliers. Cependant, dans la plupart des cas, parce que le temps que nous avions était limité, tous les dossiers pour lesquels il nous fallait de l'information supplémentaire étaient mis de côté et nous ne les traitions pas à ce moment-là.

Le sénateur L. Smith : Quel a été le problème numéro un — votre principal problème —, pendant le processus de contrôle? Était-ce le volume? L'échéancier? Quelle a été la principale difficulté que vous avez rencontrée et que vous avez réussi à surmonter?

Mme Xavier : Je dirais que c'est la question du temps. Et ce n'est pas que nous n'ayons pas réussi à la surmonter. Nous avons trouvé une stratégie. En gros, s'il fallait consacrer plus de temps à un dossier, il fallait le mettre de côté et lui accorder ultérieurement le temps qu'il fallait. Je pense que c'est une leçon très utile que nous avons tirée de cela, car c'était la façon de traiter les dossiers rapidement. Cependant, au bout du compte, il faut revenir au dossier et le traiter avec la diligence nécessaire. Je pense que c'est la principale difficulté.

M. Bolduc : Sénateur, vous nous avez demandé quelles leçons nous avions apprises. Je pense que si vous mettez la fonction publique au défi d'accomplir une tâche, la fonction publique peut faire des choses extraordinaires. Je pense que tous les ministères concernés ont conjugué leurs efforts pour former une vraie Équipe Canada.

Le président : Mesdames et messieurs, j'aimerais revenir sur certaines questions, notamment sur les recommandations de notre rapport voulant que toutes les entrevues soient enregistrées et fassent l'objet d'enregistrements audio, et que les enregistrements soient conservés pendant 10 ans.

Si je ne me trompe pas, madame Xavier, vous avez dit qu'il y avait des enregistrements audio et peut-être vidéo. Pourriez-vous me dire pourquoi vous avez des réserves par rapport à cette recommandation? Il me semble que cette recommandation est très sensée, avec la technologie de nos jours, et que l'enregistrement d'événements nous permet de savoir, sans devoir nous poser de questions, ce qui s'est effectivement produit dans le passé. Pouvez-vous me dire si vous envisagez de mettre cette recommandation en œuvre, et sinon, pourquoi ne le feriez-vous pas?

Mme Xavier : Je vais commencer par dire qu'il n'y a aucune objection à cette recommandation. Il y a en fait des caméras audiovisuelles dans tous nos points d'entrée.

Le président : Je le sais.

Mme Xavier : Le problème, ce n'est pas que l'aspect visuel ne sera pas là, mais plutôt que l'aspect audio n'y est pas. Nous faisons principalement l'enregistrement audio seulement des entrevues, comme vous l'avez recommandé. Il n'y a pas d'audio

not picking up private conversations of individuals. So we try to be very particular and specific as to where some of the features are turned on with regard to our audiovisual equipment.

You're absolutely right. We do use this technology to ensure as much as possible the factual instances of what's happened. It's just that in certain cases, depending on where you are, you may only have the visual and not the audio, but in the secondary interviews, audio is at the very least there, and in most cases both exist.

The Chair: I hate to get right down to this, but why isn't it mandatory to have video along with the audio for the secondary? It is in a stationary place. As I understand, it's generally an office where you have a private conversation, but at the same time it has implications for the individual and for the CBSA. It would seem to me that for your protection and their protection it should be mandatory because then you have a record. Perhaps you could come back to us at another time and let us know how you're updating and seeing if that can be done, because it's not a lot of expense.

Ms. Xavier: Just so you know, it is part of our infrastructure renewal, as we're going throughout our ports of entry, to ensure that where there is supposed to be audio and visual, there is. I don't want to leave you with the impression that it's not something that we're seriously doing. In some cases, it's part of the infrastructure renewal of those ports of entry.

The Chair: You meant seriously not doing?

Ms. Xavier: Sorry?

The Chair: You're seriously doing or seriously not doing?

Ms. Xavier: No, we are seriously doing. Did I say "not"? Sorry.

The Chair: I'm not quite sure how that was interpreted. At any rate, we can expect to see the visual aspect implemented over time; is that right?

Ms. Xavier: Correct.

Senator Day: What is your total budget annually?

Mr. Bolduc: It is $1.87 billion fiscal that will come to an end at the end of March.

Senator Day: Are you not anticipating any difference in the appropriation for fiscal 2016-17?

dans tous les points d'entrée. Dans les aéroports, il n'est pas possible de saisir les conversations entre les personnes. Nous essayons par conséquent d'être très attentifs et précis concernant l'équipement audiovisuel qui est en fonction.

Vous avez tout à fait raison. Nous utilisons cette technologie pour veiller autant que possible à obtenir un enregistrement des faits qui se produisent. Cependant, dans certains cas, selon l'endroit où vous vous trouvez, il se peut que vous n'ayez que le visuel, et non l'audio. Les entrevues secondaires, elles, font au moins l'objet d'un enregistrement audio, et dans la plupart des cas, il y a des enregistrements audio et vidéo.

Le président : Je déteste passer directement à cela, mais pourquoi l'enregistrement vidéo n'est-il pas obligatoire avec l'audio, pour les entrevues secondaires? Elles se passent dans un lieu fixe, d'après ce que je comprends, dans un bureau où la conversation se tient en privé, mais il y a en même temps des incidences pour le particulier et pour l'ASFC. Il me semble que cela devrait être obligatoire, pour votre protection et pour celle de la personne, parce que l'entrevue serait enregistrée. Vous pourriez revenir à une autre occasion afin de nous dire comment vous envisagez de vous organiser pour que cela soit fait, parce que ce n'est pas une grande dépense.

Mme Xavier : À titre d'information, cela fait partie du renouvellement de notre infrastructure de veiller à ce que dans tous nos points d'entrée, il y ait l'enregistrement audio et vidéo là où il le faut. Je ne veux pas vous donner l'impression que ce n'est pas quelque chose que nous faisons avec sérieux. Dans certains cas, cela se fait dans le cadre du renouvellement de l'infrastructure dans ces points d'entrée.

Le président : Que vous ne faites pas avec sérieux, vous voulez dire?

Mme Xavier : Pardon?

Le président : Que vous le faites avec sérieux, ou que vous ne le faites pas avec sérieux?

Mme Xavier : Non. Nous le faisons avec sérieux. J'ai dit « pas »? Désolée.

Le président : Je ne sais pas exactement comme cela a été interprété. Quoi qu'il en soit, nous pouvons nous attendre à ce que l'enregistrement vidéo soit mis en place avec le temps. C'est bien cela?

Mme Xavier : Oui.

Le sénateur Day : Quel est votre budget annuel total?

M. Bolduc : Il est de 1,87 milliard de dollars pour l'exercice se terminant à la fin de mars.

Le sénateur Day : Ne prévoyez-vous pas une différence dans les crédits pour l'exercice 2016-2017?

Mr. Bolduc: We have a few budget items that are sunsetting, and I think we will be watching tomorrow afternoon to see if we're referenced in the budget, but overall I think there's a slight decrease in the next fiscal. Unfortunately, I don't have the budget.

Senator Day: We can look that up. What about the total number of personnel at the Canada Border Services Agency?

Mr. Bolduc: We don't expect any significant changes to the personnel we have, which is roughly 14,000.

Senator Day: And you said 7,000 of those carry firearms now or will?

Ms. Xavier: Seven thousand of them are uniformed personnel, and, yes, the large majority of them will have a firearm in their possession.

Senator Day: The people who collect tariffs at the border and those who run the VACIS machine, the X-ray machine that looks into trucks and other things that you run through, are in uniform, but do they carry firearms?

Mr. Bolduc: Yes.

Senator Day: They do now. Just a general question on equipment, this committee visited a Border Services post in New Brunswick a number of years ago, and when I say the VACIS machine, I'm using terminology that you understand, but maybe our listeners don't.

Mr. Bolduc: Giant X-ray machine.

Senator Day: A big X-ray machine that you can drive around different places, and it was being shared between the police force and Border Services, I presume, because of lack of equipment in each, so they have to share it.

How are you coming with your technology now and the implementation of new technology?

Mr. Bolduc: Well, we operate our own VACIS machines, which are located strategically along ports at the land border and in marine ports, as you know. We're always looking for new technology, leveraging what other border organizations are doing, for example, the U.S., the U.K. and others.

I think we have a decent panoply of tools that we can use, but what's interesting these days is that what was the latest or the most updated machine two years ago, because of the evolution, you need to keep pace. So we have our own lab with people whose day-to-day activities are looking at the new technology and what could be useful to our front line.

M. Bolduc : Nous avons quelques postes budgétaires visant des programmes qui arrivent à leur terme, et je pense que nous allons voir demain si on parle de nous dans le budget, mais dans l'ensemble, je pense qu'il y a une légère baisse pour le prochain exercice. Malheureusement, je n'ai pas le budget.

Le sénateur Day : Nous pourrons regarder. Qu'en est-il du nombre d'employés à l'Agence des services frontaliers du Canada?

M. Bolduc : Nous ne nous attendons pas à des changements importants dans notre effectif actuel de quelque 14 000 employés.

Le sénateur Day : Et vous avez dit que 7 000 d'entre eux portent en ce moment ou porteront une arme à feu?

Mme Xavier : Sept milles d'entre eux sont des employés qui portent un uniforme et, oui, la grande majorité d'entre eux auront une arme à feu.

Le sénateur Day : Les personnes qui perçoivent les tarifs à la frontière et celles qui utilisent l'appareil VACIS servant à inspecter les véhicules et tout ce qui passe à la frontière par radioscopie sont en uniforme, mais est-ce qu'elles ont une arme?

M. Bolduc : Oui.

Le sénateur Day : Maintenant, oui. J'ai une question générale à propos de l'équipement. Notre comité a visité un bureau des services frontaliers au Nouveau-Brunswick, il y a plusieurs années, et quand je parle de l'appareil VACIS, j'utilise la terminologie que vous comprenez, mais peut-être pas les gens qui nous écoutent.

M. Bolduc : Appareil radioscopique géant.

Le sénateur Day : Un gros appareil radioscopique que vous pouvez déplacer et que se partageaient la police et les services frontaliers, je pense, en raison du manque d'équipement de chacun.

Comment vous organisez-vous avec votre technologie en ce moment et avec la mise en œuvre de la nouvelle technologie?

M. Bolduc : Eh bien, nous utilisons nos propres appareils VACIS, stratégiquement placés aux points d'entrée se trouvant à la frontière terrestre et dans les ports maritimes, comme vous le savez. Nous sommes toujours à l'affût de la nouvelle technologie et regardons ce que les autres services frontaliers font, entre autres ceux des États-Unis et du Royaume-Uni.

Je crois que nous avons une panoplie décente d'outils que nous pouvons utiliser, mais je pense que ce qui est intéressant, de nos jours, c'est que même si vous aviez la machine la plus nouvelle ou à jour il y a deux ans, vous devez garder la cadence en raison de l'évolution. Nous avons donc notre propre laboratoire où des gens s'emploient au jour le jour à regarder la nouvelle technologie et à explorer ce qui pourrait être utile à nos agents en première ligne.

Senator White: I talked about after October 22. I know there were issues at the Calgary airport as a result of the union pulling officers off the line, as I understand it. Can you confirm that, and tell us what you have actually solved so that it doesn't occur again?

Ms. Xavier: I think what you're referring to is a possible work refusal. Is that what you're referring to?

Senator White: I understand the union actually told their employees not to go on the line because they weren't carrying side arms.

Ms. Xavier: I won't speak to the specific union's direction to their officers. What I can tell you is that we continue to actively work with the union as well as our staff specifically in Calgary or all our other ports of entry to ensure that they have the necessary tools to do their jobs. We try to ensure that where there needs to be the side arm, they are properly certified and equipped to do so.

At this point in time, the side arm is not used in our terminal airports, as per the direction of the implementation, so for the time being, only those who are at other ports of entry and other modes are permitted to carry their side arm.

Senator White: Can you provide us with a list of how many refusals you've had over the past 36 months so that we can look at it and see whether we should be making recommendations?

Ms. Xavier: We can. I don't think we've had very many, actually. I think that might have been the only one.

Senator Mitchell: At the very bottom of page 5 of your presentation, Mr. Bolduc, and at the top of page 6, you mentioned that you've removed more than 11,000 people deemed inadmissible to Canada, with a priority on those with criminality. This was last year. You also mentioned earlier in the paragraph that it has to do with those who may pose a threat to our security.

Are you returning people whom you suspect of terrorist intent, or are you returning people who have criminal records? If you were returning people whom you suspect of terrorist intent, what steps would you take to make sure that they're not let loose when they return from wherever it is they came from?

Mr. Bolduc: We remove people who are deemed inadmissible to Canada. This can be for national security concerns, criminality, misrepresentation or other reasons. We essentially detain for four reasons. When we decide to effect an arrest and send the people into detention, either there's a flight risk, so we believe they will not show up for the rest of the proceedings; we don't know who they are, so we've got people showing up at a POE and we cannot confirm their identity; we believe they represent a risk for national

Le sénateur White : J'ai parlé de ce qui a suivi le 22 octobre. Je sais qu'il y a eu des problèmes à l'aéroport de Calgary quand le syndicat a retiré des agents de la ligne, d'après ce que je comprends. Pouvez-vous nous confirmer cela et nous dire si vous avez résolu la situation pour que cela ne se reproduise pas?

Mme Xavier : Je pense que vous parlez d'un refus de travailler. Est-ce bien le cas?

Le sénateur White : Ce que j'ai compris, c'est que le syndicat a dit aux employés de ne pas aller sur la ligne parce qu'ils ne portaient pas d'arme de poing.

Mme Xavier : Je ne vais pas parler de la directive du syndicat aux agents. Ce que je peux vous dire, c'est que nous continuons de travailler activement avec le syndicat et avec notre personnel de Calgary en particulier et de tous nos autres points d'entrée en général afin de veiller à ce qu'ils aient les outils nécessaires pour faire leur travail. Nous essayons de veiller à ce que ceux qui ont besoin d'une arme de poing aient la certification nécessaire et soient convenablement équipés.

En ce moment, l'arme de poing n'est pas utilisée dans nos terminaux d'aéroports, conformément à l'orientation de la mise en œuvre. Donc, pour le moment, seuls les employés qui sont à d'autres points d'entrée pour d'autres modes ont le droit de porter une arme de poing.

Le sénateur White : Pouvez-vous nous donner une liste donnant le nombre des refus au cours des 36 derniers mois, de sorte que nous puissions l'examiner et voir si nous devons faire des recommandations?

Mme Xavier : Oui. Je ne pense pas que nous en ayons eu beaucoup, en fait. Je pense que cela a été le seul cas.

Le sénateur Mitchell : Vers le milieu de la page 6 de votre exposé, monsieur Bolduc, vous dites que vous avez renvoyé plus de 11 000 personnes jugées interdites de territoire au Canada, en renvoyant en priorité les personnes ayant commis des actes criminels. C'était l'année passée. Vous avez aussi mentionné plus haut dans ce même paragraphe que ce sont les personnes qui pourraient constituer une menace à notre sécurité.

Est-ce que vous renvoyez des personnes que vous soupçonnez d'avoir des intentions terroristes, ou des personnes qui ont un dossier criminel? Si vous renvoyez des personnes qui sont soupçonnées d'avoir des intentions terroristes, quelles mesures prendriez-vous pour vous assurer que ces personnes ne sont pas libérées une fois retournées là d'où elles viennent?

M. Bolduc : Nous renvoyons des personnes qui sont jugées interdites de territoire au Canada. Ce peut être pour des raisons de sécurité nationale, de criminalité, de fausses déclarations ou autres. Nous avons essentiellement quatre raisons de détenir quelqu'un. Quand nous décidons de faire une arrestation et d'incarcérer quelqu'un, nous le faisons parce qu'il y a un risque de fuite, et nous croyons que la personne ne se présentera pas en cour pour les procédures; parce que nous ne savons pas qui est la

security; or they've been deemed part of a mass arrival as designated by the Minister of Public Safety. Those are the four grounds why we detain people.

When we say that we removed 11,000, the priority is always on the criminals. That's the first tranche of people we will focus on. The rest of the people that have been removed are people who have been deemed by the Immigration and Refugee Board as being inadmissible to Canada.

The Chair: Back in 2013, just under 17,000 individuals were deemed inadmissible by CBSA. In 2014, there were 44,000 inadmissible individuals who did not comply with removal orders. As far as you know, they did not leave the country. They could still be here. We were also told it takes the CBSA an average of 85 days to remove a person found inadmissible. My notes say that CBSA's lookout system contains more than 19,000 outdated lookout records.

Could you update us with respect to the number of people who were deemed to be inadmissible, who stayed in the country, even though they were asked to leave, and whom you have now identified and then removed from the country? How successful are we in removing these people?

Mr. Bolduc: I believe we are successful. The numbers have been decreasing year over year because the inventory is becoming more and more difficult to manage. To be able to remove someone, we need a travel document issued by the country of which that person is a citizen. Sometimes there is difficulty in obtaining travel documents.

The Chair: Meaning they don't want to accept them back?

Mr. Bolduc: Meaning they don't want to issue a travel document for us to be able to remove them back.

The Chair: They don't want to accept them?

Mr. Bolduc: For some they don't accept them. For other countries, it's being able to confirm their identity and that they're citizens of country X, Y and Z. That's a major obstacle.

As for the warrants you referred to, our latest count is 46,000 warrants have been issued. These are people who have not shown up for proceedings with the CBSA. It's been announced that we will be introducing entry/exit to help us manage that number. Right now, somebody could be scheduled for an interview with a CBSA officer, not show up for the interview, and we issue an arrest warrant. We enter the arrest warrant into CPIC, and the person can voluntarily decide to leave the country without us knowing about it. Until we have proof that the person left the country, the warrants remain open. So entry/exit will help us manage that, and hopefully we'll be able to reduce that number.

personne, car des gens se présentent au point d'entrée et nous ne pouvons vérifier leur identité; parce que nous croyons qu'elle présente un risque pour la sécurité nationale ou qu'elle arrive en même temps qu'un groupe nombreux de la façon désignée par le ministre de la Sécurité publique. Ce sont les quatre raisons pour lesquelles nous allons incarcérer des gens.

Quand nous disons que nous avons renvoyé 11 000 personnes, il faut préciser que les criminels sont toujours prioritaires. C'est le premier groupe de personnes auxquelles nous accordons notre attention. Les autres personnes renvoyées sont des personnes jugées par la Commission de l'immigration et du statut de réfugié comme étant interdites de territoire au Canada.

Le président : En 2013, un peu moins de 17 000 personnes ont été jugées interdites de territoire au Canada par l'ASFC. En 2014, 44 000 personnes interdites de territoires ne se sont pas conformées aux mesures de renvoi. À votre connaissance, ces personnes n'ont pas quitté le pays. Elles pourraient être toujours ici. On nous a aussi dit que l'ASFC prend en moyenne 85 jours pour renvoyer une personne jugée interdite de territoire. D'après mes notes, le système de surveillance de l'ASFC contient plus de 19 000 dossiers de surveillance désuets.

Pourriez-vous nous dire le nombre de personnes jugées interdites de territoire qui étaient restées au pays, même si on leur avait demandé de partir, et que vous avez retrouvées et renvoyées du pays? Dans quelle mesure réussissons-nous à renvoyer ces personnes?

M. Bolduc : Je crois que nous avons du succès. Les nombres diminuent d'une année à l'autre parce que l'inventaire devient de plus en plus difficile à gérer. Pour pouvoir renvoyer quelqu'un, il nous faut un titre de voyage du pays dont la personne est citoyenne. Parfois, de tels titres de voyage sont difficiles à obtenir.

Le président : En ce sens qu'ils ne veulent pas les reprendre?

M. Bolduc : En ce sens qu'ils ne veulent pas produire un titre de voyage qui nous permettrait de les renvoyer.

Le président : Ils ne veulent pas les accepter?

M. Bolduc : En effet, dans certains cas. Pour d'autres pays, c'est qu'il faut pouvoir confirmer leur identité et leur citoyenneté du pays en question. C'est un obstacle majeur.

Pour ce qui est des mandats dont vous avez parlé, le nombre le plus récent est de 46 000 mandats émis. Ce sont des personnes qui ne se sont pas présentées pour les procédures de l'ASFC. On a annoncé le projet sur les entrées et les sorties que nous mettrons en œuvre pour gérer ce nombre. En ce moment, quelqu'un peut avoir un rendez-vous avec un agent de l'ASFC et, si la personne ne se présente pas à l'entrevue, nous lançons un mandat d'arrestation. Nous saisissons le mandat d'arrestation dans le CPIC et la personne peut décider de son propre chef de quitter le pays sans que nous le sachions. Tant que nous n'avons pas la preuve du départ de la personne, le mandat demeure en vigueur. Le projet sur les entrées et les sorties nous aidera à gérer cela, ce qui, nous l'espérons, contribuera à réduire le nombre.

I would not equate the 46,000 warrants to 46,000 people that are out there without us knowing where they are. We've seen, through our CBSA wanted program, that people do leave voluntarily from Canada without informing us.

The Chair: It's still a number that perhaps we should speak to at another time.

Mr. Bolduc: I agree.

The Chair: Twenty thousand is a lot of people, individuals we may not want to have here.

Thank you very much for coming. We certainly appreciate the information you've provided to us.

Colleagues, joining us on our second panel today is Greta Bossenmaier, Chief, Communications Security Establishment Canada, Canada's electronic or signals intelligence agency.

Your mandate is to gather, analyze and report on all electronic intelligence, both national and international, that pertain to our national security here in Canada in one manner or another.

Ms. Bossenmaier was appointed Chief of the Communications Security Establishment effective February 9, 2015. Prior to her appointment, she was the Senior Associate Deputy Minister of International Development as part of the Department of Foreign Affairs, Trade and Development. Ms. Bossenmaier holds a Master of Science degree in operational research from Stanford University in California, and a Bachelor of Commerce honours degree from the University of Manitoba.

Ms. Bossenmaier, we're pleased to welcome you to this committee. This is your second appearance before us since your appointment. The last time you were here was to be part of the evidence provided for the study of Bill C-51.

We're pleased that you're able to spend an hour with us to help Canadians better understand what Communications Security Establishment Canada does and how it functions under the National Defence Act.

I understand you have an opening statement. Please begin.

[*Translation*]

Greta Bossenmaier, Chief, Communications Security Establishment Canada: Good afternoon, honourable senators.

I want to thank you for the invitation to appear before you today to talk about the work of the Communications Security Establishment and the priorities we are tackling.

Je n'établirais pas de parallèle entre les 46 000 mandats et les 46 000 personnes qui se promènent librement sans que nous sachions où elles se trouvent. Dans le cadre du programme des personnes recherchées de l'ASFC, nous avons constaté que des gens quittent volontairement le Canada sans nous en informer.

Le président : Cela reste un chiffre dont nous devrions peut-être parler une autre fois.

M. Bolduc : Je suis d'accord.

Le président : Vingt mille personnes, c'est beaucoup d'individus que nous ne voulons peut-être pas ici.

Merci beaucoup d'être venu témoigner. Nous vous sommes sans aucun doute reconnaissants des renseignements que vous nous avez fournis.

Chers collègues, pour notre deuxième panel, nous accueillons Greta Bossenmaier, qui est chef du Centre de la sécurité des télécommunications Canada, à savoir l'agence canadienne de renseignement électronique ou électromagnétique.

Votre mandat est de recueillir, d'analyser et de produire des rapports sur l'ensemble du renseignement électronique, tant à l'échelle nationale qu'internationale, se rapportant d'une manière ou d'une autre à notre sécurité nationale.

Mme Bossenmaier a été nommée chef du Centre de la sécurité des télécommunications Canada, poste qu'elle occupe depuis le 9 février 2015. Avant sa nomination, elle était sous-ministre déléguée principale du Développement international, au ministère des Affaires étrangères, du Commerce et du Développement. Mme Bossenmaier est titulaire d'une maîtrise ès sciences en recherche opérationnelle de l'Université Stanford en Californie et d'un baccalauréat en commerce, avec mention, de l'Université du Manitoba.

Madame Bossenmaier, nous sommes heureux de vous accueillir au comité. Il s'agit de votre deuxième comparution depuis votre nomination. La dernière fois que vous étiez ici, votre témoignage a été recueilli dans le cadre de l'étude du projet de loi C-51.

Nous sommes heureux que vous soyez en mesure de passer une heure avec nous pour aider les Canadiens à mieux comprendre les fonctions du Centre de la sécurité des télécommunications Canada et la façon dont il mène ses activités en vertu de la Loi sur la défense nationale.

J'ai cru comprendre que vous avez une déclaration liminaire. Veuillez commencer.

[*Français*]

Greta Bossenmaier, chef, Centre de la sécurité des télécommunications Canada : Bonjour, honorables sénateurs.

Je tiens d'abord à vous remercier de m'avoir invitée à vous parler du travail que nous accomplissons au Centre de la sécurité des télécommunications Canada, ainsi qu'à faire état de nos priorités.

Since I was appointed chief of CSE last year, I have had the opportunity to see first-hand the challenging and valuable work undertaken by our organization. I have the privilege of witnessing — on a daily basis — the professionalism, skill and determination of the women and men of CSE to help protect Canada, its people and its vital information. I am very proud of the hard work that they do, and it has indeed been a privilege to lead this organization over the past year.

By way of background, I would like to begin with what CSE does and why we do it. As you know, we have a three-part mandate under the National Defence Act.

It should be pointed out that CSE is Canada's national signals intelligence agency, and is authorized to acquire and use information from the global information infrastructure to provide for intelligence, in accordance with the intelligence priorities that the Government of Canada has identified. It is important to emphasize that CSE only targets foreign entities and communications, and in fact is prohibited by law from targeting Canadians or anyone in Canada.

[*English*]

In terms of results, our intelligence has played a vital role in supporting Canada's military operations, including the current effort in Iraq. It has helped uncover foreign-based extremist efforts to attract, radicalize and train individuals to carry out attacks in Canada and around the world. It has provided early warning to thwart foreign cyber-threats to the Government of Canada and critical infrastructure and networks. It has identified and helped defend the country against the actions of hostile foreign intelligence agencies. It has contributed to the integrity of Canada's borders and infrastructure. Finally, it has furthered Canada's national interests in the world by providing context about global events and crises, and informed Canada's decision-making in the fields of national security, defence and international affairs.

The second part of our mandate is cyberdefence and protection. CSE provides advice, guidance and services to help ensure the protection of electronic information and information infrastructures that are of importance to the Government of Canada. Our sophisticated cyber and technical expertise helps identify, prepare for and respond to the most severe cyber-threats

Depuis ma nomination au poste de chef du CST, l'an dernier, j'ai été un témoin privilégié du travail difficile, mais combien remarquable, réalisé par notre organisme. Jour après jour, j'ai le privilège de constater le professionnalisme, les compétences et la détermination dont les femmes et les hommes du CST font preuve pour protéger le Canada, les Canadiens et les renseignements essentiels. Je suis très fière du travail remarquable qu'ils accomplissent, et ce fut en effet un privilège pour moi de diriger cet organisme au cours de la dernière année.

J'aimerais d'abord vous mettre en contexte en décrivant la mission du CST, ainsi que les raisons qui la sous-tendent. Permettez-moi ainsi de rappeler que cette mission est assortie d'un mandat à trois volets, lesquels sont définis dans la Loi sur la défense nationale.

Il convient de préciser que le CST est l'organisme national canadien chargé du renseignement électromagnétique, et qu'il est autorisé à capter, ainsi qu'à utiliser les données provenant de l'infrastructure mondiale d'information, et ce, dans le but de fournir du renseignement étranger répondant aux priorités du gouvernement du Canada. En l'occurrence, je souhaiterais insister sur le fait que le CST vise uniquement les entités et les communications étrangères, et que la loi lui interdit formellement de viser des Canadiens ou des personnes se trouvant au Canada.

[*Traduction*]

En ce qui a trait aux résultats, le renseignement que nous avons produit s'est avéré d'une importance capitale pour les opérations militaires du Canada, y compris celles qui ont encore lieu en Irak. Ce renseignement a permis de mettre au jour des complots d'extrémistes étrangers qui voulaient attirer, radicaliser et entraîner des individus dans le but de perpétrer des attaques au Canada et dans d'autres régions du monde. Il a également donné lieu à des avertissements en temps opportun, lesquels ont permis de contrer des cybermenaces étrangères visant le gouvernement du Canada ainsi que les infrastructures et les réseaux essentiels. De plus, ce renseignement nous donne les moyens d'identifier les actes d'hostilité de services de renseignement étrangers et de contribuer au renforcement des mesures de protection du pays. Il a d'ailleurs été un facteur déterminant dans le maintien de l'intégrité de nos frontières et de nos infrastructures. Au reste, ce renseignement a grandement servi les intérêts du Canada en fournissant des éléments contextuels sur les crises et les événements mondiaux, permettant ainsi aux intervenants canadiens de prendre des décisions éclairées en matière de sécurité nationale, de défense et d'affaires internationales.

Le deuxième volet de notre mandat porte sur la cyberdéfense et la protection. Le CST fournit des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada. Notre expertise technique sophistiquée dans le domaine de la cybersécurité nous aide à cerner et à contrer les

and attacks against computer networks and systems and the important information they contain.

We help protect Government of Canada systems from foreign states, hackers, terrorists and criminals. We track threats from around the world, and we work with government departments and agencies to strengthen and defend systems that have been compromised. We help protect information, of value to the government, including personal information, from theft.

[*Translation*]

The third part of CSE's mandate is to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties. As Canada's national cryptologic agency, CSE possesses unique expertise and capabilities. Under the assistance mandate, those capabilities may be used to assist a Canadian law enforcement or security agency to perform tasks in accordance with their legislated mandate.

The principles of lawfulness and privacy are critical to the work of CSE. Protecting Canadians' privacy is not an afterthought. It is a fundamental part of our organizational culture and is embedded within our operational structures, policies and processes. CSE has a strong privacy framework — detailed policies and procedures, as well as internal review and independent external review, in particular that of the CSE commissioner. These measures contribute to ensuring that CSE's activities are conducted in a way that protects the privacy interests of Canadians.

[*English*]

This year marks CSE's seventieth anniversary, and throughout the past 70 years, CSE has helped protect Canada and Canadians while adapting to enormous changes in the international security environment and throughout the rapidly evolving nature of communications technology. From the Cold War to ISIS, from telegraph and radios to the global Internet, the current threats to Canada and its allies, and the very nature of our work, are increasingly more complex and more diverse than ever. It's this dynamic environment that is the underlying theme of three of CSE's top priorities.

The first of those priorities is to ensure that we continue to provide timely and valuable foreign intelligence to meet the intelligence priorities of the Government of Canada. In this

cybermenaces les plus lourdes qui pèsent sur les réseaux et les systèmes informatiques, de même que sur les importantes informations que ceux-ci contiennent.

Nous aidons à protéger les systèmes du gouvernement du Canada contre les activités malveillantes de certains États, de pirates informatiques et de criminels étrangers. Nous surveillons les menaces étrangères provenant des quatre coins du globe et nous collaborons avec les ministères, aux fins de défense et de renforcement des systèmes ayant été compromis. En outre, nous aidons à protéger contre le vol l'information gouvernementale essentielle, notamment les renseignements personnels.

[*Français*]

Le troisième volet du mandat du CST consiste à fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère. En tant qu'organisme national de cryptologie du Canada, le CST possède un savoir-faire et des capacités uniques. Dans le cadre du mandat d'assistance, le CST peut mettre ses capacités à la disposition d'organismes canadiens chargés de l'application de la loi ou de la sécurité pour permettre à ceux-ci de remplir le mandat qui leur a été confié en vertu de la loi.

La notion de respect des lois et de la vie privée constitue l'un des fondements de l'œuvre du CST. La protection de la vie privée des Canadiens n'a absolument rien d'accessoire. Le respect de la vie privée des Canadiens est une partie fondamentale de notre culture organisationnelle et fait partie intégrante de nos structures, politiques et processus organisationnels. En matière de protection de la vie privée, le CST est régi par un cadre très rigoureux : des politiques et des procédures soigneusement définies, ainsi que des examens internes, sans oublier les examens externes indépendants, tout particulièrement celui du commissaire du CST. Grâce à ces mesures, nous nous assurons que le CST effectue ses activités tout en protégeant la vie privée des Canadiens.

[*Traduction*]

Cette année marque le 70e anniversaire du CST. Pendant toutes ces années, le CST a aidé à protéger le Canada et les Canadiens, tout en s'adaptant aux immenses changements qui ont marqué la sphère de la sécurité internationale et qui caractérisent la fulgurante évolution des technologies des communications. De la guerre froide à la guerre contre l'État islamique, du télégraphe et des radios au réseau Internet mondial, les menaces pesant sur le Canada et sur ses alliés — ainsi que la nature même de notre travail — sont devenues plus complexes et plus diverses que jamais. Cet environnement en constante métamorphose constitue le dénominateur commun de trois de nos principales priorités.

La première de nos priorités consiste à nous donner les moyens de fournir continuellement et en temps opportun de précieux renseignements étrangers qui répondent aux besoins du

increasingly complex international environment, the need for foreign intelligence is as critical as ever.

I will note the example I mentioned earlier: CSE's support to the government's mission in Iraq. Just as we did in Afghanistan, CSE provides vital intelligence to this mission, and we help protect Canadian troops from threats on the ground. Intelligence has been identified as an important aspect of this mission, and I'm proud that CSE will continue this contribution as the mission evolves.

Nevertheless, there are challenges that CSE must confront to remain successful. Our foreign intelligence plays an important role in countering terrorist threats to Canada; however, CSE and our allies are dealing with significant changes in recent years, not only in the operations of terrorists, but also their adoption of new and sophisticated communications technologies. For example, ISIS has demonstrated an unprecedented ability to take advantage of modern technology. In a very short period of time, they have leveraged the Internet to spread propaganda and to inspire and plan attacks. This has underlined our need to adapt our capabilities to the rapid changes in technology and our adversaries' use of them.

The next priority for CSE that I'd like to address is an increased emphasis on cybersecurity: protecting, defending and educating to deter cyber-threats. Protecting Canada's most sensitive communications and information has been a part of CSE's business throughout our 70-year history.

While this has always been core to our mandate, the fact that more and more of the world's and Canada's government operations, business, military systems and citizens' lives are conducted online has necessitated a heightened focus on cybersecurity. The growing reliance on digital information and electronic systems by government, private industry and citizens has introduced new risk, new threats and new actors, challenging the very digital infrastructure on which Canadians rely.

The number of nation states and non-state actors that possess the capability to conduct persistent, malicious cyberoperations is growing, and Canada is an attractive target.

CSE, working alongside our government partners, is at the forefront of safeguarding information. CSE's sophisticated cyberdefence mechanisms block over 100 million malicious cyberactions against the Government of Canada every day, thus playing a critical role in safeguarding Canada's national security

gouvernement du Canada. Dans un contexte mondial qui ne cesse de se complexifier, il est devenu indispensable de se donner accès à du renseignement étranger.

Permettez-moi de rappeler l'exemple que j'ai cité plus tôt, celui concernant le soutien que le CST accorde à la mission du gouvernement en Irak. Tout comme en Afghanistan, nous fournissons du renseignement indispensable à cette mission et nous contribuons à la protection des troupes canadiennes contre les menaces qui se profilent sur le terrain. Le renseignement a été un aspect important de cette mission, et c'est avec fierté que le CST continuera d'apporter sa contribution à mesure que la mission canadienne évoluera.

En outre, le CST devra relever certains défis pour être en mesure de jouer adéquatement son rôle. Certes, le renseignement que nous fournissons est nécessaire à la défense du Canada contre les menaces terroristes. Mais, depuis un certain nombre d'années, le CST et ses alliés doivent composer avec des changements importants : les terroristes ont grandement perfectionné leurs modes d'opération et ont désormais recours à des technologies de communication sophistiquées. Par exemple, l'État islamique a démontré une capacité sans précédent à tirer avantage des technologies de pointe. En très peu de temps, il a tiré parti de l'Internet pour orchestrer sa propagande et pour planifier ses attaques. Cette conjecture nous a forcés à redéfinir nos capacités et à anticiper les changements technologiques rapides dans le but de contrer nos adversaires.

Par ailleurs, j'aimerais dire un mot sur l'importance accrue de la cybersécurité, une autre priorité capitale du CST, laquelle consiste à prévenir les cybermenaces en misant sur des mesures de protection, de défense et de sensibilisation de l'effectif. La protection des communications et des informations les plus sensibles du Canada fait partie intégrante des opérations du CST depuis 70 ans.

Et même si cet enjeu a toujours été au cœur des activités du CST, il n'en demeure pas moins que, au Canada et dans le monde, un nombre sans cesse croissant d'opérations gouvernementales, d'entreprises, de systèmes militaires et d'activités citoyennes sont tributaires de l'Internet, ce qui exige que nous intensifiions les mesures de cybersécurité. Or, le gouvernement, l'entreprise privée et les citoyens sont contraints de compter toujours davantage sur l'information numérique et les systèmes électroniques, ce qui a provoqué l'émergence de nouveaux risques, de nouvelles menaces et de nouveaux auteurs de cybermenaces, lesquels constituent un risque toujours croissant pour l'infrastructure numérique dont dépendent les Canadiens.

Le nombre d'États et d'entités non étatiques qui sont en mesure de mener des cyberopérations malveillantes et soutenues ne cesse d'augmenter et constitue une menace constante pour le Canada.

Fort d'une collaboration avec ses partenaires gouvernementaux, le CST se tient sur la ligne de front pour être en mesure de protéger adéquatement l'information. Chaque jour, les mécanismes sophistiqués de cyberdéfense du CST bloquent plus de 100 millions d'attaques malveillantes visant le

and government operations. Through CSE's educational initiatives, such as our Top 10 IT Security Actions — which I believe you have a copy of — we protect the Government of Canada's networks and information, and we help ensure that government IT professionals are informed about the latest threats and mitigation measures.

The government has also recognized that Canada's private sector and critical infrastructure, in particular those sectors at the leading edge of innovation, are also at risk of malicious cyberattacks. For this reason, CSE and its federal partners are increasingly providing cyberdefence support beyond government networks, including cyber-threat information and mitigation advice.

The third priority is to ensure that we have organizational capacity, both today and in the future, to meet the government's requirements for world-class cyberexcellence across our three-part mandate, while always upholding the highest standards of lawfulness and privacy protection, and doing all of this in an increasingly demanding environment.

[*Translation*]

This requires CSE and its people to be agile, innovative, determined and principled. That is something that we have been doing successfully for 70 years, and we will continue to do so.

[*English*]

I will conclude my opening remarks by saying that I am confident in our ability to meet these challenges, to remain resilient in the midst of significant change, to address the growing demands posed by cyber-threats, to provide timely and vital foreign intelligence to the Government of Canada and to continue to safeguard the privacy of Canadians.

My confidence stems from the professionalism and the commitment of CSE's highly skilled workforce. CSE's employees play a fundamental role in shaping our organization and capabilities and in delivering on our objectives. They are our most important asset. Their strong teamwork, their integrity and their focus on excellence are also a reflection of their commitment to public service. They are Canadians who are committed to doing the best for their country. Their dedication and skills will be instrumental to CSE's success in helping to protect Canada's

gouvernement du Canada. Il est donc clair que le CST joue un rôle essentiel en matière de protection de la sécurité nationale du Canada et des activités du gouvernement. Les initiatives éducatives du CST, comme Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information du gouvernement du Canada — je crois que vous en avez une copie —, aident à faire en sorte que les professionnels en TI du gouvernement sont au courant des plus récentes menaces et mesures d'atténuation.

Le gouvernement reconnaît en outre que le secteur privé canadien et ses infrastructures essentielles sont la cible de cyberattaques malveillantes, particulièrement dans les secteurs novateurs de pointe. C'est pourquoi le CST et ses partenaires fédéraux offrent de plus en plus de soutien en cyberdéfense, à des entités se trouvant au-delà des réseaux du gouvernement, en leur fournissant, notamment, de l'information sur les cybermenaces ou des conseils sur les mesures d'atténuation.

La troisième priorité du CST consiste à nous assurer que l'organisme dispose de capacités organisationnelles suffisantes — maintenant et à l'avenir — pour être en mesure de répondre aux demandes et aux besoins du gouvernement du Canada, lesquelles exigent que nous excellions dans les trois volets de notre mandat, tout en suivant les normes les plus rigoureuses en matière de respect des lois et de la vie privée. L'environnement dans lequel nous réalisons notre mandat est, en soi, de plus en plus exigeant.

[*Français*]

Pour être en mesure de garantir la protection de tous les Canadiens dans un environnement aussi agité, le CST et son effectif doivent se montrer souples, novateurs, déterminés et exemplaires, des attributs qui caractérisent déjà notre travail depuis 70 ans.

[*Traduction*]

Du reste, je conclurai mon allocution en réitérant ma pleine confiance en notre capacité à relever les défis qui se dressent devant nous. Nous sommes donc résolus à persévérer malgré les profonds changements; à répondre aux impératifs, toujours plus nombreux, imposés par les cybermenaces; à fournir, en temps opportun, du renseignement étranger au gouvernement du Canada; et à continuer de veiller à la protection de la vie privée des Canadiens.

Et ma confiance est absolue, car elle repose sur le professionnalisme et sur l'engagement dont fait preuve l'effectif hautement compétent du CST. Le personnel du CST est la force motrice qui définit notre organisme et nos capacités, et qui nous rend aptes à atteindre nos objectifs. Notre capital humain constitue le plus important des atouts de l'organisme. Le travail d'équipe exceptionnel de notre personnel de même que son intégrité et son souci de l'excellence n'ont d'égal que son engagement envers le service public. Nos employés sont des

national interests and security as we look forward to our next 70 years.

Again, I thank the committee for your invitation, and I welcome your questions.

The Chair: Thank you very much, Ms. Bossenmaier. I want to say that the responsibility of your organization certainly cannot be understated with respect to the responsibility you have for all Canadians.

Ms. Bossenmaier: Thank you for that, sir.

The Chair: Especially in view of the world we live in today and the global terrorist threats that are so prevalent across the world. In a letter in February 2016 you said that you detected foreign-based extremist plots against Canada and our allies. These activities are against Canada and our national interests.

Then you went on and mentioned two or three times, with respect to your opening comments, terrorism and the responsibility that you have with respect to identifying these threats, and obviously using this information when necessary and appropriate with other agencies.

Could you give a further outline of how many foreign-based extremist plots against Canada you have identified over the last five years to give us a sense of the scope of what we're dealing with here?

Ms. Bossenmaier: Thank you for the question, Mr. Chair. You're right: Communications Security Establishment Canada's foreign intelligence priorities are set by the Government of Canada. We basically work against the intelligence priorities that the Government of Canada sets for our organization and others.

The work we're doing is often in concert with other organizations that are working on foreign threats to Canada. Our role is focused on the foreign signals intelligence, looking at whatever information we can gather on foreign threats to Canada and then putting that into the mix with other intelligence that other agencies may gather.

I don't have a particular number for you, Mr. Chair, but I can tell you, as I noted in my opening remarks, that CSE's efforts have been important in dealing with and continuing to deal with these foreign threats to Canada.

The Chair: I just want to hone down on this a bit further. We're trying to get a sense of what we're dealing with here. When you open the newspaper every day, you see what's happening in

Canadiens qui, en somme, ont résolument pris fait et cause pour le Canada. Grâce à leur dévouement et à leurs compétences, le CST peut envisager les 70 prochaines années avec optimisme et mener à bien sa mission consistant à protéger les intérêts et la sécurité du Canada.

Je remercie à nouveau le comité pour son invitation et je serai heureuse de répondre vos questions.

Le président : Merci beaucoup, madame Bossenmaier. Je tiens à dire qu'on ne peut manifestement pas sous-estimer la responsabilité de votre organisme envers tous les Canadiens.

Mme Bossenmaier : Je vous en sais gré, monsieur.

Le président : C'est d'autant plus vrai compte tenu du monde dans lequel nous vivons aujourd'hui et du grand nombre de menaces terroristes qui planent aux quatre coins de la planète. Dans une lettre envoyée en février 2016, vous avez dit que vous aviez découvert des complots extrémistes d'origine étrangère visant le Canada et ses alliés. Ces activités sont menées au détriment du Canada et de nos intérêts nationaux.

Dans votre déclaration liminaire, vous avez ensuite parlé à deux ou trois reprises du terrorisme et de la responsabilité que vous avez de cerner ce genre de menaces et, de toute évidence, de communiquer à d'autres organismes l'information que vous avez recueillie, lorsque c'est nécessaire et approprié.

Pour nous donner une idée de la gravité de la situation à laquelle nous faisons face, pourriez-vous nous dire plus précisément quel est le nombre de complots extrémistes visant le Canada que vous avez découverts au cours des cinq dernières années?

Mme Bossenmaier : Merci de poser la question, monsieur le président. Vous avez raison : les priorités du Centre de la sécurité des télécommunications en matière de renseignement étranger sont établies par le gouvernement du Canada. Notre travail consiste essentiellement à s'attaquer aux priorités en matière de renseignement que le gouvernement du Canada a établies pour notre organisme et d'autres organismes.

Nous travaillons souvent de concert avec des organismes qui s'occupent d'autres menaces étrangères visant le Canada. Notre rôle consiste à mettre l'accent sur les renseignements électromagnétiques étrangers. Nous examinons toute l'information que nous pouvons recueillir au sujet de menaces étrangères visant le Canada et nous l'ajoutons ensuite au renseignement que d'autres organismes pourraient avoir recueilli.

Je n'ai pas de chiffre précis à vous donner, monsieur le président, mais je peux vous dire, comme je l'ai mentionné dans ma déclaration liminaire, que les efforts déployés par le CST ont été importants et continuent de l'être dans la lutte contre ces menaces étrangères visant le Canada.

Le président : J'aimerais approfondir un peu plus cette question. Nous essayons de nous faire une idée de la situation. Chaque jour, les journaux nous montrent ce qui se passe en

Europe, Canada and the United States. When you say you don't have a number with respect to the number of actual — I'm going to call them "plots," the activity that is occurring — is it increasing from what it was three years ago?

Ms. Bossenmaier: Mr. Chair, respectfully, I would have to suggest that that would be a good question to pose to CSIS. That organization has a responsibility to look at all threats to Canada and assess the threat information and threat perspective to Canada.

I can definitely talk to you about cyber-threats, because that is something particularly within our mandate. One of our mandates is to focus particularly on cyber-threats to the Government of Canada. In terms of cyber-threats and what we're seeing, absolutely, it's a much more dynamic environment, both the number of threats and the nature of how they materialize and how quickly, and also in terms of the different threat actors. There are now nation states, as we know. We have terrorist organizations. We have new types of cyber-threats emerging in cybercriminals.

From a cyber perspective, I can definitely answer your question in the sense of a much more dynamic environment, different types of threat actors and overall a higher pace. I think not a day goes by now that we don't open the newspaper, to your point, and read about different types of cyber-threats, whether they're in the private domain, the public sector or the business or private sector domain. It's a much more dynamic and challenging environment, I can tell you, from a cyber-threat perspective.

Senator White: Thanks for being here today. We really appreciate it.

A recent report from the U.K.'s Intelligence and Security Committee talked about whether a Chinese company should be allowed to participate in U.K. critical infrastructure. Have you had similar discussions with the Canadian government about Huawei, as an example, or other Chinese entities being involved in critical infrastructure bids?

Ms. Bossenmaier: Thank you for the question, senator. As you may know, in Canada we have an Investment Canada Act review process. Part of that is the national security review mechanism or process that can be implemented. From a CSE perspective, if we have information relevant to that national security review process, we can bring that information forward to be considered as part of that review process. The Minister of Public Safety looks at security, threats and risks overall, and that becomes part of that discussion in terms of the Investment Canada Act.

Senator White: Have you done that?

Ms. Bossenmaier: We have.

Europe, au Canada et aux États-Unis. Vous affirmez ne pas avoir de chiffre concernant le nombre de complots — je les appellerai ainsi — ou d'activités en cours, mais savez-vous si ce nombre a augmenté au cours des trois dernières années?

Mme Bossenmaier : Monsieur le président, avec tout le respect, je dirais que ce serait une bonne question à poser au SCRS. Cet organisme est chargé d'examiner toutes les menaces visant le Canada ainsi que les renseignements connexes et le danger qu'elles présentent pour le pays.

Cela dit, je peux sans aucun doute vous parler des cybermenaces, sur lesquelles porte plus précisément notre mandat. L'une de nos fonctions est de porter une attention particulière aux cybermenaces visant le gouvernement du Canada. Nous constatons que c'est un environnement beaucoup plus dynamique compte tenu du nombre croissant de cybermenaces, de la façon dont elles se matérialisent — et la rapidité avec laquelle elles sont mises en œuvre — ainsi que des différents acteurs malveillants. Nous savons qu'il est maintenant question d'États-nations. Il y a aussi les organisations terroristes. Les cybercriminels conçoivent de nouveaux types de cybermenaces.

Sur le plan cybernétique, je peux répondre à votre question en disant qu'il s'agit d'un environnement beaucoup plus dynamique compte tenu des différents types d'acteurs malveillants et de la rapidité croissante avec laquelle ils mènent généralement leurs activités. Je crois qu'il ne se passe pas une journée — pour revenir à ce que vous avez dit — sans que les journaux parlent de différents types de cybermenaces, que ce soit dans le domaine privé, le secteur public, le milieu des affaires ou le secteur privé. Sur le plan cybernétique, je peux vous assurer que c'est un environnement beaucoup plus dynamique et complexe.

Le sénateur White : Merci d'être ici aujourd'hui. Nous vous en sommes très reconnaissants.

Un récent rapport du comité du renseignement et de la sécurité du Royaume-Uni a abordé la question de savoir si une entreprise chinoise devrait être autorisée à participer aux travaux visant les infrastructures essentielles du Royaume-Uni. Avez-vous eu ce genre de discussions avec le gouvernement du Canada à propos, par exemple, de Huawei, ou d'une autre entreprise chinoise qui présente des soumissions portant sur des infrastructures essentielles?

Mme Bossenmaier : Merci de poser la question, monsieur le sénateur. Comme vous le savez peut-être, au Canada, la Loi sur Investissement Canada prévoit un mécanisme d'examen, qui porte entre autres sur les questions de sécurité nationale. Lorsque le CST a de l'information pertinente à cet égard, il peut la communiquer aux fins d'examen. Le ministre de la Sécurité publique se penche sur tout ce qui touche la sécurité, les menaces et les risques, et la question est donc abordée pendant les discussions se rapportant à la Loi sur Investissement Canada.

Le sénateur White : Avez-vous déjà procédé ainsi?

Mme Bossenmaier : Oui, nous l'avons déjà fait.

Senator White: How often? Once, twice or 10 times a year?

Ms. Bossenmaier: I don't have a number for how often we've done it, but we have done it on cases with relevance and information to bear.

Senator White: Can it be triggered by anyone else other than CSE in case you miss it? Could other bidders, the other agencies, for example, identify it as something you should do, or does it have to be triggered by you?

Ms. Bossenmaier: We're not a trigger. There are triggers within the national security review process that would cause a review to happen. We're not a bidder either, but if we have information to bring to bear that is relevant from our sector, we can bring that information to bear into the process.

Senator White: I'm just trying to figure out who would cause that to happen. For instance, could other bidders cause that to happen if they were concerned? Could outside agencies raise an issue if they thought there was some concern? I'm just trying to figure out how it gets to the stage where you actually do that.

Ms. Bossenmaier: I want to be sure I'm giving you the full information, senator. My understanding is it's a dollar threshold that may trigger certain actions, but because I'm not the party responsible for the actual review process but a contributor to it, what I would suggest is either we get back to you or have someone from Public Safety or Industry get back to you in terms of what would cause a national security review to happen.

We're a contributor to it, so I want to be sure I give you the right answer.

Senator White: You could get back to us. Thank you.

Senator Mitchell: I'm particularly interested in the issue of cybersecurity. You can see where government is probably pretty well taken care of. You mentioned that. You highlighted that in your report. We have CSIS and other agencies that are concerned about their own work, so they would be taking care of it. You also mentioned a great focus on the private sector.

What I worry about is that the private sector is quite dispersed. I don't worry about that, but I worry that, being dispersed, it would take a great deal of coordination to make sure there weren't gaps in the way in which we were protecting critical infrastructure against cyberattack.

Is there an agency within government that takes on that responsibility as the agency responsible?

Le sénateur White : À quelle fréquence? Une, deux ou dix fois par année?

Mme Bossenmaier : Je ne sais pas à quelle fréquence, mais c'est ce que nous avons fait dans les cas pertinents où nous avions de l'information qui méritait une attention particulière.

Le sénateur White : Mis à part le CST, quelqu'un d'autre peut-il enclencher le processus, au cas où vous n'auriez pas vu l'information? Les autres soumissionnaires, les autres organismes, par exemple, peuvent-ils déterminer que c'est ce que vous devriez faire, ou êtes-vous les seuls à pouvoir enclencher le processus?

Mme Bossenmaier : Nous n'enclenchons rien. Des intervenants dans le processus d'examen des questions de sécurité nationale peuvent enclencher le processus. Nous ne sommes pas soumissionnaires, mais nous avons dans notre secteur de l'information pertinente à mettre à contribution. Nous pouvons la mettre à profit dans le cadre du processus.

Le sénateur White : J'essaie seulement de comprendre qui peut intervenir pour que cela se produise. Par exemple, d'autres soumissionnaires pourraient-ils enclencher le processus s'ils sont préoccupés? Des organismes externes pourraient-ils soulever un point qui provoque une certaine inquiétude? J'essaie juste de comprendre comment vous en arrivez à procéder ainsi.

Mme Bossenmaier : Je veux être certaine de vous donner toute l'information, monsieur le sénateur. D'après ce que j'ai compris, à partir d'un certain montant, certaines mesures pourraient être prises, mais étant donné que je ne suis pas responsable du mécanisme d'examen, auquel je ne fais que contribuer, je propose que nous vous revenions là-dessus ou qu'un représentant de la Sécurité publique ou d'Industrie vous explique ce qui donne lieu à l'examen d'une question de sécurité nationale.

Nous contribuons au processus, et je veux donc être certaine de vous donner la bonne réponse.

Le sénateur White : Vous pourriez nous revenir là-dessus. Merci.

Le sénateur Mitchell : Je m'intéresse particulièrement à la question de la cybersécurité. Vous pouvez voir à quels égards le gouvernement n'a probablement aucune raison de s'en faire. Vous l'avez mentionné. Vous l'avez souligné dans votre rapport. Nous avons le SCRS et d'autres organismes qui se soucient de leur propre travail, qui s'en occupent déjà. Vous avez également parlé de la grande attention accordée au secteur privé.

Ce qui me préoccupe, c'est que le secteur privé est plutôt éparpillé. Ce n'est pas ce qui me préoccupe, mais je crains que, pour cette raison, d'énormes efforts de coordination ne soient nécessaires pour prévenir les lacunes dans la façon dont nous protégeons nos infrastructures essentielles contre les cyberattaques.

Y a-t-il un organisme gouvernemental qui assume cette responsabilité?

Ms. Bossenmaier: If I may, you made the earlier comment that it looks like we're taking care of things from the government perspective. I would provide two pieces of context around that, even from the government perspective.

The government has made a lot of progress in terms of cyberdefence. There has been a lot of emphasis on everything, from how we have structured ourselves, to bringing in the requisite players forward, to having attention put on it at the highest levels. A lot of attention has been put on the government, but I would never want anyone to be left with the sense that there is nothing left to do.

This goes back to my earlier response. It's such a dynamic environment that you can never have a laissez-faire attitude by saying we're done, we're taken care of. We always have to continue to look at new threats, new actors and new vulnerabilities. Even though the government has come a long way, we need to keep that focus and attention.

On your question with regard to the private sector, a number of years ago the government established a three-part Canada cyber-strategy. The first part of that strategy is what we've talked about, namely, protecting and securing government systems; the second pillar of that strategy focuses on supporting the private sector; and the third part of the strategy is also helping Canadian citizens directly.

The overall strategy is coordinated by the Department of Public Safety. The Department of Public Safety is the lead on that second pillar in terms of working with and supporting the private sector. To answer your question, they are the lead agency. CSE is involved in that. I'll give you perhaps two examples of our involvement, if I may, the first being from cyber-threat information. Part of our job is to look at sophisticated cyber-threats to Canada. You can get a lot of cyber-threats information from various companies, but our job is to look at the most sophisticated cyber-threats facing the country. We can share some of that cyber-threat information with the private sector.

The second piece that we do is around mitigation advice. When a cyberattack happens, a number of pieces of the system must kick into place. How do you mitigate and remedy that? We've also been providing cyber mitigation advice to the private sector. I hope that answers your question.

Senator Mitchell: Maybe you can't tell us entirely, but I would be interested in knowing how you organize it. Clearly, the banks have critical infrastructure. Clearly, pipeline companies, refineries, the energy industry have critical infrastructure, all of which is highly computerized. How do you divide up the different sectors? It would seem to me that it would take different expertise.

Mme Bossenmaier : Si je peux me permettre, vous avez mentionné plus tôt que nous semblons prendre les choses en main du côté du gouvernement. Pour situer le contexte, je vais aborder deux points qui se rapportent également à l'aspect gouvernemental.

Le gouvernement a fait beaucoup de progrès en matière de cyberdéfense. On a planché sur tous les aspects de la question, de la façon dont nous nous sommes structurés à la mise en place des acteurs nécessaires, sans oublier l'attention accordée à la question aux plus hauts niveaux. On a porté grandement attention à l'aspect gouvernemental, mais je ne voudrais jamais laisser croire qu'il n'y a plus rien à faire.

Cela est lié à ma réponse précédente. Il s'agit d'un environnement qui est tellement en constante métamorphose qu'on ne peut jamais se permettre d'adopter une attitude de laisser-faire et dire que le travail est terminé. Nous devons toujours être à l'affût des nouvelles menaces, des nouveaux acteurs et des nouvelles vulnérabilités. Même si le gouvernement a fait beaucoup de chemin, nous devons continuer à surveiller tout cela.

Au sujet de votre question concernant le secteur privé, je peux vous dire que le gouvernement a lancé, il y a un certain nombre d'années, la stratégie de cybersécurité du Canada, qui repose sur trois piliers. Le premier concerne ce dont nous avons parlé, c'est-à-dire protéger les systèmes gouvernementaux; le deuxième consiste à appuyer le secteur privé; et le troisième vise à aider directement les citoyens canadiens.

La stratégie est gérée par le ministère de la Sécurité publique. Ce ministère est responsable du deuxième pilier. Il collabore avec le secteur privé et appuie ses initiatives. Pour répondre à votre question, je dirais qu'il est l'organisme responsable. Le CST joue également un rôle. Je vais vous donner deux exemples, si vous le permettez. Le premier concerne les renseignements au sujet des cybermenaces. Notre travail consiste entre autres à nous pencher sur les cybermenaces complexes contre le Canada. Nous recevons beaucoup de renseignements sur les cybermenaces de la part de diverses entreprises, mais notre travail consiste à surveiller les cybermenaces les plus complexes qui pèsent sur notre pays. Nous pouvons communiquer certains de ces renseignements sur les cybermenaces au secteur privé.

Nous nous occupons aussi de fournir des conseils en matière d'atténuation. Lorsqu'une cyberattaque se produit, un certain nombre de mesures doivent être prises. Il faut connaître les mesures d'atténuation. Nous fournissons également au secteur privé des conseils en matière d'atténuation. J'espère que j'ai bien répondu à votre question.

Le sénateur Mitchell : Vous ne pouvez peut-être pas tout nous dire, mais j'aimerais savoir comment vous organisez tout cela. Évidemment, les banques ont des infrastructures essentielles qui sont très informatisées, et c'est le cas également des sociétés de pipelines, des raffineries et de l'industrie énergétique. Comment vous occupez-vous des différents secteurs? Il me semble qu'il faut

It would take different relationships, obviously. How do you even begin to organize that, and how do you pick which sectors? How do you prioritize?

Ms. Bossenmaier: That's a good question. It goes back to your question about a lot of different players, sectors and interests.

I refer back to my colleagues in Public Safety with the responsibility to look at critical infrastructure not only from a cyber perspective but overall in terms of critical infrastructure. My understanding is they have organized along with a number of key sectors. I believe they have 10 sectors, and each sector is organized around common themes and interests. They deal with those sectors, and I guess they organize themselves accordingly in terms of what are the key interests and the key players in each of those sectors.

[*Translation*]

Senator Carignan: I would like to come back to Senator Lang's question about the number of foreign-based extremist plots against Canada over the past five years. I understand it is difficult to provide a precise figure, but can you give us a rough estimate? Arrests are another issue. That data should nevertheless be accessible. Can you give us a clearer picture?

Ms. Bossenmaier: Thank you for your question. I will answer in English.

[*English*]

We are not a law enforcement organization, senator. We are a foreign signals intelligence organization and a cyberdefence organization. In terms of arrests, that was not the domain of my organization.

Again, looking at the overall threat picture to Canada, it's the responsibility of CSIS to look at the overall threat environment facing our country. Unfortunately, I won't be able to give you a precise number of arrests or that kind of outcome. I'd have to refer to my colleagues at CSIS or the RCMP.

[*Translation*]

Senator Carignan: Can you give us an order of magnitude when it comes to specific elements you have identified that have led to an exchange of information with CSIS?

[*English*]

Ms. Bossenmaier: Once again, senator, I don't have an exact number or order of magnitude that I can provide to you regarding how they've used information or, again, what the actual outcome is.

des expertises différentes. Il faut entretenir différentes relations, bien entendu. Comment organisez-vous tout cela et comment choisissez-vous les secteurs? Comment établissez-vous les priorités?

Mme Bossenmaier : C'est une bonne question. Elle est liée à votre question concernant le fait qu'il y a un grand nombre d'acteurs, de secteurs et d'intérêts différents.

Mes collègues du ministère de la Sécurité publique ont la responsabilité de surveiller les infrastructures essentielles, non seulement du point de vue de la cybersécurité, mais aussi sur le plan de la protection en général des infrastructures essentielles. Je crois savoir qu'ils ont établi un certain nombre de secteurs clés. Je crois qu'il y en a une dizaine et que chaque secteur est lié à des thèmes et des intérêts communs. Ils s'occupent de ces secteurs, et j'imagine qu'ils s'organisent en fonction des principaux intérêts et des principaux acteurs au sein de chacun de ces secteurs.

[*Français*]

Le sénateur Carignan : J'aimerais revenir à la question du sénateur Lang sur le nombre de complots d'étrangers extrémistes qui ont eu lieu au cours des cinq dernières années contre le Canada. Je comprends qu'il est difficile de donner un chiffre précis, mais pouvez-vous nous donner un ordre de grandeur? Il y a aussi la question des arrestations. Ces données devraient tout de même être accessibles. Pouvez-vous nous en donner un aperçu plus précis?

Mme Bossenmaier : Merci pour votre question. Je vais répondre en anglais.

[*Traduction*]

Nous ne sommes pas un organisme d'application de la loi, monsieur le sénateur. Nous sommes un organisme qui fournit du renseignement étranger et qui s'occupe de la cyberdéfense. Pour ce qui est des arrestations, cela ne relève pas de mon organisme.

En ce qui concerne l'ensemble des menaces, il appartient au SCRS d'examiner l'ensemble des menaces pour le Canada. Malheureusement, je ne suis pas en mesure de vous fournir le nombre précis d'arrestations. Il faudrait que je consulte mes collègues du SCRS ou de la GRC.

[*Français*]

Le sénateur Carignan : Quant aux éléments précis que vous avez détectés et qui ont donné lieu à un échange d'information avec le SCRS, pouvez-vous nous donner un ordre de grandeur?

[*Traduction*]

Mme Bossenmaier : Encore une fois, monsieur le sénateur, je ne peux pas vous fournir un chiffre exact ni un ordre de grandeur concernant la façon dont l'information a été utilisée ou vous faire part des résultats réels.

[*Translation*]

Senator Carignan: In the case of external agencies that are hostile toward Canada, are threats to Canada identified often? What are the main sources of those hostile external agencies? Do they come from China, from Russia? What are the main suspects or hostile agencies that pose a risk?

[*English*]

Ms. Bossenmaier: Senator, are you speaking particularly from a cyber-threat perspective?

[*Translation*]

Senator Carignan: Yes, or other elements you may have identified.

[*English*]

Ms. Bossenmaier: Maybe I'll speak again from a cyber-threat perspective. As I mentioned, it's a very dynamic environment now — not only in terms of the nature of the threats we're seeing but also, to your point, in terms of the various types of threat actors.

Perhaps I could try to characterize them in four major buckets. The first are sophisticated nation states that are working in the cyber domain. Without actually naming any of the particular countries — we don't name our targets, our methods or our capabilities in our organization — there are definitely sophisticated nation states that are conducting cyberoperations and cyberattacks.

We're seeing the rise of non-state actors that are now getting into looking at cyber from an offensive perspective. I gave the example in my opening remarks about how we're now seeing terrorist organizations that are looking to use the global Internet infrastructure to plan attacks, for sure to radicalize and inspire attacks. We've seen that increasing over the recent past. It's sort of a new phenomenon, terrorist organizations using the Internet for that purpose. It is a relatively inexpensive cost to entrants, but they have the ability to connect with so many people in a borderless world. The rise of non-state actors has been a new phenomenon.

There is also the rise of cybercriminals. We think of criminals in our non-cyber world, but the rise of cybercriminals is interesting and, again, presents more challenging aspects that we've been seeing in the last little while. We hear now of cyber ransom, where cybercriminals are holding companies and individuals ransom by locking them out of their own computer systems and actually asking them to pay or forcing them to pay to get back onto their computer systems. That is a new type of criminal activity that we wouldn't have seen in the recent past.

[*Français*]

Le sénateur Carignan : Dans le cas des agences externes qui sont hostiles au Canada, arrive-t-il fréquemment que des menaces soient détectées qui visent le Canada? De plus, quelles sont les sources principales de ces agences extérieures hostiles? Nous viennent-elles de la Chine, de la Russie? Quels sont les principaux suspects ou organismes hostiles qui posent des risques?

[*Traduction*]

Mme Bossenmaier : Parlez-vous particulièrement du point de vue d'une cybermenace?

[*Français*]

Le sénateur Carignan : Oui, ou d'autres éléments que vous pourriez avoir détectés.

[*Traduction*]

Mme Bossenmaier : Je vais répondre encore une fois du point de vue d'une cybermenace. Comme je l'ai mentionné, il s'agit d'un environnement en constante métamorphose, non seulement sur le plan de la nature des menaces, mais aussi, comme vous le mentionnez, sur le plan des divers auteurs de menaces.

Je pourrais peut-être essayer de les classer en quatre grandes catégories. La première englobe les États-nations avancés qui œuvrent dans le cyberespace. Sans nommer des pays en particulier — au sein de notre organisme, nous ne nommons jamais nos cibles et nous ne parlons jamais de nos méthodes ou de nos capacités —, je peux vous dire que certains États-nations avancés mènent des cyberopérations et des cyberattaques.

Nous constatons que des acteurs non étatiques envisagent le cyberespace d'un point de vue offensif. Dans ma déclaration liminaire, j'ai expliqué que des organisations terroristes utilisent Internet pour planifier des attentats, pour radicaliser des gens et susciter des attentats. Cela se fait de plus en plus depuis un certain temps. Que des organisations terroristes utilisent Internet à cette fin constitue un phénomène nouveau. Il s'agit d'une façon relativement peu coûteuse de communiquer avec un très grand nombre de personnes dans un environnement sans frontières. L'augmentation du nombre d'acteurs non étatiques est un nouveau phénomène.

Il y a aussi une augmentation du nombre de cybercriminels. On parle des criminels dans le monde réel, mais il est intéressant de se pencher sur la hausse du nombre de cybercriminels, car cela met en évidence des phénomènes qui sont apparus dernièrement. On entend maintenant parler de cyberrançon dans des situations où des cybercriminels tiennent des entreprises et des personnes en otage en bloquant l'accès à leurs propres systèmes informatiques et en leur demandant de payer ou en les obligeant à payer une somme d'argent pour pouvoir de nouveau avoir accès à leurs systèmes informatiques. Il s'agit d'un nouveau type d'activité criminelle qui n'existait pas jusqu'à tout récemment.

We often talk about the hackers. Well, there are different motives, perhaps, but we've seen organizations now that are bringing down websites — not necessarily to steal information or to infiltrate the websites, but to be able to stop legitimate business from happening. They could be doing that to try to raise awareness for their cause or to campaign around a particular issue.

There is a diverse and dynamic set of threat actors that we're seeing changing and evolving. What that means for an organization like ours is that we need to continue to ensure that we are adapting and being aware and trying to stay ahead of what the threat actors are and what that threat environment looks like. More to your point, that's not just a threat environment to Canada; it's a global threat environment.

Senator Wells: Thank you, Ms. Bossenmaier. Does the CSE have a public complaints channel? How can Canadians feel assured that you're not harvesting data related to personal and legal actions and that this information isn't shared with our allies?

Ms. Bossenmaier: Thank you for the question, senator. I think you had the privilege of having before you, not too long ago, the Communications Security Establishment Commissioner. I'll refer to the role of the CSE Commissioner, actually, in answering a couple of your questions, if I may.

In terms of review, I would say CSE does have a very robust independent review mechanism in place, in the form of the Communications Security Establishment Commissioner: a respected jurist who has a lot of experience and a staff that is very experienced with the nature of our work and has full access to all of our systems, our people and our information — that is, independent but with full access to our organization.

If someone has a concern or complaint, they can raise that with the commissioner; that is one of the commissioner's roles. As well, internal to our organization, we have a series of folks that our own employees can go to, including an ethics and values organization. That has a mechanism to allow someone inside of the organization to raise an issue or raise a complaint; they can go inside to our ethics and values coordinator.

Senator Ngo: Does CSE have the legal authority to monitor permanent residents in Canada or Canadian citizens who are participating as jihadist foreign fighters?

Ms. Bossenmaier: We are a foreign signals intelligence organization, and our mandate is derived directly from the National Defence Act. In terms of targeting people under our foreign signals intelligence mandate, we are not allowed, under the National Defence Act, to target Canadians anywhere, or

Nous parlons souvent des pirates informatiques. Les motifs sont peut-être différents, mais certaines organisations bloquent des sites web, pas nécessairement pour voler des renseignements ou infiltrer des sites web, mais pour empêcher des activités commerciales légales d'avoir lieu. Elles peuvent faire cela pour sensibiliser les gens à leur cause ou pour militer au sujet d'un enjeu en particulier.

Il existe un groupe varié d'auteurs de menaces qui est en train d'évoluer. Pour un organisme comme le nôtre, cela signifie que nous devons continuer de nous adapter, de rester à l'affût, d'essayer de prévoir ce que feront les auteurs de menaces et d'évaluer les menaces. Pour répondre davantage à votre question, je peux dire que ce ne sont pas des menaces seulement pour le Canada, mais pour le monde entier.

Le sénateur Wells : Je vous remercie, madame Bossenmaier. Existe-t-il au CST un mécanisme de plaintes? Comment les Canadiens peuvent-ils être certains que vous ne recueillez pas des données de nature personnelle et juridique et que ces renseignements ne sont pas communiqués à nos alliés?

Mme Bossenmaier : Je vous remercie pour votre question, monsieur le sénateur. Je crois que vous avez eu le privilège, il n'y a pas très longtemps, de recevoir le commissaire du Centre de la sécurité des télécommunications. Pour répondre à certaines de vos questions, je vais faire référence au rôle du commissaire du CST, si vous me le permettez.

Pour ce qui est des examens, je peux dire que le CST s'est doté d'un mécanisme d'examen indépendant très solide. Je veux parler du Bureau du commissaire du Centre de la sécurité des télécommunications. Le commissaire est un juriste respecté qui possède une vaste expérience et le personnel du bureau connaît très bien la nature de notre travail et profite d'un accès complet à tous nos systèmes, à notre personnel et à nos renseignements. Il s'agit d'un bureau indépendant qui a plein accès à tout ce qui concerne notre organisme.

Si une personne a une préoccupation à exprimer ou une plainte à formuler, elle peut s'adresser au commissaire. Le commissaire a notamment pour rôle de s'occuper de cela. En outre, au sein de notre organisme, nos propres employés peuvent s'adresser à des responsables de l'éthique et des valeurs. Les gens au sein de l'organisation peuvent soulever un problème ou formuler une plainte; ils peuvent s'adresser à notre responsable de l'éthique et des valeurs.

Le sénateur Ngo : Est-ce que le CST a l'autorisation légale de surveiller les résidents permanents au Canada ou les citoyens canadiens qui sont recrutés comme combattants étrangers djihadistes?

Mme Bossenmaier : Notre organisme fournit du renseignement étranger et notre mandat est défini dans la Loi sur la défense nationale. Pour ce qui est de cibler des gens dans le cadre du volet de notre mandat qui consiste à fournir du renseignement étranger, nous ne sommes pas autorisés, en vertu de la Loi sur la défense

anyone in Canada. We are a foreign signals intelligence organization.

Senator Ngo: Even though those Canadians or permanent residents are participating as jihadist foreign fighters?

Ms. Bossenmaier: From a CSE mandate, we are not allowed. It's against our authority to target Canadians regardless of where they are, or anyone in Canada.

The Chair: Where are we getting the information on these Canadians that have made the decision to become jihadist fighters over in the Middle East? Who is monitoring them? If you're not doing it, who is?

Ms. Bossenmaier: Thank you, senator. I'll make two points to address your question. First of all, we're a foreign signals intelligence organization.

The Chair: They're over in a foreign land.

Ms. Bossenmaier: We do foreign signals intelligence. There are other types of intelligence activities. For example, you had my colleague from CSIS here not long ago.

We have a three-part mandate, as I mentioned in my opening remarks. The first is foreign signals intelligence that has to be directed at people outside of Canada and not Canadians. We have a cyberdefence mandate that I have talked a lot about so far. We have a third mandate, which is an assistance mandate. Under that, a federal law enforcement or security agency can request the assistance of CSE if they have the legal mandate to do so, and we are then allowed to provide assistance to them under their legal authority. So, if an organization has the legal authority to investigate someone abroad and they need assistance, they can ask CSE to assist them in that perspective, and we do so under their authority, under their legal mandate. That's the third part of our mandate.

The Chair: Let's get this clear: CSIS can ask you to conduct foreign surveillance on a Canadian that's involved in jihadist terrorist activity. Is that correct?

Ms. Bossenmaier: They can ask us, but they have to have the legal authority to do so.

The Chair: When do they have the legal authority?

Ms. Bossenmaier: It depends on their circumstance, Mr. Chair, if I may. Depending on what their circumstance is, they would have to seek a warrant and ask in that warrant if they can conduct the activity, and whether they can ask for our assistance. If they have the legal authority to do that, then we would consider it.

The Chair: I want to ask another question if you don't mind, colleagues.

nationale, à cibler des Canadiens, où qu'ils se trouvent, ou des personnes au Canada. Nous sommes un organisme qui fournit du renseignement étranger.

Le sénateur Ngo : Même si ces Canadiens ou ces résidents permanents sont des combattants étrangers djihadistes?

Mme Bossenmaier : Le mandat confié au CST ne nous le permet pas. Nous n'avons pas l'autorisation de cibler des Canadiens, peu importe où ils se trouvent, ni personne au Canada.

Le président : D'où proviennent les renseignements que nous possédons au sujet des Canadiens qui ont décidé de devenir des combattants djihadistes au Moyen-Orient? Qui les surveille? Si ce n'est pas vous, qui le fait?

Mme Bossenmaier : Je vous remercie, monsieur le sénateur. J'ai deux choses à dire pour répondre à votre question. Premièrement, nous sommes un organisme qui fournit du renseignement étranger.

Le président : Ces personnes se trouvent à l'étranger.

Mme Bossenmaier : Nous fournissons du renseignement étranger. Il existe d'autres types d'activités de renseignement. Par exemple, vous avez reçu il n'y a pas très longtemps mon collègue du SCRS.

Notre mandat comporte trois volets, comme je l'ai mentionné dans ma déclaration liminaire. Le premier volet concerne le renseignement étranger qui porte sur des personnes qui se trouvent à l'extérieur du Canada et non pas sur des Canadiens. Le deuxième volet concerne la cyberdéfense, dont j'ai amplement parlé jusqu'à maintenant. Le troisième volet consiste à fournir une assistance. Dans le cadre de ce volet, un organisme fédéral responsable de l'application de la loi ou de la sécurité peut demander l'aide du CST s'il dispose d'un mandat légal pour ce faire. Nous sommes alors autorisés à lui fournir une assistance en vertu de son autorisation légale. Donc, si un organisme détient l'autorisation légale d'enquêter sur une personne à l'étranger et qu'il a besoin d'aide, il peut demander l'assistance du CST à cet égard. Nous lui fournissons alors une assistance en vertu de son mandat légal. Cela relève du troisième volet de notre mandat.

Le président : Soyons clairs : le SCRS peut vous demander de surveiller un Canadien qui participe à des activités terroristes djihadistes. Est-ce exact?

Mme Bossenmaier : Il peut nous le demander, mais il doit avoir l'autorisation légale de le faire.

Le président : Quand dispose-t-il de cette autorisation légale?

Mme Bossenmaier : Cela dépend des circonstances, monsieur le président, si je puis dire. Selon les circonstances, il doit obtenir un mandat et demander s'il peut mener cette activité et s'il peut demander notre aide. S'il obtient l'autorisation légale de le faire, alors nous pouvons envisager de l'aider.

Le président : J'aimerais poser une autre question, si vous le voulez bien, chers collègues.

Do you think you should have the authority to do that surveillance when a Canadian or a permanent resident is identified overseas in these types of activities, so that you can do your job?

Ms. Bossenmaier: We have a three-mandate job, Mr. Chair, which comes to us from the National Defence Act. Part C of that mandate does allow us to assist federal law enforcement and security agencies in their mandates. In the other parts of our mandate, again, we deal with foreign signals intelligence.

The Chair: It sounds to me like you're somewhat prohibited.

Senator Day: I think that's a good check on your activity. In the event of Part C — and this is the assistance to other law enforcement agencies — that agency has to involve lawyers and judges in order to satisfy you that you can do the activity they're asking you to help them with.

Ms. Bossenmaier: That's correct. We have different mandates.

Senator Day: Yes. So this "prohibited by law from targeting Canadians" is only with respect to the first part of your mandate?

Ms. Bossenmaier: With respect to the first two.

Senator Day: First two.

Ms. Bossenmaier: Yes.

Senator Day: The second mandate is what I wanted to talk to you about: cybersecurity. You're saying that you're prohibited from targeting Canadians or anyone in Canada with respect to cyberterrorism and cyberactivities.

Ms. Bossenmaier: That's correct.

Senator Day: Is there a law enforcement agency in Canada that could ask for your assistance under Part C to deal with cybersecurity issues?

Ms. Bossenmaier: You'll feel like I'm answering every question in two parts, but I'll answer this one in two parts as well.

You're absolutely correct, senator. The second part of our mandate is a protection mandate for electronic systems of importance to the Government of Canada. We look at foreign threats; we look at threats to Canada; we help provide mitigation advice; we help engineer solutions for the Government of Canada, for example; and we also, through our sophisticated cyberdefence mechanisms, defend government systems from threats. I'll give an example: If a sophisticated cyberactor is trying to penetrate into a government system, we will help identify and defend against that based on technologies and systems that we have in place.

Croyez-vous que vous devriez obtenir l'autorisation d'effectuer cette surveillance lorsqu'on sait qu'un Canadien ou un résident permanent est engagé dans de telles activités, afin que vous puissiez faire votre travail?

Mme Bossenmaier : Nous avons un mandat à trois volets, monsieur le président, qui est défini dans la Loi sur la défense nationale. Le troisième volet de notre mandat, que j'appelle la partie C, nous permet de fournir une assistance aux organismes fédéraux responsables de l'application de la loi et de la sécurité, conformément à leurs mandats. Un autre volet de notre mandat, je le répète, consiste à fournir du renseignement étranger.

Le président : Il me semble que vous avez un peu les mains liées.

Le sénateur Day : Je crois que c'est une bonne façon de contrôler vos activités. Dans le cas de la partie C — l'assistance à d'autres organismes d'application de la loi — l'organisme en question doit faire appel à des avocats et à des juges pour vous convaincre que vous pouvez mener l'activité qui permettra de l'aider.

Mme Bossenmaier : C'est exact. Notre mandat comporte différents volets.

Le sénateur Day : Oui. Alors, cette interdiction, en vertu de la loi, de ne pas cibler des Canadiens concerne seulement le premier volet de votre mandat?

Mme Bossenmaier : Elle concerne les deux premiers volets.

Le sénateur Day : Les deux premiers.

Mme Bossenmaier : Oui.

Le sénateur Day : J'aimerais parler du deuxième volet du mandat, c'est-à-dire la cybersécurité. Vous dites que vous ne pouvez pas viser des Canadiens ou quiconque au Canada en ce qui concerne le cyberterrorisme et les cyberactivités.

Mme Bossenmaier : C'est exact.

Le sénateur Day : Y a-t-il au Canada un organisme d'application de la loi qui pourrait demander votre aide en matière de cybersécurité, en vertu du troisième volet, la partie C de votre mandat?

Mme Bossenmaier : Vous allez vous dire que je réponds à chaque question en deux parties, car je vais répondre à celle-ci en deux parties également.

Vous avez tout à fait raison, monsieur le sénateur. Le deuxième volet de notre mandat consiste à protéger les systèmes électroniques importants pour le gouvernement du Canada. Nous surveillons les menaces étrangères; nous surveillons les menaces pour le Canada; nous fournissons des conseils en matière d'atténuation; nous contribuons à mettre au point des solutions pour le gouvernement du Canada, notamment, et, grâce à nos mécanismes très élaborés de cyberdéfense, nous protégeons les systèmes gouvernementaux contre les menaces. Je vais vous donner un exemple. Si un cyberacteur compétent essaie d'entrer

Again, we're not a law enforcement organization. Part C of our mandate deals with providing assistance to a federal law enforcement agency that has a legal mandate to conduct that business. For example, the RCMP could also, under their legal mandate, ask us to assist them in an instance that they needed our assistance — again, under their legal authority.

Senator Day: I guess my question was going to cyber and cyberactivity, and I thought I had to go to the second part of your authority, but if we're dealing with something outside of the information system of the government, we're into the third part. For example, what role do you have in terrorism and counterterrorism on social media? Is it always only under the third part, assistance to other government agencies in developing strategies to deal with terrorism and counterterrorism on the Internet?

Ms. Bossenmaier: I'll have to talk about Part B of our mandate to begin with, because it talks about protecting and defending and providing assistance to systems of importance to the Government of Canada. Systems of importance to the Government of Canada absolutely include Government of Canada systems, but that also gets into other systems of importance. I had a question from another senator about critical infrastructure, which could be a system of importance to the Government of Canada.

Senator Day: That could be anything.

Ms. Bossenmaier: As such, we can provide support. I talked about giving mitigation advice, for example, and cyber-threat information, from a law enforcement perspective, because that would be under Part C of our mandate, providing assistance through the federal law enforcement security agency.

Senator Day: Just to finish this up, does the advice include monitoring?

Ms. Bossenmaier: For the private sector?

Senator Day: Yes.

Ms. Bossenmaier: We are not monitoring the private sector.

Senator Day: So from a social media point of view, who is doing that? If you're not doing it, who is?

Ms. Bossenmaier: We think of ourselves as individual Canadians. When we're on the Internet, we're hopefully doing things with good Internet hygiene and keeping our computers safe and following the right kinds of processes. Just as businesses protect their operations from a variety of threats, they're also protecting themselves from cyber-threats. From a CSE

dans un système du gouvernement, nous allons contribuer à l'identifier et à contrer cette attaque à l'aide des technologies et des systèmes dont nous disposons.

Je le répète, nous ne sommes pas un organisme d'application de la loi. La partie C de notre mandat consiste à fournir une assistance à un organisme fédéral d'application de la loi qui dispose d'un mandat légal pour faire ce qu'il souhaite. Par exemple, la GRC pourrait, en vertu de son mandat légal, nous demander de l'aide lorsqu'elle en a besoin. Je le répète, nous fournissons une assistance conformément à l'autorisation légale de l'organisme.

Le sénateur Day : Ma question porte sur les cyberactivités, et je croyais que cela était lié au deuxième volet de votre mandat, mais s'il est question d'une activité qui n'est pas liée aux systèmes d'information du gouvernement, il s'agit du troisième volet. Par exemple, quel rôle jouez-vous en ce qui concerne le terrorisme et la lutte contre le terrorisme dans les médias sociaux? Agissez-vous toujours en vertu du troisième volet, c'est-à-dire aider d'autres organismes gouvernementaux à élaborer des stratégies pour lutter contre le terrorisme dans Internet?

Mme Bossenmaier : Je vais devoir d'abord parler du deuxième volet, la partie B de notre mandat, car il consiste à protéger les systèmes importants du gouvernement du Canada et à fournir une assistance à cet égard. Les systèmes importants pour le gouvernement du Canada englobent bien entendu des systèmes du gouvernement canadien, mais aussi d'autres systèmes qui sont importants. Un autre sénateur m'a posé une question au sujet des infrastructures essentielles, qui pourraient être des systèmes importants pour le gouvernement du Canada.

Le sénateur Day : Ce pourrait être n'importe quoi.

Mme Bossenmaier : Oui, et nous pouvons fournir une assistance. J'ai dit que nous fournissons des conseils en matière d'atténuation, par exemple, ainsi que des renseignements sur les cybermenaces, du point de vue de l'application de la loi, parce que nous pouvons le faire en vertu de la partie C de notre mandat, qui consiste à fournir une assistance aux organismes fédéraux chargés de l'application de la loi et de la sécurité.

Le sénateur Day : En terminant, pouvez-vous me dire si les conseils que vous fournissez portent sur la surveillance?

Mme Bossenmaier : Du secteur privé?

Le sénateur Day : Oui.

Mme Bossenmaier : Nous n'effectuons pas de surveillance du secteur privé.

Le sénateur Day : Alors, en ce qui concerne les médias sociaux, qui s'en occupe? Si ce n'est pas votre organisme, qui le fait?

Mme Bossenmaier : Nous nous voyons comme des individus. Lorsque nous utilisons Internet, nous respectons, je l'espère, l'étiquette et nous veillons à assurer la sécurité de nos ordinateurs et à adopter les bonnes procédures. Les entreprises protègent leurs activités contre diverses menaces et elles se protègent elles-mêmes contre les cybermenaces. Le CST, en collaboration avec le

perspective, we're looking at, along with our colleagues particularly in Public Safety, how we can share our knowledge and expertise with them so that they can better defend themselves.

Senator White: Thanks for your replies. I have to say that your answers tend to bring more questions for some of us. I think it has to do with the job you do, not so much with the questions or the answers.

Is any proactive work being done with Canadians? When we talk about cyber-threat, I would argue that it has greater potential against individuals more often than it has against corporations and such. It is a greater amount but not the number of threats.

Does CSE do any work to try to help Canadians understand the cyber-threats so that they are better prepared? You talk about being vigilant; but not a lot of people are vigilant, to be fair. Are you doing any proactive work in Canada? Who is doing that work?

Ms. Bossenmaier: I'll try to be clear. I will refer back to the government's cyber-strategy. Briefly, a three-part cyber-strategy was put in place a number of years ago to look at three things. First is to protect Government of Canada networks, where we have a very important role from CSE's perspective in terms of defence, prevention and education. Second is to support and help to support private industry in their cyberprotection roles. The third part of the strategy, senator, is exactly to your point: to look at helping Canadian citizens living and working in this increasingly cyber world.

For example, my colleagues in Public Safety come out with information and advice to citizens in terms of cyberawareness week and things that you can do to be better cyber-prepared. I've given everyone today a copy of the CSE's top 10. Those top 10 are good advice from CSE, in our experience given what we're seeing in dealing with cyber-threats, that we're encouraging and providing guidance to all government departments to do. As well, many of those are appropriate to private industry, for example.

It's about education, getting the message out and helping to share that information. Public Safety is very much in the zone of working with private citizens and the CSE to share our advice and guidance where we can.

I may also mention two other things, senator. The government has committed to launching a cyber review in the next little while that will be under the purview of the Minister of Public Safety with support from a number of ministers, including the Minister

ministère de la Sécurité publique, en particulier, est en train d'examiner comment nous pourrions faire profiter le secteur privé de nos connaissances et de notre expertise pour qu'il puisse mieux se protéger.

Le sénateur White : Je vous remercie pour vos réponses. Je dois dire que, pour certains d'entre nous, elles soulèvent davantage de questions. Je crois que c'est en raison du travail que vous faites plutôt que des questions qui ont été posées ou des réponses que vous avez données.

Est-ce qu'on accomplit du travail proactif auprès des Canadiens? Lorsqu'il est question des cybermenaces, je dirais que ce travail est souvent plus efficace auprès des particuliers que des entreprises. C'est plus efficace, mais il n'y a pas d'incidence sur le nombre de menaces.

Le CST aide-t-il les Canadiens à comprendre les cybermenaces afin qu'ils soient mieux préparés à y faire face? Vous parlez de vigilance, mais il faut avouer que bien des gens ne sont pas vigilants. Est-ce que vous effectuez du travail proactif au Canada? Qui fait ce travail?

Mme Bossenmaier : Je vais essayer d'être claire. Je vais revenir à la stratégie de cybersécurité du gouvernement. En résumé, il s'agit d'une stratégie qui repose sur trois piliers et qui a été mise en œuvre il y a quelques années dans le but d'accomplir trois choses. Premièrement, protéger les systèmes du gouvernement du Canada. À cet égard, le CST joue un rôle très important en matière de protection, de prévention et d'éducation. Deuxièmement, il s'agit d'aider le secteur privé à mener ses activités de cyberprotection. La troisième partie de cette stratégie, monsieur le sénateur, concerne ce que vous venez de dire, à savoir aider les Canadiens, qui vivent et travaillent dans un monde axé de plus en plus sur le cyberespace.

Par exemple, mes collègues du ministère de la Sécurité publique diffusent des renseignements et des conseils à l'intention des citoyens pour les sensibiliser à la cybersécurité et les renseigner sur ce qu'ils peuvent faire pour mieux se protéger. J'ai remis à tout le monde aujourd'hui une copie du document présentant les 10 meilleures mesures de sécurité à adopter. Il s'agit de bons conseils fournis par le CST, qui sont fondés sur ce que nous observons en ce qui concerne les cybermenaces. Nous encourageons tous les ministères gouvernementaux à suivre ces conseils. Un grand nombre de ces mesures peuvent être appliquées dans le secteur privé.

Il s'agit d'éduquer les gens, de faire passer le message et d'aider à transmettre l'information. Le ministère de la Sécurité publique s'emploie à sensibiliser les citoyens et il collabore avec le CST pour diffuser des conseils et donner des orientations lorsque c'est possible.

Je peux aussi mentionner deux autres choses, monsieur le sénateur. Le gouvernement s'est engagé à lancer sous peu un examen sur la cybersécurité, sous les auspices du ministère de la Sécurité publique, avec l'appui d'un certain nombre de ministres,

of National Defence to look at cybersecurity and cyber issues in Canada. That important review will come forward and no doubt may touch on a lot of the conversations we've had today.

The Minister of National Defence is also undertaking a defence review, and cyber will likely be a part of that conservation as well.

In particular, the cyber review led by Public Safety with support from my minister and others no doubt will look at these important questions in terms of cybersecurity for Canada.

Senator Mitchell: I'm interested in your top 10. You mentioned that you shared Shared Services Canada Internet gateways. Recently there was a report in the media about the problems with Shared Services Canada, specifically with respect to security issues in the RCMP's system and unanticipated security issues holding that up. How do you sort of reconcile the two?

Ms. Bossenmaier: Senator, I can tell you from an overall security posture from the Government of Canada that Shared Services Canada and moving government departments onto shared services from an infrastructure perspective has been absolutely key to improving the Government of Canada's cyber preparedness and cyber readiness. Our number one recommendation, and they are in order of priority, for government departments is fully utilized Shared Services infrastructure from a cyberprotection perspective. The additional kinds of cyberprotection tools that are in place are key. That's really our number one piece of advice.

I'll mention one more piece around shared services. Shared Services Canada is building solutions and services for all government departments. CSE is working with our Shared Services colleagues to help build in and design in security from the beginning — security by design. It's a matter of building stronger systems from the beginning and not doing it across 90 or 100 different departments. Do it once for the Government of Canada. From a cybersecurity perspective, the standing up of Shared Services Canada and having departments use them for their infrastructure services and core applications has actually been a key part of the Government of Canada's cyberoperations.

I guess someone asked me the question earlier about what other governments are doing. Other governments are looking at the way we operate in Canada, from a cyber perspective in terms of the government, and are recognizing that this is such a critical component to strengthening the Government of Canada's systems.

Senator Mitchell: Is it optional? Can a department opt in or out of shared services? If you're having to put so much emphasis on it, it sounds optional.

dont le ministre de la Défense nationale, afin d'examiner la cybersécurité et les enjeux à cet égard au Canada. Cet important examen portera sans doute sur un grand nombre des sujets dont nous avons discuté aujourd'hui.

Le ministre de la Défense nationale entreprendra également un examen de la politique de défense, et il est fort probable que la cybersécurité sera étudiée dans le cadre de cet examen.

L'examen sur la cybersécurité qui sera mené par le ministère de la Sécurité publique avec l'aide du ministre responsable du CST et d'autres ministres permettra de se pencher sur ces questions importantes qui touchent la cybersécurité au Canada.

Le sénateur Mitchell : Je m'intéresse aux 10 meilleures mesures à adopter. Vous avez mentionné que vous avez partagé la passerelle Internet de Services partagés Canada. Récemment, les médias ont fait état de problèmes en ce qui concerne Services partagés Canada, précisément relativement à la sécurité des systèmes de la GRC et à des problèmes de sécurité imprévus. Qu'en est-il à ce sujet?

Mme Bossenmaier : Monsieur le sénateur, je peux vous dire que, du point de vue de la sécurité globale du gouvernement du Canada, la création de Services partagés Canada et l'initiative visant à faire en sorte que des ministères partagent des services informatiques ont contribué de façon très importante à accroître la cyberpréparation du gouvernement du Canada. Ce que nous recommandons en premier lieu aux ministères gouvernementaux, c'est d'utiliser pleinement l'infrastructure de Services partagés, dans une optique de cyberprotection. Les autres outils de cyberprotection qui existent sont également essentiels. C'est le principal conseil que nous donnons aux ministères.

J'aimerais mentionner une autre chose au sujet de Services partagés Canada. Cet organisme produit des solutions et des services pour tous les ministères du gouvernement. Le CST collabore avec les intervenants de Services partagés Canada pour concevoir et intégrer les éléments liés à la sécurité dès le départ — c'est la sécurité intégrée à la conception. Il s'agit de bâtir de meilleurs systèmes au départ et de ne pas recommencer dans 90 ou 100 ministères différents. On le fait une fois pour le gouvernement du Canada. En ce qui concerne la cybersécurité, l'établissement de Services partagés Canada et son utilisation par les ministères pour leurs services d'infrastructure et leurs applications fondamentales représentent un élément essentiel des cyberactivités du gouvernement du Canada.

Je pense que plus tôt, on m'a demandé ce que font les autres gouvernements. D'autres gouvernements examinent les activités du gouvernement du Canada sur le plan cybernétique, et ils reconnaissent qu'il s'agit d'un élément essentiel au renforcement des systèmes de notre gouvernement.

Le sénateur Mitchell : Est-ce facultatif? La décision d'utiliser Services partagés Canada ou non revient-elle aux ministères? Si vous devez insister à ce point, cela semble facultatif.

Ms. Bossenmaier: Shared Services Canada covers a number of core departments. For some smaller, perhaps regional, departments, there was some optionality. We're saying that everybody should get on and use it fully for whatever they can because it provides a really strong cyberprotection.

[*Translation*]

Senator Carignan: I was looking at your chart on risk reduction. I understand that, even when the rules are followed, there is still a substantial risk of cyberattacks. When it comes to espionage or the possibility of us being victims of espionage or infiltration, do you have a training program for members of Parliament, senior officials, directors and department heads on precautionary measures to be taken to avoid being victims of espionage, such as in telephone conversations or exchanges?

We are hearing that there is a threat, that we are victims of certain things and that you protect the systems. But I have never heard about training provided to members of Parliament on what to avoid. Are there any training programs for senior officials or individuals likely to be victims of espionage?

[*English*]

Ms. Bossenmaier: It's an excellent question. When you first look at the chart, you see that the threat surface at the end doesn't go away. It goes back to my earlier comment that none of us can be complacent. We can never think that we're done, that it's taken care of, that it's over. The threat constantly evolves as more and more work is being done on the Internet. We need to be constantly vigilant about it.

One of our roles at the Communications Security Establishment is to help provide education and training to IT specialists within the Government of Canada. A lot of really good training is happening elsewhere in the Government of Canada in terms of broader training and even systems training. But for IT security expertise, we run special training programs for IT specialists to help them become more aware and more able to address those threats and issues when they go into their departments. You raise an excellent point. It's not enough. It's necessary, but it's not sufficient to speak only to the IT practitioners and the security practitioners. We need to speak and share that information all the way up the chain to the other managers, the highest management that we have.

One of my roles is that I speak to, for example, my deputy minister colleagues and give regular updates on everything from the types of threats that we're seeing to what they as senior managers, as leaders in the federal public service, need to do. You can't leave this to your IT professionals. They are very

Mme Bossenmaier : Services partagés Canada s'occupe de quelques grands ministères. Les plus petits ministères, peut-être les ministères régionaux, ont parfois le choix. Nous affirmons cependant que tous les ministères devraient profiter pleinement de ces services pour répondre à leurs besoins, car ils offrent une cyberprotection très robuste.

[*Français*]

Le sénateur Carignan : Je regardais votre affiche sur la réduction des risques. Je comprends que, même lorsque les règles sont suivies, il demeure des éléments substantiels de risque de cyberattaques. En ce qui a trait à l'ensemble de l'espionnage ou de la possibilité pour nous d'être victimes d'espionnage ou d'infiltration, avez-vous un programme de formation s'adressant aux membres du Parlement, aux cadres supérieurs, aux directeurs et aux chefs de service sur les mesures de précaution à prendre pour éviter d'être victime d'espionnage, soit dans le cadre de conversations téléphoniques ou d'échanges?

Nous entendons dire qu'il y a une menace, que nous sommes victimes de certaines choses et que vous protégez les systèmes, mais je n'ai jamais entendu parler d'une formation donnée aux membres du Parlement sur les choses à éviter. Existe-t-il des programmes de formation pour les cadres supérieurs ou pour les personnes susceptibles d'être victimes d'espionnage?

[*Traduction*]

Mme Bossenmaier : C'est une excellente question. À première vue, dans l'affiche, on peut constater que la menace de surface, à la fin, est toujours présente. Cela revient au commentaire que j'ai formulé plus tôt, c'est-à-dire que personne ne peut se permettre de relâcher sa vigilance. Nous ne pouvons jamais penser que notre travail est terminé, que tout a été fait, que la situation est réglée. La menace évolue constamment au fil des travaux effectués dans Internet. Nous devons demeurer vigilants à cet égard.

L'un des rôles du Centre de la sécurité des télécommunications est notamment d'aider à offrir l'éducation et la formation nécessaires aux spécialistes des TI au sein du gouvernement du Canada. On offre déjà, ailleurs au sein du gouvernement du Canada, une très bonne formation générale et même une formation sur les systèmes. Toutefois, en ce qui concerne l'expertise en matière de sécurité des TI, nous offrons des programmes de formation spéciale aux spécialistes des TI, afin de les aider à pouvoir cerner et résoudre ces menaces et ces problèmes lorsqu'ils retournent dans leurs ministères respectifs. Vous avez soulevé un excellent point. Ce n'est pas suffisant. C'est nécessaire, mais il ne suffit pas de parler seulement aux spécialistes des TI et de la sécurité. Nous devons communiquer ces renseignements à tous les gestionnaires, jusqu'au plus haut niveau de gestion de l'organisation.

Mon rôle consiste notamment à parler à mes collègues sous-ministres et à leur fournir régulièrement des mises à jour sur toutes sortes d'enjeux, des types de menaces que nous détectons aux mesures qu'ils doivent prendre en leur qualité de cadres supérieurs et de dirigeants de la fonction publique fédérale. Ces

experienced and play critical roles, but it takes a management imperative to say, "This is important. I'm going to spend time and resources on that."

I speak to my colleagues about the importance of following the top 10 in terms of the types of threats we're seeing. I also work with our colleagues at the Treasury Board Secretariat and at Shared Services for when a cyberattack happens. It's not if — it's when a cyberattack happens. How does one then respond as a senior leader within the organization?

To your question about the House of Commons, I'm not sure. I've been in the CSE for a year; I'm not sure if we've ever provided any type of guidance. I would presume that, within Parliament, some type of process or training would be happening. That's definitely something I can look into, to see whether there's something that CSE could help with; I could get back to you, chair, about what services are available. I'm not sure.

The Chair: If you would report back, that would be good.

Ms. Bossenmaier: It would be my pleasure.

The Chair: I notice time is marching on, colleagues. If I could ask you one question before you go, it has to do with the suspension of some of the metadata with our Five Eyes partners, with the United States, the U.K., Australia and New Zealand. Perhaps you can describe exactly what took place there? Second, did they suspend sharing metadata with us? What steps are we taking to ensure that our metadata meets our legislative requirements and, at the same time, to provide the information to our allies?

Ms. Bossenmaier: Mr. Chair, I have a short answer or a longer answer.

The Chair: Just be concise. Yes, no, yes, no.

Ms. Bossenmaier: I'll try with the short one, and if you feel that I need to go back, I'd be happy to do that.

With regard to this metadata issue, I would start by first saying that the information that we're talking about is metadata. It is information about a communication. It's not the communication itself. It's the context, not the content, of the communication. It's basically information that's used by computer systems to route or identify or manage telecommunications across the global Internet. Metadata is not the content.

I spent a bit of time talking today about our various authorities. CSE is mandated to collect metadata as part of the National Defence Act. We're authorized to acquire and use

décisions ne peuvent pas revenir aux professionnels des TI. Ils ont beaucoup d'expérience et ils jouent un rôle essentiel, mais il revient à la gestion de conclure qu'un enjeu est important et qu'il faut y consacrer le temps et les ressources nécessaires.

Je parle à mes collègues de l'importance de suivre les 10 recommandations les plus importantes selon le type de menaces détecté. Je collabore également avec nos collègues du Secrétariat du Conseil du Trésor et avec ceux de Services partagés Canada en prévision du moment où se produira une cyberattaque. En effet, il ne s'agit pas de savoir si une attaque se produira, mais quand elle se produira. Il faut déterminer comment un haut dirigeant d'une organisation doit réagir dans un tel cas.

En ce qui concerne votre question sur la Chambre des communes, je ne suis pas certaine. Je travaille pour le CST depuis un an; je ne suis pas certaine que nous ayons élaboré des lignes directrices. Je présume qu'il existe un certain type de processus ou de formation au sein du Parlement. Je peux certainement mener quelques recherches, afin de déterminer si le CST peut faire quelque chose à cet égard. Je pourrais vous communiquer les services offerts, monsieur le président. Mais je n'en suis pas certaine pour l'instant.

Le président : Si vous pouviez nous communiquer la réponse, nous vous en serions reconnaissants.

Mme Bossenmaier : Je le ferai avec plaisir.

Le président : Le temps file, chers collègues. J'aimerais vous poser une question avant votre départ, et elle concerne la suspension du partage de certaines des métadonnées avec nos partenaires du Groupe des cinq, c'est-à-dire avec les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande. Pourriez-vous nous décrire ce qui s'est produit dans ce cas? Deuxièmement, ces pays ont-ils cessé de nous transmettre des métadonnées? Quelles mesures prenons-nous pour veiller à ce que nos métadonnées répondent à nos exigences prévues par la loi tout en fournissant ces renseignements à nos alliés?

Mme Bossenmaier : Monsieur le président, je peux vous donner une réponse brève ou une réponse longue.

Le président : Veuillez être concise. Oui, non, oui, non.

Mme Bossenmaier : Je vais tenter de vous fournir la réponse brève, et si vous souhaitez que je précise certains points, je le ferai avec plaisir.

Tout d'abord, j'aimerais préciser que les renseignements dont nous parlons sont des métadonnées. Ce sont des renseignements au sujet d'une communication, mais il ne s'agit pas de la communication elle-même. C'est le contexte, et non le contenu, de la communication. Ce sont essentiellement des renseignements qui sont utilisés par des ordinateurs pour diriger, identifier ou gérer les télécommunications dans l'ensemble d'Internet. Les métadonnées ne représentent donc pas le contenu.

Aujourd'hui, j'ai parlé un peu de nos divers pouvoirs. Le CST a le mandat de recueillir des métadonnées dans le cadre de la Loi sur la défense nationale. Nous sommes autorisés à obtenir et à

information from the global information infrastructure to produce foreign intelligence in accordance with the government priorities that I spoke to you about. In the course of a regular system upgrade, CSE itself detected that some of this metadata that we do share with our Five Eyes colleagues was not being minimized. There's another term: What's "minimized"? "Minimized" means altering certain fields that could have a privacy interest. During a regular system upgrade, we identified that certain fields were not being properly minimized.

CSE proactively did a number of things. First of all, CSE informed the Minister of National Defence and informed the CSE Commissioner, whom you saw here not along ago. CSE also suspended the sharing of the metadata. CSE proactively undertook a review to try to understand what was happening and also undertook an assessment of the privacy impact of that. We assessed the privacy impact as low based on a whole series of privacy protection measures that we have in place.

CSE then worked closely with our commissioner, who was in the midst of a review on metadata within our organization, and he noted in his report and maybe publicly his belief that this metadata incident was unintentional — it was a systems technical deficiency — and that we cooperated fully with him to address it.

As for what we have done since, we have not resumed the sharing of metadata yet. In his statement on this issue, the minister said he needs to be assured that whatever system we put in place has to be robust and meet the privacy protection measures that are required. We are in the throes of ensuring that we are developing a system that will do both things in, help to protect Canada's national security but also, at the same time, ensure that we meet the privacy protection measures that are required. When we have such a system to propose to the minister, we will bring that to the minister for his consideration.

The Chair: Just as a follow up, what did you do with the metadata that was shared and that was found to be not within your legislative mandate to share? Where is that? Has it been destroyed?

Ms. Bossenmaier: As to the metadata that was shared, as I mentioned, we have a series of privacy protection measures in place to help to ensure the privacy protection of that metadata. Looking at that suite of privacy protection measures, we assessed the privacy impact as low. We did not have the metadata deleted from our Five Eyes systems. They have regular retention and deletion schedules that they follow that will result in that metadata being overwritten through their normal practices.

utiliser des renseignements provenant de l'infrastructure mondiale d'information pour produire du renseignement étranger conformément aux priorités du gouvernement dont je vous ai parlé. Pendant une mise à jour régulière du système, le CST s'est rendu compte que certaines de ces métadonnées que nous partageons avec nos collègues du Groupe des cinq n'étaient pas minimisées. Si vous vous demandez ce que signifie « minimisées », c'est lorsqu'on modifie certains champs qui pourraient présenter un intérêt en matière de vie privée. Donc, au cours d'une mise à jour régulière du système, nous avons repéré certains champs qui n'étaient pas minimisés de façon appropriée.

Le CST a pris quelques mesures proactives. Tout d'abord, l'organisme a communiqué avec le ministre de la Défense nationale et avec le Commissaire du CST, qui a récemment comparu devant le comité. Le CST a également suspendu le partage de métadonnées. L'organisme a entrepris un examen proactif pour tenter de comprendre ce qui s'était produit et a également mené une évaluation de l'incidence de cet événement sur la vie privée. En nous fondant sur la série de mesures de protection de la vie privée en vigueur, nous avons conclu que cette incidence était faible.

Les employés du CST ont ensuite collaboré étroitement avec le Commissaire du CST, qui était au beau milieu d'un examen des métadonnées au sein de notre organisme, et il a noté dans son rapport — et peut-être exprimé publiquement — qu'à son avis, l'incident lié aux métadonnées n'était pas intentionnel, c'est-à-dire qu'il s'agissait d'une déficience technique des systèmes, et que nous avions collaboré pleinement avec lui pour régler ce problème.

En ce qui concerne les mesures prises, nous n'avons pas repris le partage des métadonnées. Lorsqu'il s'est prononcé sur cet incident, le ministre a dit qu'il devait être convaincu que le système que nous mettions en place était solide et qu'il était équipé des mesures de protection de la vie privée requises. Nous sommes en train de concevoir un système qui fera ces deux choses, c'est-à-dire qu'il aidera à protéger la sécurité nationale du Canada, mais qu'il veillera également à ce que les mesures de protection de la vie privée soient adéquates. Lorsque nous serons en mesure de proposer un tel système au ministre, nous le soumettrons à son examen.

Le président : J'ai une question de suivi. Qu'avez-vous fait des métadonnées qui avaient été partagées lorsqu'on s'est rendu compte que leur partage ne faisait pas partie de votre mandat législatif? Où sont-elles? Ont-elles été détruites?

Mme Bossenmaier : Comme je l'ai mentionné, une série de mesures de protection de la vie privée sont en œuvre pour protéger la confidentialité des métadonnées qui sont partagées. Nous avons utilisé ces mesures de protection de la vie privée pour déterminer que l'incidence de ce partage sur la vie privée était faible. Nous n'avons pas supprimé ces métadonnées de nos systèmes du Groupe des cinq, car ces systèmes suivent des horaires de conservation et d'élimination qui entraîneront la suppression de ces métadonnées au cours de leurs activités courantes.

Again, based on the suite of privacy measures that we have in place, we also felt confident that the overall privacy impact was low.

The Chair: I could probably follow that up further, but, Senator Day, I'm going to give you the last question. Be very concise.

Senator Day: What minister?

Ms. Bossenmaier: The Minister of National Defence.

Senator Day: In your report, you stated that CSE's sophisticated cyberdefence mechanisms block over 100 million malicious cyberactions against the government every day.

Ms. Bossenmaier: Correct.

Senator Day: Is each of these malicious cyberactions a cyberattack, as we've discussed? Are they synonymous?

Ms. Bossenmaier: You have attack. You have infiltration. You have incident. The best way to describe this is these are probes. These are probes looking at vulnerabilities against the Government of Canada's systems. These are actions looking to map our systems, to probe, to look for vulnerabilities. As to that number, an extremely alarming number, 100 million per day, we've seen significant growth in that number, senator, over the last number of years. If I had to go back a number of years, it was probably at 60 million, 70 million and now to 100 million. So there has been a significant increase. That's just people trying to figure out the vulnerabilities, probing, trying to understand, map, sort of as the first foray into a full-blown cyberattack.

Senator Day: A pre-attack.

Ms. Bossenmaier: You could use that terminology.

The Chair: I would like to thank Ms. Bossenmaier for coming before us. We appreciate what you had to say.

In our third and fourth panels today, we'll continue our look at threats to the security of Canada, including but not limited to cyberespionage, threats to critical infrastructure, terrorist recruitment and financing, and terrorist operations and prosecutions. Our focus in the next two panels this afternoon will be the threats to Canada's critical infrastructure.

Joining us on our third panel is Stephanie Carvin, Assistant Professor of International Relations at the Norman Paterson School of International Affairs at Carleton University. Ms. Carvin earned her PhD from the London School of Economics and recently published a book entitled *Science, Law, Liberalism and the American Way of Warfare: The Quest for*

Encore une fois, en nous fondant sur la série de mesures de protection de la vie privée en vigueur, nous pouvions affirmer avec confiance que dans l'ensemble, les répercussions sur la vie privée étaient faibles.

Le président : Je pourrais vous poser d'autres questions sur le sujet, mais je vais permettre au sénateur Day de poser la dernière question. Veuillez être très bref.

Le sénateur Day : Quel ministre?

Mme Bossenmaier : Le ministre de la Défense nationale.

Le sénateur Day : Dans votre rapport, vous avez indiqué que les mécanismes de cyberdéfense complexes du CST bloquent, chaque jour, plus de 100 millions de cyberactions malveillantes contre le gouvernement.

Mme Bossenmaier : C'est exact.

Le sénateur Day : Chaque cyberaction malveillante était-elle une cyberattaque, comme nous en avons discuté? Ces deux termes sont-ils des synonymes?

Mme Bossenmaier : Il y a des attaques, il y a des infiltrations et il y a des incidents. La meilleure façon de les décrire, c'est de les comparer à des sondes. Ces sondes cherchent les vulnérabilités dans les systèmes du gouvernement du Canada. Elles dressent des cartes de nos systèmes afin de cerner leurs vulnérabilités. Le nombre de ces intrusions, c'est-à-dire 100 millions par jour, est extrêmement inquiétant, et il a nettement augmenté ces dernières années, sénateur. En effet, il y a quelques années, il était probablement de 60 ou de 70 millions, et maintenant, il est de 100 millions. Il a donc nettement augmenté. Il s'agit seulement de gens qui tentent de cerner les vulnérabilités, de sonder les systèmes et de tenter de les comprendre et d'en dresser la carte; c'est en quelque sorte une première intrusion dans le cadre d'une cyberattaque complète.

Le sénateur Day : C'est une attaque préliminaire.

Mme Bossenmaier : Vous pourriez utiliser cette terminologie.

Le président : J'aimerais remercier Mme Bossenmaier d'avoir comparu devant le comité. Nous vous sommes reconnaissants de vos commentaires.

À l'aide de notre troisième et de notre quatrième groupe de témoins, nous continuerons d'examiner les menaces à la sécurité du Canada, notamment le cyberespionnage, les menaces aux infrastructures essentielles, le recrutement et le financement des terroristes et les opérations antiterroristes et les poursuites contre les terroristes. Nos deux prochains groupes de témoins se concentreront sur les menaces contre les infrastructures essentielles du Canada.

Nous accueillons donc, dans le troisième groupe de témoins, Stephanie Carvin, professeure adjointe, Relations internationales, Norman Paterson School of International Affairs, Université Carleton. Mme Carvin est détentrice d'un doctorat de la London School of Economics et a récemment publié un livre intitulé *Science, Law, Liberalism and the American Way of Warfare : The*

Humanity in Conflict. She currently teaches in the areas of critical infrastructure protection, technology and warfare, and foreign policy.

Next to Ms. Carvin is Adam Chapnick, Deputy Director of Education at the Canadian Forces College and Professor of Defence Studies at the Royal Military College of Canada. Mr. Chapnick holds an M.A. in international affairs from Carleton University and a PhD in history from the University of Toronto. He has published six books and over 40 academic essays and book chapters. He currently teaches courses in Canadian government, strategic decision making and Canadian foreign policy. He is also a frequent commentator on international security issues and Canada-U.S. relations.

Welcome to the committee. I understand each of you has an opening statement. Mr. Chapnick, if you want to begin.

Adam Chapnick, Professor and Deputy Director, Education, Canadian Forces College, Department of National Defence, as an individual: Thanks very much to the committee for inviting me. The reason we thought I might go first is that Dr. Carvin is the real expert here. I have some general comments to make as someone who teaches strategic decision making at the federal level in a national security program. The views that I have for you today are my own. Although I'm technically a Department of National Defence employee, I have complete academic freedom. So the views are from me, not from DND.

The main message I hope you take away from my comments is as follows: I know Michel Coulombe spoke to you two weeks ago, and he mentioned the importance of the United States and Canada-U.S. relations to any discussion of national security. My point is that any discussion of Canadian national security cannot underestimate the critical importance of maintaining a strong, stable relationship with the United States. I'd actually go further than Mr. Coulombe and suggest that a breakdown of cooperation at the Canada-U.S. border is a greater threat to long-term Canadian prosperity than any so-called national security threat. That border is critical to our prosperity.

In that context, there are four implications that I'd suggest this committee take into consideration when we're talking about national security as it relates to critical infrastructure. I think there are four measurements of security that we should be thinking about.

The first is the physical and cyber, the traditional idea of security as it relates to Canada's critical infrastructure, the most obvious one.

Quest for Humanity in Conflict. Elle enseigne actuellement dans les domaines de la protection, la technologie et la guerre liées aux infrastructures essentielles et de la politique étrangère.

Nous accueillons également Adam Chapnick, directeur adjoint, Éducation, Collège des Forces canadiennes, et professeur en études de la défense au Collège militaire royal du Canada. M. Chapnick détient une maîtrise en affaires internationales de l'Université Carleton et un doctorat en histoire de l'Université de Toronto. Il a publié six ouvrages et plus de 40 essais universitaires et chapitres d'ouvrages. Il donne actuellement des cours sur le gouvernement canadien, la prise de décisions stratégiques et la politique étrangère du Canada. Il commente fréquemment les questions de sécurité internationale et les relations entre le Canada et les États-Unis.

Je vous souhaite la bienvenue au comité. D'après ce que je comprends, vous livrerez chacun un exposé. Monsieur Chapnick, nous vous écoutons.

Adam Chapnick, professeur et directeur adjoint, Éducation, Collège des Forces canadiennes, ministère de la Défense nationale, à titre personnel : J'aimerais remercier les membres du comité de m'avoir invité à comparaître. Nous avons décidé qu'il serait préférable que je livre mon exposé en premier, car Mme Carvin est une experte dans le domaine. J'aimerais formuler quelques commentaires généraux en ma qualité de professeur qui enseigne la prise de décisions stratégiques au fédéral dans le cadre d'un programme de sécurité nationale. Je vous parlerai aujourd'hui de mes opinions personnelles. Même si je suis techniquement un employé du ministère de la Défense nationale, je profite d'une liberté universitaire complète. Les opinions que je vous communiquerai aujourd'hui sont donc les miennes, et non celles du MDN.

Voici le message principal que j'aimerais que vous reteniez de ma comparution. Comme l'a mentionné Michel Coulombe devant votre comité il y a deux semaines, les États-Unis et les relations entre le Canada et les États-Unis sont des sujets importants qui devraient figurer dans toutes les discussions sur la sécurité nationale. J'aimerais faire valoir que dans toute discussion sur la sécurité nationale du Canada, on ne peut se permettre de sous-estimer l'importance essentielle du maintien d'une relation solide et stable avec les États-Unis. J'irais encore plus loin que M. Coulombe et j'avancerais qu'une rupture de la coopération transfrontalière entre le Canada et les États-Unis représenterait une menace plus grande pour la prospérité canadienne à long terme que toute autre menace à la sécurité nationale. En effet, cette frontière est essentielle au maintien de notre prospérité.

Dans ce contexte, je recommande aux membres du comité de tenir compte de quatre hypothèses lorsqu'on parle de la sécurité nationale des infrastructures essentielles. Je crois donc que nous devrions tenir compte de quatre mesures de la sécurité.

La première concerne la sécurité, tant matérielle que numérique, c'est-à-dire la sécurité des infrastructures essentielles du Canada au sens traditionnel — la plus évidente.

The second is the security of shared North American critical infrastructure, again, in the traditional sense of cyber and physical.

The third and fourth are the ones I'd like to add. The third is the Canadian public's perception of the security of Canadian and North American critical infrastructure. And the fourth is American perceptions of Canada's commitment to secure Canadian and North American critical infrastructure. So there's Canadian, North American, the Canadian public's perception and American perceptions of what we are actually doing.

With those measurements in mind, I have four operational-level recommendations to meet and manage these implications.

First of all, Public Safety Canada must continue to push ahead on its 2014-17 Action Plan for Critical Infrastructure, with its focus on three things: one, sustaining and enhancing inter-Canadian partnerships; two, sharing and protecting information; and three, implementing an all-hazards management approach. That's the first step.

The second step is that when the new United States president arrives in 2017, I think that Public Safety Canada must ensure that the 2010 Canada-United States Action Plan for Critical Infrastructure is renewed and reinvigorated. I think that is critical.

Third, I believe that Canadians, and especially service providers, must be made better aware of how they can personally contribute to national and continental security.

Fourth, I think that Americans must be made aware of what Canadians and their government are doing to promote national and continental security.

There are a couple of risks that come with pursuing these recommendations. I'll identify two of them, and then I'll suggest some mitigation efforts that can be made.

The first risk is that if we educate Canadians about the security threats facing this country's and North America's critical infrastructure, we can inadvertently provide fodder for U.S. isolationists and economic protectionists who seek to thicken their northern border to support their own domestic industries. If we make this country look insecure, those who want to manipulate the market to support their own can more easily do that.

Second, in educating Americans about Canadian efforts to better coordinate continental security, we can inadvertently create fear among certain members of the Canadian public that the United States is already too intimately involved in the Canadian national security process. Such fear, however irrational, could

La deuxième concerne la sécurité des infrastructures essentielles nord-américaines communes, encore une fois, au sens traditionnel de la sécurité matérielle et numérique.

La troisième et la quatrième mesure sont celles que j'aimerais ajouter. La troisième concerne la perception de la population canadienne à l'égard de la sécurité des infrastructures essentielles du Canada et de l'Amérique du Nord. Et la quatrième mesure concerne la perception des Américains à l'égard de l'engagement pris par le Canada de protéger les infrastructures essentielles du Canada et de l'Amérique du Nord. Il y a donc la perception des Canadiens et des Américains, à l'échelle du Canada et de l'Amérique du Nord, à l'égard de nos activités dans ce domaine.

En gardant ces mesures à l'esprit, j'aimerais formuler quatre recommandations opérationnelles visant la gestion de ces hypothèses.

Tout d'abord, Sécurité publique Canada doit continuer de mettre en œuvre son Plan d'action sur les infrastructures essentielles 2014-2017, en insistant particulièrement sur trois éléments. Tout d'abord, soutenir et élargir les partenariats intercanadiens. Deuxièmement, partager et protéger l'information. Troisièmement, mettre en œuvre une approche de gestion tous risques. C'est la première étape.

La deuxième étape, c'est que Sécurité publique Canada devrait veiller, à mon avis, à ce que le Plan d'action canado-américain sur les infrastructures essentielles de 2010 soit renouvelé et redynamisé lors de l'élection du nouveau président ou de la nouvelle présidente des États-Unis en 2017. Je crois que c'est essentiel.

Troisièmement, je crois que les Canadiens, et surtout les fournisseurs de services, doivent être mieux informés de ce qu'ils peuvent faire personnellement pour contribuer à la sécurité nationale et continentale.

Quatrièmement, je crois que les Américains doivent savoir ce que les Canadiens, et leur gouvernement, font pour promouvoir la sécurité nationale et continentale.

Donner suite à ces recommandations comporte quelques risques. Je vais cerner deux d'entre eux, et je suggérerai des efforts d'atténuation qui peuvent être entrepris.

Le premier risque, c'est qu'en instruisant les Canadiens sur les menaces à la sécurité qui planent sur les infrastructures essentielles de leur pays et de l'Amérique du Nord, il se peut que, sans le vouloir, nous amenions de l'eau au moulin des isolationnistes et des protectionnistes économiques américains qui cherchent à renforcer leur frontière au nord pour soutenir leurs industries nationales. Si nous générons des doutes sur la sécurité de notre pays, nous facilitons la tâche à ceux qui souhaitent manipuler le marché pour appuyer leur propre marché.

Deuxièmement, en instruisant les Américains sur les efforts déployés par les Canadiens pour mieux coordonner la sécurité continentale, nous pourrions, sans le vouloir, faire craindre à la population canadienne que les États-Unis participent déjà trop intimement au processus de sécurité nationale canadien. De telles

limit the political capital available to the Canadian government to support increased continental integration, which I believe will likely be necessary on the security side to maintain U.S. confidence and a relatively open yet still safe Canada-U.S. border.

How do we manage these risks? First of all, keeping in mind that there is no perfect security solution, I think we need to focus on establishing a narrative that supports increased North American resilience in the face of what will inevitably be demanding security challenges in the future. This means stronger partnerships at three levels: first, between Canadians and their government; second, between Canadian federal departments, their provincial and municipal counterparts, private owners and operators of critical infrastructure, and private industry more broadly; and third, between Canada and the United States on as many levels as possible.

Second, although this committee in particular has had a lot of success in the past drawing public attention to national security risks by highlighting Canadian vulnerabilities, in the context of this challenge, I recommend that great caution be taken in using fear to spur Canadians to action. Drawing extensive attention to Canadian and North American vulnerabilities, without paying sufficient notice to progress that has and will be made in terms of mitigation efforts, risks encouraging Canada's American partners — who will continue, I believe, to privilege security over trade — to conclude that an open border with Canada is a liability that cannot be countenanced.

In sum, to reiterate, any discussion of Canadian national security cannot underestimate the critical importance of maintaining a strong, stable relationship with the United States. Breakdown of cooperation at the border is the greatest threat that we face as a country when it comes to security and prosperity. It follows that we must focus — and this committee should focus, I hope — not just on the reality of the threats to Canadian and North American critical infrastructure — and as Dr. Carvin will suggest, they're very real — but also on the commitment of the government and the people of Canada to manage those threats appropriately. I'll stop there. Thank you.

Stephanie Carvin, Assistant Professor, International Relations, Norman Paterson School of International Affairs, as an individual: Thank you for inviting me to speak to you today. By way of background, I've worked as a national security analyst with the government for three years. Now at Carleton, I teach at the Norman Paterson School of International Affairs, and specifically in our master's program in infrastructure protection and international security.

craintes, même si elles sont irrationnelles, pourraient limiter le capital politique dont dispose le gouvernement canadien pour soutenir l'intégration continentale accrue qui sera vraisemblablement nécessaire sur le plan de la sécurité pour maintenir la confiance des États-Unis et une frontière canado-américaine relativement ouverte, mais toujours sécuritaire.

Comment gérons-nous ces risques? Tout d'abord, en gardant à l'esprit qu'il n'existe pas de solution parfaite en matière de sécurité, je pense que nous devrions nous concentrer sur l'élaboration d'un discours qui appuie une résilience nord-américaine accrue face aux défis qui nous attendent inévitablement à l'avenir en matière de sécurité. Cela se traduit par la promotion de partenariats plus solides à trois niveaux : tout d'abord, entre les Canadiens et leur gouvernement; deuxièmement, entre les ministères fédéraux canadiens, leurs homologues provinciaux et municipaux, les propriétaires et les exploitants privés d'infrastructures essentielles, ainsi que le secteur privé en général; troisièmement, entre le Canada et les États-Unis, sur le plus grand nombre de plans possible.

Deuxièmement, même si votre comité a déjà réussi à attirer l'attention du grand public sur les risques relatifs à la sécurité nationale en mettant en évidence les vulnérabilités canadiennes, dans le contexte de ce défi, je recommande d'exercer une grande prudence avant de recourir à la peur pour inciter les Canadiens à l'action. En attirant trop l'attention sur les vulnérabilités canadiennes et nord-américaines sans accorder suffisamment d'attention aux progrès qui ont été et qui seront réalisés en matière d'atténuation, on risque d'inciter les partenaires américains du Canada — qui continueront, je crois, de privilégier la sécurité au détriment du commerce — à conclure qu'une frontière ouverte avec le Canada est un risque que l'on ne peut plus tolérer.

En somme, je rappelle qu'on ne peut jamais, dans les discussions sur la sécurité nationale du Canada, sous-estimer l'importance fondamentale d'une relation forte et stable avec les États-Unis. L'effritement de la coopération à la frontière est la plus grande menace à laquelle notre pays est confronté sur les plans de la sécurité et de la prospérité. Par conséquent, nous devons nous concentrer non seulement sur les menaces à l'infrastructure essentielle canadienne et nord-américaine (et comme Mme Carvin l'expliquera, ces menaces sont bien réelles), mais aussi sur l'engagement du gouvernement et de la population canadienne à gérer ces menaces convenablement. J'espère que c'est également la priorité de ce comité. Je vais m'arrêter là. Merci.

Stephanie Carvin, professeure adjointe, Relations internationales, Norman Paterson School of International Affairs, à titre personnel : Je vous remercie de m'avoir invitée à prendre la parole devant vous aujourd'hui. Pour vous mettre en contexte, j'ai travaillé comme analyste en matière de sécurité nationale au sein du gouvernement pendant trois ans. Je suis désormais à Carleton, où j'enseigne à la Norman Paterson School of International Affairs, particulièrement dans le programme de maîtrise sur la protection de l'infrastructure et la sécurité internationale.

Today I will keep my remarks to what I see as the main national security threats to critical infrastructure and key challenges for policy-makers going forward.

In my view, national security threats to critical infrastructure can be characterized as diffuse, dynamic and fluid. First, these threats are diffuse in that they are spread out amongst a wide variety of actors. For example, many recent studies have demonstrated that there is no obvious profile for those who seek to engage in extremist violence. It is true that many are young and male, but there's diversity within this Canadian cohort of extremists, including young women. Additionally, whereas during the Cold War threats from states emanated from the militaries and their intelligence services, states with hostile intentions towards Canada and the West today have substantially widened their tool kits to achieve their ends. This includes economic and cyber instruments.

Second, threats to critical infrastructure are dynamic. They are constantly changing and adapting to their environment. Violent extremists and their supporters are able to capitalize on information flows enhanced by social media platforms that increasingly allow for mass communication but also targeted propagandizing and facilitations. States can also take advantage of new technologies to enhance their reach into our society and infrastructures, or monitor those they see as rivals and potential challengers to their authority within our borders.

Third, threats to critical infrastructure are fluid. They are malleable and can adapt in order to move around obstacles put in their path. This enhances their resiliency in the face of counterterrorism pressure, counterespionage strategies, and national security efforts against them.

Importantly, these three characteristics highlight a strong uniting feature of these major threats to our critical infrastructure, namely, the fact that they thrive in network form. This allows them to access areas they may not otherwise have access to, to easily engage with others around the world, and to exploit nodes that connect high-tech pathways to ancient smuggling routes still exploited today for illicit ends. Paradoxically, this means these threats require the critical infrastructure networks they threaten.

In this sense, it's important to recognize that the threat is not just nefarious elements that seek to destroy critical infrastructure, but also those that seek to exploit one critical infrastructure sector in order to achieve its aims against another.

Je limiterai mes observations d'aujourd'hui à ce que je considère comme les principales menaces à la sécurité nationale et à l'infrastructure essentielle, ainsi que les principaux défis qui attendent les décideurs.

À mon avis, on peut caractériser les menaces à la sécurité nationale et à l'infrastructure essentielle de diffuses, dynamiques et fluides. Premièrement, ces menaces sont diffuses en ce sens qu'elles émanent d'une grande variété d'acteurs. Par exemple, beaucoup d'études récentes montrent qu'il n'y a pas de profil évident des personnes susceptibles de s'adonner à la violence extrémiste. Il est vrai que bon nombre de ces personnes sont jeunes et de sexe masculin, mais il y a une grande diversité dans la cohorte canadienne des extrémistes, qui comprend aussi des jeunes femmes. En outre, si pendant la guerre froide, les menaces à la sécurité nationale émanaient des armées et des services de renseignement des États, de nos jours, les États ayant des intentions hostiles envers le Canada et l'Occident ont beaucoup élargi leur éventail d'outils pour parvenir à leurs fins. Ils englobent désormais des tactiques économiques et informatiques.

Deuxièmement, les menaces à l'infrastructure essentielle sont dynamiques. Elles changent constamment et s'adaptent à leur environnement. Les extrémistes violents et leurs sympathisants peuvent tirer profit du flux d'information exponentiel des médias sociaux, qui permettent de plus en plus non seulement la communication de masse, mais aussi la propagande ciblée et la facilitation de la violence. Les États peuvent également tirer parti des nouvelles technologies pour rejoindre davantage notre société et nos infrastructures ou pour garder à l'œil leurs présumés rivaux et les opposants potentiels à leur autorité à l'intérieur de nos frontières.

Troisièmement, les menaces à l'infrastructure essentielle sont fluides. Elles sont malléables et peuvent s'adapter pour contourner les obstacles qui se dressent sur leur chemin. Elles s'en trouvent d'autant plus résilientes face à la pression antiterroriste, aux stratégies de contre-espionnage et aux efforts de protection nationale à leur encontre.

Il importe de remarquer que ces trois caractéristiques ont un point commun fort, puisque les principales menaces à notre infrastructure essentielle se trouvent multipliées par la force du réseau. Le réseau leur donne accès à des zones autrement inaccessibles, leur permet de tisser facilement des liens partout dans le monde et d'exploiter des noyaux qui combinent la haute technologie aux anciennes voies du trafic clandestin toujours exploitées de nos jours à des fins illicites. Paradoxalement, cela signifie que ces menaces ont besoin des réseaux de l'infrastructure essentielle qu'elles ciblent.

Ainsi, il faut reconnaître que la menace ne provient pas seulement de vils éléments qui cherchent à détruire l'infrastructure essentielle, mais également d'individus qui cherchent à exploiter un secteur de l'infrastructure essentielle pour parvenir à ses fins contre l'autre.

I will highlight three major threats to critical infrastructure that exemplify the characteristics I have just spoken of.

First, extremist violence. Activities that support violent extremism include radicalization, facilitation, financing and conducting attacks. The threats from al Qaeda and Islamic State-inspired groups are the paramount threat to Canada. They manifest into three separate threats to critical infrastructure: extremist travellers using and threatening transportation; those who wish to conduct attacks within our borders, whether a lone act or attacks or those approved or even directed by the leadership of extremist groups overseas; and finally, the financing and facilitation of these individuals on Canadian soil.

However, it is essential that we recognize that the extremist attacks do not come from one source. This is especially true for critical infrastructure in Canada. It is worth remembering that every attack against critical infrastructure between 2004 and October 2014 was allegedly conducted by either left-wing groups or single-issue extremist groups. This includes the 2004 bombing of a hydro tower in Quebec, claimed by Résistance internationaliste; the May 2010 bombing of an RBC bank in Ottawa; and the July 2010 bombing of a Canadian Forces recruitment centre in Trois-Rivières, Quebec.

Second, cybersecurity. It is well known that Canada is regularly subjected to hostile cyberoperations. The majority of these are cyberexploitation attacks that seek to gain information, not only from governments but from private companies and institutions that states and private actors believe will give them tactical and strategic advantages in business, military and foreign affairs.

However, we are increasingly seeing cyberattacks that may cause physical damage to supervisory control and data acquisition, or SCADA, systems and critical infrastructure itself. The 2012 attack against Saudi Aramco and the 2013 data breach of a dam in New York are illustrative of the growing risks.

Finally, there are cyberactivities such as ransomware viruses which blackmail operators for cash, including this year a hospital in California. In fact, a recent report suggests that up to 30 per cent of ransomware attacks are targeted at hospitals. These operations may not constitute a threat to the security of Canada, but they may be funding illicit activities.

The final threat is state-owned enterprises, or SOEs. In my view, Canada needs to rethink its strategy regarding SOEs. While Canadian infrastructure requires foreign investment, the extent to

Je vais vous donner trois exemples de graves menaces à l'infrastructure essentielle qui illustrent les caractéristiques que je viens de décrire.

Il y a d'abord la violence extrémiste. Les activités qui favorisent l'extrémisme violent comprennent la radicalisation, la facilitation, le financement et l'orchestration d'attaques. Les menaces exercées par Al-Qaïda et les groupes inspirés par l'État islamique sont les principales menaces qui pèsent contre le Canada. Elles se manifestent sous la forme de trois types de menaces à l'infrastructure essentielle : il y a les voyageurs extrémistes qui utilisent et menacent l'infrastructure de transport; il y a les personnes qui souhaitent lancer des attaques de l'intérieur de nos frontières, qui peuvent être l'œuvre d'un loup solitaire ou être approuvées ou même dirigées par des dirigeants de groupes extrémistes à l'étranger; finalement, il y a le financement et la facilitation des activités de ces personnes en sol canadien.

Cependant, il est essentiel de reconnaître que les attaques extrémistes ne proviennent pas toutes d'une même source. C'est particulièrement vrai des attaques contre l'infrastructure essentielle du Canada. N'oublions pas que toutes les attaques commises contre l'infrastructure essentielle entre 2004 et octobre 2014 seraient l'œuvre soit de groupes de gauche, soit de groupes extrémistes défendant une cause particulière. Elles comprennent l'attentat à la bombe, en 2004, contre un pylône hydroélectrique au Québec, qui a été revendiqué par Résistance internationaliste; l'attentat à la bombe de mai 2010 contre une banque de la RBC à Ottawa; ainsi que l'attentat à la bombe de juillet 2010 contre un centre de recrutement des Forces canadiennes à Trois-Rivières, au Québec.

Deuxièmement, il y a la cybersécurité. Il est bien connu que le Canada fait souvent l'objet de cyberopérations hostiles. La majorité des cyberattaques visent à obtenir de l'information, non seulement des gouvernements, mais aussi d'entreprises et d'institutions privées que des États ou divers autres acteurs estiment susceptibles de leur procurer des avantages tactiques et stratégiques militaires, commerciaux ou en politique étrangère.

Cependant, nous observons de plus en plus de cyberattaques susceptibles de causer des dommages physiques aux réseaux et à l'infrastructure essentielle des systèmes de contrôle et d'acquisition de données (ou SCADA) eux-mêmes. L'attaque de 2012 contre Saudi Aramco et la violation de données de 2013 sur un barrage à New York illustrent bien ces risques croissants.

Enfin, il y a les cyberactivités comme la transmission de virus destinés à réclamer des rançons, comme l'envoi de courriels frauduleux pour exiger de l'argent, et il y en a eu cette année pour un hôpital en Californie. En fait, un rapport récent laisse entendre que jusqu'à 30 p. 100 de ce type d'attaques visent des hôpitaux. Ces activités ne constituent peut-être pas de menaces à la sécurité du Canada, mais elles peuvent servir à financer des activités illicites.

Le dernier type de menace est celui que représentent les entreprises d'État. À mon avis, le Canada doit repenser sa stratégie concernant les entreprises d'État. Si l'infrastructure

which we should allow companies with direct or clandestine links to foreign governments to control the backbone of our economy and society is something that our leadership must reflect on, especially when these countries have shown hostile intentions towards Canadian interests. Aided by the resources of a state, including information gathered by cyberespionage, SOEs have an unmatched advantage in our system, based on the rule of law and the notion of free and fair competition, which may result in a skewering of the playing fields and an uncompetitive advantage.

Although Canada made changes to its Investment Canada Act following CNOOC's purchase of Nexen in 2012, challenges remain. SOEs can easily find ways to own less than 50 per cent of a company and still maintain control over it. They can also find ways to disguise their ties to states through layers of legitimate and shell companies, rendering it very difficult for Canadian authorities who may actually be calling the shots.

In my final few minute I will speak about what I see are the central challenges ahead for policy-makers. The first major challenge is the balancing of threat reduction in ways that do not inhibit the flows of the networks I discussed earlier. In enhancing our border security, we do not want to risk establishing impediments to tourism and trade. While protecting our companies from SOEs, we do not want to block them from much-needed foreign investment.

Second, the very nature of our system that makes critical infrastructure work is also what makes it vulnerable. This is true in at least three ways. First, critical infrastructure sectors are of necessity linked to one another. A collapse in one may have catastrophic effects in another. Second, redundancy in these systems is important, but it also serves to add complexity and even potentially make them more vulnerable with more components in a system. Finally, our federal system of government and Canada's capitalist system means that responsibility in our system is shared over many levels of government and among many actors. Developing a framework in which to develop standards and strengthen our infrastructure has been a challenge for years and is likely to remain so.

The irony of major attacks and disasters is that they provoke moments that a nation looks to its government for leadership at the very time it is least capable of acting, and this is the central challenge for government and this committee going forward.

Thank you for inviting me to speak.

Senator Mitchell: Thanks to both of you. These are provocative presentations. I'm very interested, Professor Chapnick, in the relationship you draw between fomenting fear and emphasizing

canadienne nécessite effectivement des investissements étrangers, nos dirigeants doivent réfléchir à la question de savoir si nous devons autoriser des entreprises ayant des liens directs ou clandestins avec des gouvernements étrangers à contrôler l'épine dorsale de notre économie et de notre société, particulièrement si ces pays ont déjà démontré des intentions hostiles à l'égard des intérêts canadiens. Grâce aux ressources d'État, dont la collecte de renseignements par le cyberespionnage, les entreprises d'État jouissent d'un avantage sans commune mesure dans notre système, qui se font sur la primauté du droit et le concept de la concurrence libre et juste, ce qui peut fausser les règles du jeu et leur conférer un avantage concurrentiel.

Bien que le Canada ait modifié sa Loi sur Investissement Canada après l'acquisition de Nexen par CNOOC, en 2012, certaines difficultés demeurent. Les entreprises d'État peuvent facilement se porter acquéreuses de moins de 50 p. 100 des parts d'une entreprise tout en en préservant le contrôle. Elles peuvent également trouver le moyen de maquiller leurs liens avec des États par une succession de sociétés légitimes et fictives, ce qui rend la tâche très difficile pour les autorités canadiennes qui doivent établir les règles.

Je prendrai les quelques minutes qu'il me reste pour vous parler des principaux défis qui attendent nos décideurs. Le premier consiste à trouver le juste équilibre entre la réduction de la menace et le maintien du bon fonctionnement des réseaux dont j'ai déjà discuté. Nous ne voudrions pas qu'une sécurité accrue à la frontière pose des obstacles au tourisme et au commerce. Bien que nous voulions protéger nos entreprises des entreprises d'État, nous ne voulons pas leur bloquer l'accès aux investissements étrangers dont elles ont tant besoin.

Ensuite, la nature même du système qui rend notre infrastructure essentielle fonctionnelle la rend également vulnérable, cela pour au moins trois raisons. Premièrement, les secteurs de l'infrastructure essentielle sont nécessairement liés les uns aux autres. L'effondrement d'un secteur peut avoir des effets catastrophiques sur l'autre. Deuxièmement, si la redondance est importante dans ce système, elle y ajoute de la complexité et peut même accroître sa vulnérabilité en raison du plus grand nombre de composantes. Enfin, le régime fédéral et capitaliste du gouvernement au Canada est tel que la responsabilité est partagée entre divers ordres de gouvernement et divers acteurs. Depuis longtemps, il apparaît difficile d'établir un cadre nous permettant de nous doter de normes et de renforcer notre infrastructure, et la tâche risque fort de rester ardue.

L'ironie, c'est que les grandes attaques et catastrophes provoquent des moments où un pays s'attend à ce que son gouvernement fasse preuve de leadership au moment même où il est le moins apte à agir, c'est là le principal défi pour le gouvernement et le comité.

Je vous remercie de m'avoir invitée à vous parler.

Le sénateur Mitchell : Je vous remercie tous les deux. Ce sont là des présentations provocatrices. J'aimerais beaucoup, monsieur Chapnick, que vous me parliez un peu plus de la relation que vous

fear in Canada and its relationship to trade with the United States. You would at least include in that fomenting of fear, fear about radical attacks and terrorism, would you not?

Mr. Chapnick: Historically, one of the ways to get Canadians' attention on the challenges that we face in national security is to draw attention to vulnerabilities that we already have. This committee has actually been extremely good at that in terms of security to airports, for example, where Canadians only learned about this largely because this committee did some work. The report was on the news, and all of a sudden Canadians were asking, "What are you doing about security at airports?"

Senator Mitchell: Do you want to say that again?

Senator White: We'd like it in writing.

Mr. Chapnick: We need to make Canadians aware, but we have a trend in the United States right now where there's a good-sized constituency that is simply looking for excuses to tighten controls at the border and looking for reasons to make it harder for Canadian goods to cross that border. If we suggest that Canada is not doing a good enough job securing its own, that is the exact information they need to justify pushing through policies that make the border thicker than it has to be.

So there's a real balance to be had between recognizing the vulnerabilities that we have but also speaking about what we're doing to deal with them, rather than just using the recognition of the vulnerabilities to get Canadians to say to their government, "What are you doing about this?" That is the fear I have. There are all sorts of vulnerabilities, including the ones you mentioned, sir.

Senator Mitchell: Until recently, the focus on dealing with the terrorist threat in Canada has really been laws, some would argue threats to civil liberties. I voted against Bill C-51. My Liberal colleagues in the Senate also voted against Bill C-51, because they felt it went too far that way.

Could either or both of you comment on the emphasis that some say — in fact, I think I've even heard Senator White suggest — that policing organizations feel that the best days of their work are when they work within the community to prevent ever having to get to a point where laws need to be applied and civil liberties need to be threatened.

There is, is there not, much more developing evidence that working within communities and catching young people who are going down the wrong path early — that such a thing is perhaps the way to emphasize — and it would be consistent with what you're saying about minimizing this fomenting of fear?

voyez entre le fait de fomenter et d'alimenter la peur au Canada et nos liens commerciaux avec les États-Unis. Quand vous parlez de fomenter la peur, vous pensez à tout le moins à la peur du terrorisme et des attaques radicales, n'est-ce pas?

M. Chapnick : L'une des façons d'attirer l'attention des Canadiens sur les risques pour notre sécurité nationale a toujours consisté à attirer l'attention sur les vulnérabilités que nous avons déjà. Le comité le fait d'ailleurs extrêmement bien lorsqu'il parle de la sécurité des aéroports, par exemple, puisque les Canadiens n'en ont entendu parler qu'en grande partie en raison des travaux du comité. Le rapport du comité a fait les manchettes et soudainement, les Canadiens se sont mis à se demander ce qu'on faisait de la sécurité dans les aéroports.

Le sénateur Mitchell : Voulez-vous répéter ce que vous venez de dire?

Le sénateur White : Nous aimerions avoir ces commentaires par écrit.

M. Chapnick : Il faut informer les Canadiens, mais il y a une tendance en ce moment, aux États-Unis, selon laquelle une bonne partie de l'électorat cherche simplement des excuses pour resserrer les contrôles à la frontière, pour rendre plus difficile le passage des produits canadiens à la frontière. Si nous laissons entendre que le Canada n'en fait pas assez pour assurer la sécurité, c'est exactement le genre d'information dont ces gens ont besoin pour justifier l'adoption de politiques qui rendraient la frontière plus hermétique.

Il faut donc vraiment mesurer nos propos; il faut reconnaître nos vulnérabilités, mais également parler de ce que nous faisons pour y remédier. Il ne faut pas simplement nous limiter à reconnaître les vulnérabilités pour que les Canadiens disent à leur gouvernement : « Que faites-vous de cela? » C'est ma crainte. Il y a toutes sortes de vulnérabilités, dont celles que vous avez mentionnées, monsieur.

Le sénateur Mitchell : Jusqu'à tout récemment, les mesures pour lutter contre la menace terroriste au Canada se sont vraiment concentrées sur les lois, et certains diraient qu'elles compromettent les libertés civiles. J'ai voté contre le projet de loi C-51. Mes collègues libéraux au Sénat ont eux aussi voté contre le projet de loi C-51, parce qu'ils estimaient qu'il allait trop loin.

Pouvez-vous, l'un ou l'autre ou tous les deux, réagir sur l'insistance avec laquelle — je pense que j'ai même entendu le sénateur White insister là-dessus — les organisations de maintien de l'ordre répètent que la partie la plus efficace de leur travail est celle qui se passe dans la collectivité, afin de prévenir les situations où il faudrait appliquer les lois et menacer les libertés civiles.

Il y a de plus en plus de preuves, n'est-ce pas, que l'idéal est de travailler dans les collectivités et d'arrêter très tôt les jeunes engagés sur la mauvaise voie, et c'est peut-être ce sur quoi il faudrait mettre l'accent. Cela va d'ailleurs dans le sens de ce que vous avez dit sur la nécessité de cesser de fomenter la peur?

Ms. Carvin: That's a very challenging question. Thank you for it.

Based on my experience in government and studying this from an academic perspective, there are two things. First, we have to be careful when we assign national security agencies a role in covering violent extremism. I don't necessarily think it's what they're good at or good for. This is why, generally speaking, I'm in support of an office for a coordinator for radicalization, which is one of the current proposals — someone who can coordinate efforts.

The challenge there is, what does coordination mean? Is it directing? Is it looking for best practices and sharing those best practices across cities? Again, it's actually a very similar problem to critical infrastructure in municipal, provincial and then federal programs. So I think that's one positive step.

The other step I would suggest in that direction in terms of a non-legal approach is that we need to responsibly widen our understanding of what the effects of terrorism are. I do not mean this in a scary way but in an empathetic way. We need to actually promote awareness that when extremists go into communities, regardless of what communities, they target children; they may try to siphon funds and redirect them to terrible purpose; and they create terrible situations in mosques, churches and things like this. This could potentially have very devastating effects on communities.

The two things I would promote are a lot of care and consideration toward the ways we think about CVE, countering violent extremism, in Canada, including what the role of the counter-radicalization office — I think I have the name entirely wrong, for which I apologize — will be; and the second thing is to have an empathetic widening of our understanding of how these extremists actually affect the communities. When a child goes off, the family of these individuals suffers terrible stigma. Maybe they can't go to their community centre anymore, and they hide it.

Those two approaches might hopefully prove fruitful.

Senator White: I have only one question. Thank you very much. Interesting commentary — and also some of the challenges we're seeing when you talk about borders with the U.S.

Do you see a need for us to have a national standard when it comes to infrastructure, whether it be at the municipal, provincial or federal level, that allows us to satisfy — rather than being treated differently, if it's New Brunswick and Maine compared to Saskatchewan and North Dakota — that we have a national standard that ensures that we are meeting a particular level when we are talking about trade with the United States?

Mme Carvin : C'est une question très difficile. Je vous en remercie.

D'après mon expérience au gouvernement et mes recherches sur la question, il y a deux choses à retenir. D'abord, il faut être prudent quand on assigne aux organismes responsables de la sécurité nationale un rôle dans la lutte contre l'extrémisme violent. Je ne pense pas nécessairement que ces organismes soient les mieux placés pour le faire ni qu'ils le fassent bien. C'est pourquoi, de manière générale, je serais favorable à la création d'un bureau de coordination contre la radicalisation, comme on le propose actuellement, il pourrait y avoir quelqu'un responsable de coordonner nos efforts.

Cependant, il faut se demander en quoi consiste cette coordination. S'agit-il de diriger les efforts? S'agit-il de déterminer quelles sont les meilleures pratiques pour les diffuser d'une ville à l'autre? Encore une fois, le problème est très similaire à celui qui se pose pour l'infrastructure essentielle dans les programmes municipaux, provinciaux, puis fédéraux. Je pense donc que ce serait un pas dans la bonne direction.

L'autre mesure que je recommanderais, toujours dans un cadre non judiciaire, serait d'approfondir notre compréhension des effets du terrorisme, en toute responsabilité. Je ne parle pas là de cultiver la peur, mais l'empathie. Nous devons sensibiliser les gens au fait que dans les communautés, quelles qu'elles soient, les extrémistes visent les enfants; ils peuvent essayer de siphonner des fonds et de les rediriger à des fins terribles; ils créent des situations terribles dans les mosquées, dans les églises et ailleurs. Cela peut avoir des effets dévastateurs sur les communautés.

Ce sont là deux choses à prendre vraiment en considération, à mon avis, quand nous pensons à la lutte contre l'extrémisme violent au Canada, ainsi qu'au rôle du futur bureau de lutte contre la radicalisation (je pense que je n'ai absolument pas le bon nom, je m'en excuse). Je pense aussi qu'il faut comprendre avec beaucoup plus d'empathie la façon dont ces extrémistes touchent les communautés. Quand un enfant disparaît ainsi, sa famille souffre d'une terrible stigmatisation, si bien qu'elle ne peut peut-être plus se rendre à son centre communautaire et qu'elle se cache.

J'espère que ces deux approches seront fructueuses.

Le sénateur White : Je n'ai qu'une question. Merci beaucoup. C'est un commentaire intéressant, et j'ai bien aimé également vos observations sur les risques liés à nos frontières avec les États-Unis.

Croyez-vous que nous aurions besoin d'une norme nationale en matière d'infrastructure, que ce soit au niveau municipal, provincial ou fédéral, qui nous permettrait d'établir que nous respectons les critères nationaux, plutôt qu'il y ait des normes différentes au Nouveau-Brunswick, au Maine, en Saskatchewan et au Dakota du Nord, pour nous assurer de maintenir un certain niveau de sécurité pour le commerce avec les États-Unis?

Mr. Chapnick: That's a very fair question. We should have a national understanding. Given the jurisdictional challenges that we face in this federal country, having an organization like Public Safety declare to all provinces, municipalities and their relevant public sectors that "Thou shalt do things this way" could discourage some of the information sharing that we need. In other words, if they are not meeting the arbitrarily imposed national standards, they may be more inclined to not reveal such a thing. That is as opposed to, "We have some national priorities. We have a national understanding of the language we're going to use to explain what 'secure' means, and it may be that different provinces have slightly different approaches to meeting those national ideas."

The most important thing is to encourage cooperation. Imposing national standards in that context may actually discourage some of the openness and cooperation that we need.

Senator White: I appreciate that, but Public Safety Canada came to be as a result of post-9/11. The Department of Homeland Security happened in the south. It didn't include the FBI; it probably should have.

In Canada, Public Safety came about with promises of standards. We still don't have a national standard for a police officer in this country. We have 198 agencies, and they could be as different as A to Z.

Don't you think that maybe that's why Public Safety was put in place, to start identifying some of those? I'm not arguing standard or no standard, but we have nothing right now. It's absolutely right that the argument from the U.S. side could be that we're a threat or risk because, to be fair, the argument from me could be the same. I'm not convinced, either, in some cases.

Mr. Chapnick: Part of the reason Public Safety was put in place was to coordinate, because there was no central agency to wrap their heads around all of the different security-related institutions at every level that we have. More than to regularize and standardize, it was to figure out what was going on across the country. Whether Public Safety has done a good job of that is certainly up for discussion. Can they do better? Probably.

Senator White: We'll invite you back for that discussion.

Mr. Chapnick: However, I would say that given that 90 per cent of the critical infrastructure in Canada is privately owned, Public Safety doesn't have the same type of leverage to impose that it would if 90 per cent of the infrastructure in Canada were federally owned and controlled. It's not speaking from a position of power in quite the same way that it would be in other circumstances. So it would be challenging for Public Safety to do what you'd like it to do effectively.

M. Chapnick : Vous avez bien raison de poser la question. Nous avons besoin d'une compréhension nationale. Compte tenu du partage des compétences dans ce pays fédéral, si une organisation comme Sécurité publique déclare à toutes les provinces, les municipalités et leurs fonctions publiques respectives « vous devez faire les choses de telle façon », certaines administrations pourraient hésiter à communiquer des renseignements dont nous avons besoin. Autrement dit, si une administration ne respecte pas les normes nationales imposées arbitrairement, elle pourrait être tentée de ne pas le révéler. C'est différent de : « Nous avons des priorités nationales. Nous avons une compréhension nationale de la terminologie utilisée pour expliquer ce que signifie "sécuritaire", et les différentes provinces peuvent prendre des moyens légèrement différents pour respecter ces idées nationales. »

Le plus important est de favoriser la coopération. Dans ce contexte, le fait d'imposer des normes nationales pourrait réduire l'ouverture et la coopération dont nous avons besoin.

Le sénateur White : Je comprends, mais Sécurité publique Canada a été créé après les événements du 11 septembre. Son pendant au sud de la frontière est le département de la Sécurité intérieure. Il ne comprend pas le FBI, mais devrait probablement l'inclure.

Au Canada, Sécurité publique a été créé avec la promesse de normes. Nous n'avons toutefois encore aucune norme nationale pour les policiers au Canada. Il y a 198 organismes responsables de la sécurité, et leurs normes peuvent aller de A à Z.

Ne croyez-vous pas que c'est peut-être justement la raison pour laquelle Sécurité publique a été créé, pour commencer à établir des normes? Je ne cherche pas à déterminer s'il convient ou non d'établir des normes, mais nous n'avons rien en ce moment. Il est tout à fait vrai que les États-Unis pourraient prétendre que nous présentons une menace ou un risque, en toute honnêteté, puisque je pourrais défendre le même argument. Je ne suis pas convaincu non plus, dans certains cas.

M. Chapnick : Le ministère de la Sécurité publique Canada a été mis en place en partie pour coordonner nos efforts, parce qu'il n'y avait pas d'agence centrale responsable de surveiller toutes les institutions liées à la sécurité aux différents ordres de gouvernement. Il a été créé davantage pour comprendre ce qui se passait d'un bout à l'autre du pays que pour régulariser et normaliser les pratiques. Est-ce que Sécurité publique Canada s'est montré à la hauteur de la situation? Nous pourrions sûrement en discuter. Pourrait-il faire mieux? Probablement.

Le sénateur White : Nous vous réinviterons pour en discuter.

M. Chapnick : Cependant, je dirais que comme 90 p. 100 de l'infrastructure essentielle au Canada est de propriété privée, Sécurité publique Canada n'a pas le même pouvoir pour imposer ses règles que si 90 p. 100 de l'infrastructure au Canada était de propriété et sous contrôle fédéral. Il n'a pas exactement la même position d'autorité qu'il aurait dans d'autres circonstances. Il serait donc difficile pour le ministère de la Sécurité publique Canada de faire efficacement ce que vous aimeriez qu'il fasse.

Senator White: But we do it for nuclear. They're not owned by the federal Government of Canada. Whether a province owns it or it's privately owned, we do it for nuclear across this country right now.

So you're suggesting we couldn't do it for other high-level infrastructure?

Mr. Chapnick: I think that nuclear has a special way of getting into the public mindset that allows people to look at it with different rules than they would, say, hydro. People hear nuclear, they think of Hiroshima or Nagasaki, in which case their flexibility on control is different than —

Senator White: Great answer. Thank you.

Senator Beyak: Thank you for your excellent presentations. You have a great understanding of what we have to face.

I was interested in what you said about the border, because given that so many things are dependent on us cooperating and getting along — I'm thinking of the defence strategies, and the rail and highway systems — should we be moving toward some sort of bilateral agreement? Those are practices that they already do. Can we learn from them or other countries?

I liked what you said about making sure we keep it balanced — recognize the threat but also keep the border open.

Mr. Chapnick: I'll try to answer generally, and then Stephanie can answer in more detail.

This 2010 Canada-United States Action Plan for Critical Infrastructure is the beginning of that. It needs to be reinvigorated with a new American administration, but that is the place to go there. Encouraging this government to put some emphasis on that organization is not a bad thing.

Ms. Carvin: I would echo that.

The other thing I would suggest, though, is that when we're talking about the U.S. and Canada, one of the challenges — and I teach this in my class — is that we haven't actually really been able to define "critical infrastructure." Canada and the U.S. have sectors that we've defined, but what within those sectors is critical is really up for debate. For example, I've seen reports from the United States that suggest that tourism sites are critical infrastructure, as they're important for morale and the economy.

So that's one of the challenges we have, namely, understanding the principle of criticality in these systems.

Le sénateur White : Nous le faisons pourtant pour le nucléaire. Les centrales n'appartiennent pas au gouvernement fédéral du Canada. Que les infrastructures appartiennent à une province ou à une société privée, nous le faisons déjà pour le nucléaire au Canada en ce moment.

Laissez-vous entendre que nous ne pourrions pas faire de même pour d'autres d'infrastructures de haut niveau?

M. Chapnick : Je pense que le nucléaire occupe une place spéciale dans l'esprit du public, qui permet d'envisager des règles différentes de celles qui s'appliqueraient à l'hydroélectricité, par exemple. Quand on entend le mot « nucléaire », on pense à Hiroshima ou à Nagasaki, de sorte que la prédisposition au contrôle n'est pas la même que...

Le sénateur White : Excellente réponse. Merci.

La sénatrice Beyak : Je vous remercie de ces excellents exposés. Vous comprenez très bien les défis auxquels nous sommes confrontés.

Vos propos sur la frontière ont capté mon attention, parce qu'il y a tellement de choses qui dépendent de notre bonne coopération et de notre bonne entente. Je pense aux stratégies de défense, au réseau ferroviaire, aux autoroutes. Devrions-nous envisager une forme d'entente bilatérale? Il en existe déjà. Pourrions-nous apprendre des ententes déjà en place ou d'autres pays?

J'ai aimé ce que vous avez dit sur l'équilibre : il faut reconnaître la menace, mais tout de même garder la frontière ouverte.

M. Chapnick : Je vais essayer de vous répondre de manière générale, puis Stephanie pourra vous répondre de façon plus détaillée.

Tout commence par le Plan d'action canado-américain sur les infrastructures essentielles, qui a été signé en 2010. Il faudra redonner un souffle nouveau à ce plan avec la nouvelle administration américaine, mais c'est le bon outil. Il n'est pas mauvais d'encourager le gouvernement à mettre l'accent sur cette organisation.

Mme Carvin : Je suis d'accord.

Il y a aussi autre chose, et j'en parle dans mes cours. Quand on parle des relations entre les États-Unis et le Canada, l'une des difficultés, c'est que nous n'avons jamais vraiment réussi à définir « infrastructure essentielle ». Il y a des secteurs que nous avons définis au Canada et aux États-Unis, mais il reste à définir ce qui est vraiment essentiel dans ce secteur. Par exemple, j'ai lu des rapports des États-Unis selon lesquels les lieux touristiques seraient des infrastructures essentielles, puisqu'ils sont importants pour la culture et l'économie.

C'est donc l'une des difficultés, il faut nous entendre sur le caractère essentiel de ces infrastructures.

That doesn't stop us, however, from looking at the very basic things, such as the electrical grid, for which already there's great interprovincial and state cooperation — also things like railways. Any cooperation like that can facilitate trade. Keeping an open border should definitely be supported.

Senator Beyak: Those are excellent observations, though, because we haven't really described it, have we?

Ms. Carvin: No, we haven't. It's one of the things I actually like to open my class with when I teach. What is critical infrastructure? Everyone has a general idea of what infrastructure is, but what is critical infrastructure?

One example I like to give is what about a hospital parking lot? Normally you wouldn't associate a parking lot as critical infrastructure, but in an emergency the doctors need to get to the hospital and park their cars, and we need to get people in and out. You have to widen it, but you don't want to widen it too much so that suddenly all parking lots are critical infrastructure, so it is a challenge. It has to take into consideration the local context.

The Chair: If I could just maybe have a few comments in respect to this, and maybe we can hear from Mr. Chapnick on this and Ms. Carvin. You talk about our relationship with the United States of America, and I don't think anyone would argue that we need to have good relationships with Americans, and they need to have good relationships with us. We have NORAD and an electrical system that provides a great deal of electricity for the Eastern Seaboard and on the West Coast. Our countries are intertwined.

At the same time I would like to go further, Mr. Chapnick, on what you had to say in respect to us having our own debate in Canada about our vulnerabilities. Are we taking the necessary steps to meet our responsibilities in the area of public security? If we're not, why not? That's part of a democracy, part of a public debate. That's why we have these meetings, and that's why you're here.

I would like to comment on this. The fact is that over the last 10 years we have gone into I think well over 40 free trade agreements with other countries, which gives us diversification and the ability to take our product and sell it to the highest bidder, depending on what it is.

Wouldn't that be part of our conversation with our friends south of the border, that we are becoming a much more diversified country, much more independent, yet at the same time we are your partner and we're prepared to work with you as long as you're prepared to work with us?

Cela ne nous empêche pas, cependant, de nous pencher sur des éléments de base, comme le réseau électrique, pour lequel il y a déjà de la coopération interprovinciale et internationale. Il y a aussi les chemins de fer. Toute coopération du genre peut faciliter le commerce. Quoi qu'il en soit, il faut absolument maintenir l'ouverture de la frontière.

La sénatrice Beyak : Ce sont là d'excellentes observations, parce que nous n'avons jamais vraiment précisé ce que nous entendons par là, n'est-ce pas?

Mme Carvin : Non. C'est d'ailleurs l'une des choses que j'aime mentionner d'entrée de jeu quand je donne un cours. Qu'entend-on par « infrastructure essentielle »? Tout le monde a une idée générale de ce qu'est l'infrastructure, mais qu'est-ce que l'infrastructure essentielle?

J'aime donner l'exemple du stationnement d'un hôpital. On ne considère habituellement pas un stationnement comme de l'infrastructure essentielle, mais en situation d'urgence, les médecins doivent pouvoir se rendre à l'hôpital et y stationner leur voiture; les gens doivent pouvoir y circuler. Il faut donc élargir la définition, mais on ne veut pas trop l'élargir non plus, puis que soudainement, tous les stationnements soient considérés comme des infrastructures essentielles. C'est compliqué. Il faut tenir compte du contexte local.

Le président : J'aimerais avoir votre opinion sur un sujet, peut-être M. Chapnick et ensuite Mme Carvin. Vous avez parlé de notre relation avec les États-Unis. Je crois que personne ne discuterait le fait que nos deux pays doivent entretenir de bonnes relations. Nous participons au NORAD et notre réseau électrique fournit de l'électricité à beaucoup d'habitants des côtes Est et Ouest. Nos deux pays sont inextricablement liés.

Mais, j'aimerais pousser plus loin. Monsieur Chapnick, vous dites que le Canada doit avoir son propre débat sur ses vulnérabilités. Prenons-nous les mesures nécessaires pour assumer nos responsabilités en matière de sécurité publique? Sinon, pourquoi? C'est une question démocratique; elle doit être soumise à un débat public. C'est la raison pour laquelle nous organisons ce genre de réunion et pour laquelle nous vous avons invité.

J'aimerais vous entendre à ce sujet. Au cours des 10 dernières années, nous avons conclu, si je ne m'abuse, plus de 40 accords de libre-échange avec d'autres pays, ce qui nous offre plus de diversité et nous permet de vendre nos produits aux plus offrants, selon le produit.

Ne devrait-on pas discuter avec nos voisins du Sud à ce sujet, leur dire que nous sommes de plus en plus diversifiés et indépendants, mais que nous nous sommes un de leur partenaire et souhaitons collaborer avec eux, s'ils sont prêts à collaborer avec nous?

Mr. Chapnick: I think, senator, that some codependency is taking place: 35 American states look to Canada as their number one trading partner, and another 12 look to Canada as either their number two or three.

I think the challenge is that American trade with Canada represents about 12 per cent to 14 per cent of their GDP, and our trade with the United States is somewhere around 30 per cent of our GDP. So if the border were to close tomorrow, it would hurt us a lot faster than it would hurt them.

When it comes to the trading agreements, I agree that government has done a good job opening doors, but it remains the private sector's job to walk through them, and still today 75 per cent of our exports go to the United States. In spite of the fact that there are about 40 more countries we have agreements with — assuming CETA goes through — they're not being taken advantage of to the point that the percentage of Canadian exports is changing dramatically. We were as high as 87 at one point, but 75 per cent is pretty big.

The Chair: I wanted to raise that because that is another issue in this part of the discussion.

Senator Jaffer: Thank you for your presentations. I have questions for both of you. I'll start with you, Mr. Chapnick.

When I was listening to you, I was hearing the word "fear," fear in the community. Correct me if I'm wrong, but I was hearing that we have to be careful that we don't raise the fear, especially talking about Canadians. There has to be education.

I'm very interested, because I'm sure you've thought about this. What do you mean by "education," and how would that education be implemented?

Mr. Chapnick: That's a very good question. Thank you, senator.

I think we have to help Canadians understand what they can do to make themselves less vulnerable, for example, at the cyber level. Why is your password so important? Why is sharing your password such a bad idea? If we start at the grassroots with some basic security 101 issues that you can teach your children — in addition to crossing the street you also don't do this and you do that — I think we can change the conversation and the culture about what security means. From there we can move to how Canada is responding to the challenges instead of challenges you should be afraid of.

We end up talking about the same thing, but I would prefer to have the conversation in the context of what Canada is doing, as opposed to why you should be afraid.

Does that answer part of your question?

M. Chapnick : Je crois, sénateur, que nous sommes de plus en plus codépendants : pour 35 états, le Canada est le principal partenaire commercial, et pour 12 autres, le Canada est le deuxième ou troisième partenaire commercial en importance.

Le problème, c'est que les échanges commerciaux entre les deux pays représentent environ 12 à 14 p. 100 du PIB des États-Unis, mais environ 30 p. 100 du PIB du Canada. Donc, nous avons beaucoup plus à perdre de la fermeture de la frontière américaine que les Américains.

Je suis d'accord avec vous que le gouvernement a fait du bon travail pour ouvrir des portes avec les accords commerciaux, mais il revient au secteur privé de franchir le seuil de ces portes. Encore aujourd'hui, 75 p. 100 de nos exportations sont destinées aux États-Unis. Malgré le fait que nous ayons signé environ 40 accords commerciaux — si l'on tient pour acquis que l'AECG sera ratifié —, les entreprises n'en profitent pas, en ce sens que les exportations canadiennes vont encore sensiblement au même endroit. Auparavant, 87 p. 100 de nos exportations étaient destinées aux États-Unis, mais 75 p. 100, c'est encore très élevé.

Le président : Je voulais soulever la question, car c'est un autre élément de cette discussion.

La sénatrice Jaffer : Merci pour vos exposés. J'aurais une question à poser aux deux témoins. Je vais d'abord m'adresser à vous, monsieur Chapnick.

Vous avez parlé de la peur au sein de la communauté. Vous me corrigerez si j'ai tort, mais vous dites que nous devons être prudents afin de ne pas susciter la peur, notamment chez les Canadiens. Il y a un travail d'éducation à faire.

Je suis curieuse. Je suis convaincue que vous y avez déjà réfléchi, mais qu'entendez-vous par « éducation » et comment faudrait-il procéder?

M. Chapnick : C'est une très bonne question. Merci, sénatrice.

Nous devons apprendre aux Canadiens quoi faire pour être moins vulnérables, par exemple, en ce qui concerne le cyberespace. Pourquoi le mot de passe est-il si important? Pourquoi est-ce une si mauvaise idée de partager son mot de passe? En enseignant des principes de base en matière de sécurité, des principes que les gens peuvent transmettre à leurs enfants — outre les mesures de sécurité à respecter pour traverser la rue —, nous réussirons à changer le discours et la culture en matière de sécurité. Ensuite, nous pourrons parler de la réaction du Canada face aux menaces plutôt que des menaces qu'il faudrait craindre.

On parle de la même chose, mais je préfère discuter de ce que fait le Canada que des menaces qu'il faudrait craindre.

Est-ce que cela répond en partie à votre question?

Senator Jaffer: I think that's very useful. When you say what Canada is doing, that would certainly raise the comfort level of Canadians. I wanted you to explain what you meant by "fear," and I think I understand.

I have a question for you, Ms. Carvin. I was very interested when you spoke about radicalization. I felt you spoke with a lot of passion about what it does to the family and what it does to the mosque. That is one side of the equation.

What does it do to the mosque, to the community, when the community feels threatened by the authorities, when CSIS walks into your mosque? I hear all kinds of horror stories. I'm sure you've studied this. There is a double-edged sword. There is one threat from your child, who sadly becomes radicalized, and the other is when authorities walk in. That's another fear and threat, and I would like you to explain that, please.

Ms. Carvin: Absolutely. Thank you for the question. I think the big fear is overreaction, and this is actually one of the things that extremists are often trying to promote —that they're not on your side; they can't protect you. It's awful. That just creates more fear, generally speaking.

I think it would be very important for the government to consider finding ways that communities can talk about these issues without feeling that they're going to end up in a database. What resources can we put forward around perhaps the question about non-legal remedies? We have to find ways for parents to feel comfortable going to someone who can do something.

You often see that perhaps the parent wants to take a child to an authority figure, but that authority figure may not have the resources to do something about it. Trying to connect resources to people in such a way that they don't feel that they're putting their entire family in some kind of database is important.

I'm not sure what stories you've heard. I don't think that national security authorities even have the ability to just walk into a mosque or anything like that, but the disruption — they can walk into a workplace. I believe those things are taken very much into the way they work. That's just based on my understanding of the process.

This is what I was saying about also having a more empathetic understanding of the effect on the community. I think we need better research on what happens in these processes. When you have extremists, is the result a galvanizing effect? Is that because we've actually put resources in place, or is it actually damaging social capital within these communities? It's a fascinating issue.

Senator Day: Thank you both for being here. It's a very interesting discussion.

La sénatrice Jaffer : C'est très utile. Il serait certainement réconfortant pour les Canadiens de savoir ce que fait le Canada. Je voulais savoir ce que vous vouliez dire par « peur », et je crois que je comprends maintenant.

Madame Carvin, j'aurais une question pour vous. J'ai bien aimé vous entendre parler de radicalisation. Vous avez parlé avec passion des conséquences de la radicalisation sur les familles et les mosquées. C'est une partie de l'équation.

Quel est l'impact sur la mosquée ou la communauté lorsque celle-ci se sent menacée par les autorités ou lorsque le SCRS se présente à la mosquée? J'entends toutes sortes d'histoires d'horreur. Je suis convaincue que vous avez étudié la question. C'est une lame à double tranchant; d'un côté, il y a la menace de l'enfant qui, malheureusement, a été radicalisé, et d'un autre côté, il y a les autorités qui se présentent à la mosquée. C'est une autre sorte de menace, une autre sorte de peur. J'aimerais vous entendre à ce sujet.

Mme Carvin : Certainement. Merci pour cette question. À mon avis, la plus grande peur, c'est la réaction excessive. C'est souvent l'une des choses que les extrémistes tentent de promouvoir — les autorités ne sont pas de votre côté; elles ne peuvent pas vous protéger. C'est horrible. De façon générale, cela ne fait qu'alimenter la peur.

Il serait très important que le gouvernement étudie des façons de permettre aux membres de ces communautés de parler de ces problèmes sans craindre de se voir ajouter à une base de données. Que pourrait-on faire, par exemple, pour leur offrir des recours non judiciaires? Nous devons trouver des moyens pour que les parents se sentent à l'aise de consulter une personne qui peut intervenir.

Souvent, les parents veulent emmener leur enfant pour parler à une figure d'autorité, mais cette personne n'a peut-être pas les ressources nécessaires pour faire quelque chose. Il est important de jumeler les ressources avec les citoyens sans que ceux-ci aient l'impression que les informations sur les membres de leur famille seront versées dans une base de données.

J'ignore quelles histoires vous avez entendues, mais je ne crois pas que les organismes de sécurité nationale aient le pouvoir de se présenter tout bonnement dans une mosquée, mais elles peuvent déranger — elles peuvent se présenter sur les lieux de travail. Je crois que c'est une des techniques qu'elles utilisent, selon ce que j'ai pu comprendre du processus.

Ce que je disais, c'est qu'il faut faire preuve d'empathie et comprendre quel est l'impact sur la communauté. À mon avis, nous avons besoin de plus de recherches sur les conséquences de ces processus. S'il s'agit d'extrémistes, une telle intervention pourrait-elle les stimuler en raison de la présence de nos ressources ou entraînerait-elle la détérioration du capital social avec ces communautés? C'est fascinant comme question.

Le sénateur Day : Merci à vous deux d'avoir accepté notre invitation. C'est une discussion fort intéressante.

Mr. Chapnick, you gave us two suggestions of how to manage the risks. You talk about the inevitability of demanding security challenges for the future. I guess we're all starting to recognize that.

Could you tell us what you had in mind? You talk about partnerships, but what did you have in mind in terms of increased North American resilience?

Mr. Chapnick: That is a very good question, senator.

I remember after 9/11 there was 7/7 in Great Britain. The day after 7/7 the British went back to work, and there was a great degree of national pride in the way the British said, "You can't scare us. You can disrupt us, but you can't scare us." I think we need that type of culture in North America.

If something bad happens, we and the Americans together, instead of hearing that the terrorists came from Canada, should say that we're going to fix this and we're going back to work. I think we need to work to build a relationship that is strong enough to withstand the problems we're going to have. I don't think you can create 100 per cent security. I think there will be breaches, and it is how we deal with them that matters. If we deal with them separately from the United States, I think we're asking for problems because they can cause trouble to our economy very quickly.

Senator Day: So it's how we will bounce back from attacks. I do quite a bit of work with NATO, and that term "resilience" has taken on major prominence. I expect you will see it repeated several times in the meeting in Poland that is coming up this summer, in July.

The other question is for Ms. Carvin, if you could help me — as soon as I find what I was thinking about — regarding the point you made with respect to ransom at a hospital on the Internet. We're familiar with ships being hijacked and then someone asking for ransom, and we're familiar with threats that we're going to blow something up if you don't deposit some money in a mailbox somewhere. We see that kind of thing quite often.

Can you tell us about this situation, I think you said in California? Is this a growing trend? What are we doing about this one? Is it the same? We react to the ships being hijacked quite nicely as an international community. How are we reacting to ransom on the Internet?

Ms. Carvin: Thank you for your question. Yes, it is something of a growing trend. I have some excellent students who did some research on this last term, which is great.

One of the concerns is that it's not just the information systems that these ransomware viruses go to but to the actual medical equipment itself. Increasingly, we can see computer ransomware being targeted at actual medical equipment, and that's a bad situation. This is something that we have to increasingly consider. There's not a lot of attention on it.

Monsieur Chapnick, vous avez proposé deux façons de gérer le risque. Selon vous, il est inévitable que nous ayons à composer avec des défis exigeants en matière de sécurité à l'avenir. Je crois que nous commençons à le comprendre.

Que proposez-vous exactement? Vous parlez de partenariats, mais que proposez-vous exactement par rapport à une résilience accrue en Amérique du Nord?

M. Chapnick : C'est une très bonne question, sénateur.

Je me souviens qu'après le 11 septembre, il y a eu le 7 juillet, en Grande-Bretagne. Le lendemain, les Britanniques sont retournés au travail. C'était une grande fierté nationale de dire aux terroristes : « Vous ne nous effrayez pas. Vous pouvez perturber nos vies, mais vous ne nous effrayez pas. » Je crois que nous devons encourager une telle culture en Amérique du Nord.

Si une attaque devait survenir, plutôt que de dire que les terroristes sont venus du Canada, les Canadiens et les Américains devraient s'engager à régler le problème et à se remettre au travail. Nous devons bâtir une relation suffisamment solide pour résister à de telles situations. Il est impossible, selon moi, d'avoir une sécurité à toute épreuve. Il y aura toujours des atteintes, mais l'important, c'est notre façon d'y réagir. Si nous travaillons seuls, sans l'aide des États-Unis, je crois que nous aurons des problèmes, car ces atteintes peuvent perturber très rapidement notre économie.

Le sénateur Day : Donc, l'important, c'est notre réaction à de telles attaques. Je travaille beaucoup avec l'OTAN et le mot « résilience » revient très souvent. J'ai l'impression qu'on l'entendra beaucoup lors de la réunion qui aura lieu en juillet prochain, en Pologne.

Ma deuxième question s'adresse à Mme Carvin. J'aurais besoin de votre aide — dès que je me rappellerai ce que je voulais dire. Vous avez parlé d'une rançon demandée à un hôpital par l'entremise d'Internet. Nous savons que des navires sont détournés et retenus contre une rançon ou que des individus menacent de faire exploser une bombe si on ne leur verse pas un montant d'argent dans une boîte aux lettres quelconque. Cela se produit souvent.

Pourriez-vous nous donner des détails sur ce qui s'est produit? C'était en Californie, c'est cela? Est-ce une tendance à la hausse? Comment réagissons-nous dans ce genre de situation? Est-ce la même chose? La communauté internationale réagit bien lorsque des navires sont détournés. Comment réagissons-nous à une rançon demandée par l'entremise d'Internet?

Mme Carvin : Merci pour cette question. C'est effectivement une tendance à la hausse. J'ai d'excellents étudiants qui ont fait des recherches sur le sujet au dernier trimestre, ce qui est très bien.

Une des choses inquiétantes, c'est que ces rançongiciels ne s'attaquent pas seulement aux systèmes informatiques, mais aussi à l'équipement médical en tant que tel. De plus en plus, l'équipement médical est visé, et c'est dangereux. Nous devons en tenir compte de plus en plus. On n'accorde pas beaucoup d'importance à cela.

As to what we are doing, to be honest, I can't tell you. It's beyond my knowledge. I believe we need to direct more attention to this, particularly when it comes to hospitals, but there really is no standard as far as I'm aware for the cyberprotection of medical equipment. Even if you could develop it, the rate at which these ransomware viruses develop and the many vulnerabilities to them pose such considerable challenge in trying to deal with them going forward that I do believe this is something we'll increasingly be dealing with in Canada in the next couple of years. I wish I could be more optimistic on this point, but right now I'm just not.

Senator Day: I'm a little concerned. I don't know if you were here for the last witness from Communications Security Establishment Canada, but she made the point that incidents of cyberattack or some cyberactivity that is not welcome are up to 100 million a day. To fit in with that, I can't see how we're going to deal with this very quickly.

Ms. Carvin: I believe that Canada is dealing with a cybersecurity strategy, but it seems to be a little slow in coming. I know that it was part of the last government and part of this government to have cybersecurity initiatives, but it does really get back to the heart of some of the challenges we have with critical infrastructure, with the additional problem that this is moving exponentially faster than some of the other challenges that we're having.

I believe it is something the government should absolutely be prioritizing. It comes down to the challenge when I was in government. What are the paramount threats to national security and how do you rank terrorism over cyber? In this case, I'm not sure it's useful to think of them. They rely on one another to a certain extent, but this is such a considerable problem in such a multifaceted number of ways that I absolutely would advocate much more attention and much more resources being dedicated to the cyber issues that we're facing if only because they're so interconnected to all the other problems I talked about.

The Chair: Could I just perhaps go into a different area, and Ms. Carvin, perhaps you have some knowledge on this. I'm referring to the issue that is now being addressed more in the United States than in Canada, namely, the issue of electromagnetic pulse. In your research and background, have you any comments regarding how you see it in the United States? It's just becoming an issue here in Canada, actually through our committee, for public discussion.

Ms. Carvin: It's a very glamorous issue in some ways because I think the weapon has been featured in so many films and things like that. We've seen a lot of it.

I would put two things forward first. First, you can actually produce effects similar to those of an electronic magnetic pulse without an actual electronic magnetic pulse. There are believed to be conventional weapons that could do it, such as a cobalt bomb. It is believed this may have been used by the Americans in the Balkans and in the Iraq conflicts, and they were able to produce a

Comment réagissons-nous? Sincèrement, je l'ignore. Cela dépasse mes compétences. À mon avis, nous devons prêter plus d'attention à ce dossier, surtout en ce qui a trait aux hôpitaux, mais, à ma connaissance, il n'existe aucune norme pour la cyberprotection de l'équipement médical. Même si nous pouvions développer une telle protection, en raison de la vitesse à laquelle ces rançongiciels sont créés et des nombreuses vulnérabilités qu'ils peuvent exploiter, le défi est énorme. À mon avis, c'est un problème grandissant avec lequel le Canada devra composer au cours des prochaines années. J'aimerais être plus optimiste, mais, pour le moment, je ne peux pas.

Le sénateur Day : Cela m'inquiète. J'ignore si vous étiez présente lors du témoignage de la représentante du Centre de la sécurité des télécommunications Canada, mais elle a souligné qu'il y a jusqu'à 100 millions de cyberattaques ou d'activités indésirables dans le cyberespace chaque jour. Dans ce contexte, j'ignore comment nous pourrions réagir rapidement.

Mme Carvin : Je crois que le Canada travaille à une stratégie de cybersécurité, mais elle tarde à venir. Je sais que le gouvernement précédent était intéressé par des projets de cybersécurité, tout comme le gouvernement actuel. Mais, cela nous ramène au cœur du problème des infrastructures essentielles, sans compter que les problèmes liés à la cybersécurité prennent rapidement de l'ampleur, plus que d'autres problèmes avec lesquels nous devons composer.

Selon moi, le gouvernement devrait absolument faire de ce dossier une priorité. On se posait la même question lorsque je travaillais au gouvernement. Quelles sont les principales menaces à la sécurité nationale et où se classe la cybersécurité par rapport au terrorisme? Dans ce cas-ci, je ne crois pas qu'il soit utile de les voir séparément. Dans une certaine mesure, ils dépendent l'un de l'autre, mais les problèmes liés à la cybersécurité sont si importants et multidimensionnels qu'il faudrait leur accorder, selon moi, beaucoup plus d'attention et de ressources, simplement parce qu'ils sont si étroitement liés à tous les autres problèmes que nous avons soulevés.

Le président : J'aimerais aller dans une autre direction, madame Carvin. Peut-être aurez-vous des informations à nous fournir. J'aimerais parler de l'impulsion électromagnétique. On en parle davantage aux États-Unis qu'au Canada. Dans le cadre de vos recherches, et selon votre expérience, où en sont les États-Unis sur cette question? L'impulsion électromagnétique commence à susciter un débat au Canada, notamment parce que notre comité tient des discussions publiques sur le sujet.

Mme Carvin : C'est un sujet très prestigieux, disons, car une arme semblable a figuré dans de nombreux films, notamment. Nous l'avons souvent vu.

Je dirais deux choses. Premièrement, il est possible de reproduire l'effet d'une impulsion électromagnétique sans avoir recours à l'impulsion électromagnétique elle-même. Selon certains, des armes conventionnelles, comme la bombe au cobalt, permettraient d'obtenir un effet semblable. D'autres avancent que c'est ce que les Américains ont fait dans les

similar effect to an electronic magnetic pulse. It is not just an electronic magnetic pulse that is at issue here; there are other ways of doing it.

Second, to a certain extent I think there is some skepticism within the academic community as to how much of a threat these are. The more important thing is do you want to have a strong electrical grid irrespective of where these threats are. There could be a solar flare, for example. To a certain extent, I think that would be more likely than an EMP. There is no reason not to have strong, protected electrical grids.

With EMPs, the often heard line is the only way you really get one is with a nuclear weapon, and if a nuclear bomb goes off in Canada, we will probably have considerably larger problems than just the electricity not working.

That being said, the other factor here is would a terrorist group use one? In my view, terrorists or violent extremists in Canada tend to be practical in their orientation. They're instrumental and want to get things done. Rather than getting hold of one of these, they would use a pressure cooker gun or a bomb in a mall to produce chaotic effects.

Would a state use one? You have the usual suspects. China needs us to be fully operational for them to be profitable. Would North Korea use it? The extent to which they have a nuclear weapon is not entirely clear yet. I don't yet believe they have the capacity to deliver such an attack, if they did.

I'm not saying they don't exist, and I'm not saying they're there. I just think we need to take a breath. There seems to be an industry of individuals with kind of sketchy former ties to the intelligence sector that are trying to push this forward. To a certain extent, I think these succeed because the idea of an EMP is so terrifying that a lot of people get scared. However, when you sit down and think about who would use it and what would be the strategy behind it, it is a bit more sobering. There is no reason why we shouldn't have a very strong electrical grid that could protect against either solar flares or other electrical problems.

The Chair: That is a very significant financial commitment.

Ms. Carvin: Yes.

The Chair: That is, to upgrade the current system the way it exists today. Are you telling this committee that, even from the point of view of a solar possibility and also the other possibilities that are out there, Canada should be seriously looking at not only the expansion of existing grids but also the current grids, looking at reinforcing them? If they are, it is a huge financial commitment.

Ms. Carvin: The last great threat to our electrical infrastructure was a tree branch in Ohio in 2003 which caused the blackout. Maybe we should also look at trimming the trees. It's hard for me

Balkans et lors des conflits en Irak. Ils ont pu reproduire l'effet d'une impulsion électromagnétique. Le problème n'est pas seulement l'impulsion électromagnétique; le problème, c'est qu'il y a d'autres façons d'obtenir une telle impulsion.

Deuxièmement, je crois qu'il y a un certain scepticisme dans le milieu universitaire quant à la menace que représente l'impulsion électromagnétique. L'important, c'est d'avoir un réseau électrique solide, peu importe les menaces. On pourrait parler d'éruptions solaires, par exemple. D'ailleurs, je crois que les éruptions solaires sont plus probables que les impulsions électromagnétiques. Il n'y a aucune raison pour ne pas disposer d'un réseau électrique solide et protégé.

On entend souvent dire que la seule façon d'obtenir une impulsion électromagnétique, c'est de faire exploser une bombe nucléaire. Si une bombe nucléaire explose au Canada, une panne d'électricité sera le moindre de nos soucis.

Cela dit, l'autre question qu'il faut se poser c'est, est-ce qu'un groupe terroriste utiliserait une arme nucléaire? À mon avis, les extrémistes violents au Canada ont tendance à être plus pratiques. Ils veulent jouer un rôle actif, participer à l'attaque. Plutôt que d'utiliser une arme nucléaire, ils fabriqueraient une bombe à l'aide d'un autocuiseur ou utiliseraient une arme à feu dans un centre commercial pour semer le chaos.

Est-ce qu'un pays utiliserait une arme nucléaire? Les mêmes suspects reviennent. Sur le plan économique, la Chine a besoin d'un Canada entièrement fonctionnel. Est-ce que la Corée du Nord utiliserait une arme nucléaire? Nous ignorons encore si le pays possède cette capacité. Si oui, je doute qu'il soit en mesure de mener une telle attaque.

Je ne dis pas que les armes à impulsion électromagnétique n'existent pas ni qu'elles existent. Je dis seulement qu'il faut prendre un peu de recul. On dirait qu'un groupe d'individus douteux ayant déjà eu des liens avec le secteur du renseignement tente de promouvoir le concept de l'impulsion électromagnétique. Je crois qu'ils connaissent un certain succès, car l'idée d'une telle arme est si terrifiante, qu'elle effraie beaucoup de gens. Toutefois, lorsqu'on réfléchit à qui pourrait disposer d'une telle arme et à quelle fin, on revient sur terre. Il n'y a aucune raison pour que nous n'ayons pas un réseau électrique très solide protégé contre des éruptions solaires ou tout autre problème de nature électrique.

Le président : Cela nécessiterait un engagement financier considérable.

Mme Carvin : En effet.

Le président : Je parle de la mise à niveau du système actuel. Dites-vous au comité que même en tenant uniquement compte de la possibilité d'une éruption solaire ou d'autres facteurs possibles, le Canada devrait non seulement songer sérieusement à élargir les réseaux actuels, mais aussi à les renforcer? Si c'est le cas, il s'agit d'un énorme engagement financier.

Mme Carvin : La dernière grande menace pour notre infrastructure électrique remonte à 2003, lorsqu'une panne d'électricité généralisée a été causée par la chute d'une branche

to say. I think it is a little much to go that far. It's the high-impact, low-probability event that all analysts kind of think about going forward. I do believe that the risk of such an event is fairly low. Is that the actual standard to which we want to develop our critical infrastructure? I think we have to balance the probability with things that might be better spent on, again, tree-cutting issues, general maintenance and things like that. I can't say that it would be my first recommendation to this committee.

Senator Mitchell: Mr. Chapnick, again, back to the Canada-U.S. border and the thinning of it, it seems to me that it would follow from your observations that the agreement that was captured by Mr. Trudeau and Mr. Obama with respect to the exchange of information isn't an undue threat to privacy or a concern in that regard.

Mr. Chapnick: I think that Canadians will have to accept that we are going to have to trade a little bit of privacy for the combination of security and access.

Senator Mitchell: Dr. Carvin, I think this committee is very interested in looking at a specific study on cybersecurity. An earlier witness mentioned the fact that it's really focused in Public Safety, and it's in the minister's mandate letter, in fact. If you were the Minister of Public Safety for a day or two, what would you suggest needs to be done for Public Safety to coordinate effectively, particularly for the private sector?

You can see where the federal and provincial governments are at least definable in a way that the private sector isn't. What does it take to do that?

Ms. Carvin: Thank you for the question. I believe, to a certain extent, one of the most important things we could do is information sharing, not just between federal agencies, but also between the private and the government sectors.

As it stands, private companies have virtually no incentive to go public with their giant data breaches; we've seen the horror stories that result, whether it's Target or Sony, from their data breaches.

Again, to a certain extent, it's creating strong relationships with the private sector so that they feel comfortable coming forward with their needs or saying, "We've come into an attack here," just so we have a better understanding of the scale of the problem. I can't speak to what the CSE representative, perhaps, said, but it's my understanding the government has a fairly good idea of the number of attacks against the government, but we

d'arbre, en Ohio. Nous devrions peut-être aussi songer à l'élagage des arbres. C'est difficile à dire. Je pense qu'il est exagéré d'aller aussi loin. Tous les analystes se penchent désormais sur les événements lourds de conséquences, mais peu probables. Je suis convaincue que le risque qu'un tel événement se produise est assez faible. Est-ce la norme que nous voulons appliquer pour le développement de nos infrastructures essentielles? À mon avis, nous devons établir un équilibre entre la probabilité d'un événement et les choses pour lesquelles l'argent serait utilisé à meilleur escient comme l'abattage des arbres, l'entretien général, et cetera. Je ne peux dire si ce serait là ma première recommandation pour le comité.

Le sénateur Mitchell : Monsieur Chapnick, pour revenir encore une fois à la frontière canado-américaine et à la simplification des processus à la frontière, il me semble que vos observations laissent entendre que l'accord sur l'échange de renseignements conclu entre MM. Trudeau et Obama ne représente pas une menace indue pour la protection des renseignements personnels ou une préoccupation à cet égard.

M. Chapnick : Je pense que les Canadiens devront accepter que le Canada fasse des concessions sur le plan de la protection des renseignements personnels pour obtenir à la fois la sécurité et l'accès.

Le sénateur Mitchell : Madame Carvin, je pense que le comité souhaite ardemment une étude sur la cybersécurité. Un témoin précédent a mentionné que le ministère de la Sécurité publique y porte une attention particulière et, en fait, la question est évoquée dans la lettre de mandat du ministre. À votre avis, si vous étiez ministre de la Sécurité publique pendant une journée ou deux, que devrait faire le ministère pour assurer une collaboration efficace, en particulier avec le secteur privé?

Vous êtes à même de constater quels aspects peuvent, à tout le moins, être définis pour le gouvernement fédéral et les gouvernements provinciaux, ce qui n'est pas le cas pour le secteur privé. Que faut-il faire pour y parvenir?

Mme Carvin : Je vous remercie de la question. Dans une certaine mesure, je crois que l'une des choses les plus importantes que nous pourrions faire serait de partager des renseignements, non seulement entre les organismes fédéraux, mais aussi entre les secteurs privé et public.

Actuellement, pratiquement aucune mesure n'incite les entreprises privées à divulguer les fuites importantes de données dont elles ont fait l'objet. Nous avons vu les histoires d'horreur qui découlent de telles fuites, comme dans le cas de Target ou de Sony.

Encore une fois, il s'agit dans une certaine mesure d'établir des relations solides avec le secteur privé pour que les acteurs de ce milieu soient à l'aise de présenter leurs demandes ou de divulguer qu'ils ont fait l'objet d'une attaque afin que nous ayons une meilleure idée de l'ampleur du problème. Je ne peux me prononcer sur les propos de la représentante du CST, mais je crois comprendre que le gouvernement a une assez bonne idée du

don't actually necessarily have the mandate to understand the number of attacks against the private sector or against Canada as a whole.

I think one of the most important things the government could do is to promote better information sharing, in some kind of confidential way, so that companies would feel better coming forward with their breaches. We would have, perhaps, a better understanding of where they're coming from, but also what the private sector is doing in reacting to it, if they're doing anything at all, which might be another problem as well.

Senator Jaffer: I have a quick question for you, Ms. Carvin. I believe that the community would cooperate much more if it didn't think it was going to be part of a database, or if their child would be marked. I believe the mother knows when the child has more money or weapons, or is doing something out of the ordinary. But a mother is not going to go to the authorities because of what could happen to that child.

I wonder if either of you have ideas about how we can create that place of trust that families can go to without their child being marked.

Ms. Carvin: Thank you for that question. This issue is one that fascinates me very much.

What I would suggest first, however, is that one of the problems that communities have is that they do actually have challenges in identifying those indicators that their child may be moving toward violence. Perhaps they had a partying lifestyle beforehand, and suddenly they're religious, and they say, "This is a great thing. This is not a bad thing at all." Perhaps they're not that familiar with some of the websites they're going to, or not monitoring them. Increasingly, we're seeing that radicalization takes place online, on smartphones, and through targeted recruitment over peer-to-peer messaging. I think it's hard for parents to know.

I'm a little bit concerned that we haven't yet properly defined the role of law enforcement agencies in the CVE, or countering violent extremism, efforts. One of the things those law enforcement agencies can do is work with the communities to provide those indicators to help create trust. But then, as you say, the second problem emerges, which is how you then establish those relationships where they can come forward to a trusted partner.

We're seeing innovative stuff happening in Montreal and, to a certain extent, in Calgary, in terms of trust and commitments. Public Safety Canada had round tables where they went to the communities and shared stories and narratives, and I think it's wonderful that they did that.

nombre d'attaques dont il fait l'objet. Toutefois, en réalité, nous n'avons pas nécessairement le mandat de chercher à déterminer le nombre d'attaques contre le secteur privé ou contre le Canada en général.

À mon avis, l'une des choses les plus importantes que le gouvernement pourrait faire serait de favoriser un meilleur échange d'informations, de façon confidentielle, pour que les entreprises soient plus à l'aise de divulguer les incidents. Cela nous permettrait peut-être d'avoir une meilleure compréhension de leur origine et de la façon dont on y réagit dans le secteur privé, si réaction il y a, ce qui pourrait aussi être un problème.

La sénatrice Jaffer : J'ai une brève question pour vous, madame Carvin. Je crois que la population collaborerait davantage si les gens n'avaient pas le sentiment que ce serait intégré à une base de données ou qu'un enfant serait fiché. Je suis convaincue qu'une mère le sait lorsque son enfant a plus d'argent, des armes ou un comportement inhabituel. Toutefois, une mère ne se tournera pas vers les autorités en raison des conséquences possibles pour cet enfant.

Je me demande si l'un ou l'autre d'entre vous a des idées sur la façon dont nous pourrions créer un lieu de confiance vers lequel les familles pourraient se tourner sans qu'un enfant se retrouve fiché.

Mme Carvin : Je remercie la question. C'est un enjeu qui me fascine beaucoup.

Premièrement, je dirais qu'à l'échelle communautaire, un des problèmes est que les gens ont de la difficulté à cerner les indicateurs qui démontrent qu'un jeune a une tendance vers la violence. Il est possible qu'ils voient d'un bon œil qu'un jeune qui avait peut-être auparavant tendance à faire la fête se tourne soudainement vers la religion. Il est également possible qu'ils ne connaissent pas certains sites web que les jeunes consultent, ou qu'ils n'exercent aucune surveillance. On constate de plus en plus que la radicalisation tend à se faire en ligne, à l'aide de téléphones intelligents et par un recrutement ciblé au moyen de messages entre pairs. À mon avis, il est difficile pour les parents de savoir ce qui se passe.

Je suis quelque peu préoccupée qu'on n'ait pas encore défini adéquatement le rôle des organismes d'application de la loi dans la lutte contre l'extrémisme violent, ou LEV. Les organismes d'application de la loi peuvent notamment collaborer avec les communautés afin de définir ces indicateurs et ainsi favoriser la confiance. Mais c'est alors, comme vous l'avez indiqué, que le deuxième problème se pose : il s'agit de savoir comment établir des relations qui inciteront les gens à se manifester auprès d'un partenaire de confiance.

Il y a eu à Montréal — et à Calgary, dans une certaine mesure — des activités novatrices visant à favoriser la confiance et la mobilisation. Le ministère de la Sécurité publique a organisé des tables rondes au cours desquelles les participants ont fait le récit de leur expérience. Je pense que c'était une idée formidable.

Those kinds of initiatives — perhaps not at the pointy end of the stick, but much further down the stick, as it were, to go forward and explain what the roles are — are absolutely vital, but I also believe that much of this has to be community-driven, and this perhaps is where the offers of the coordinator for radicalization or CVE will come in handy because they can look at the different efforts and say, "Have you tried this? This program is working here." There is a lot of potential.

Senator Beyak: Thank you, Mr. Chapnick and Professor Carvin. You're both impressively knowledgeable on this issue.

I wonder if you could give me your opinion on a three-part question. We had Professor Rudner here back in 2010, and he said at the time that Canada's approach to critical infrastructure was passive and reactive.

I wonder three things: whether you have feel we have come forward since that time; if you agree with his assessment; and if either of you have found, in your research, a model that is working elsewhere — a nation that has got it right — that we could learn from instead of reinventing the wheel. Thank you.

Ms. Carvin: Thank you for that challenging question. Fortunately, the program I teach on was partially founded by Martin Rudner. He is a very interesting individual who is passionate about these issues.

I would suggest that because of some of unfortunate events we have experienced, like the October 2014 attacks and the increasing awareness of cyber issues, I no longer believe that we are passive. I believe there is general awareness of these issues and what these threats are, and that has something to do with it. If that's coming forward, I think that is one important step that we are definitely taking.

In terms of a model that is working, what I can tell you is that we, in our program, are regularly approached — this isn't an advertisement, I swear — by countries from the Middle East in particular, who see us as a model, and they don't know how to make policy in this area. We sometimes are able to provide them with advice, or they send individuals on our courses, to learn what the Canadian system is and how it's doing, and sometimes that's as simple as how you create a policy between different levels of government. We can have those conversations.

I don't want to say we're the best model, but perhaps we shouldn't always be afraid that we're the worst, either, because other countries are actually looking to us.

Mr. Chapnick: Very briefly, Martin Rudner taught me, so that connection is all over the place.

Les initiatives de ce genre sont absolument essentielles pour aller de l'avant et définir les rôles — peut-être pas en détail, mais en général, pour ainsi dire —, mais je crois aussi qu'une bonne partie de ces activités doit être axée sur les communautés, et c'est peut-être là l'aspect pour lequel les propositions du coordonnateur de la lutte contre la radicalisation ou contre l'extrémisme violent seront utiles. Il pourra en effet examiner les diverses activités et chercher à savoir si on a essayé certains programmes qui fonctionnent ailleurs. Il y a un potentiel énorme.

La sénatrice Beyak : Monsieur Chapnick, madame Carvin, je vous remercie. Vous avez tous les deux des connaissances remarquables sur cet enjeu.

J'ai une question à trois volets pour laquelle j'aimerais avoir vos commentaires. Lorsqu'il est venu témoigner au comité en 2010, le professeur Rudner a indiqué que l'approche du Canada à l'égard des infrastructures essentielles était passive et réactive.

Je m'interroge sur trois aspects. Avons-nous progressé depuis, à votre avis? Souscrivez-vous à cette évaluation? L'un ou l'autre d'entre vous a-t-il trouvé, dans le cadre de ses recherches, un modèle qui fonctionne ailleurs — je parle d'un pays qui aurait trouvé une bonne solution —, un modèle duquel nous pourrions nous inspirer plutôt que de chercher à réinventer la roue? Merci.

Mme Carvin : Je vous remercie de la question; c'est une question difficile. Il se trouve, heureusement, que le programme que j'enseigne a partiellement été mis sur pied par M. Martin Rudner. C'est un homme fort intéressant qui est passionné par ces questions.

Je dirais que nous n'avons plus une approche passive, d'abord en raison de certains événements malheureux que nous avons vécus, comme les attaques survenues en octobre 2014, puis parce que nous avons une sensibilisation accrue aux enjeux liés au cyberespace. Je crois qu'il y a maintenant une connaissance générale des enjeux et des menaces, et que ces événements ont joué un rôle à cet égard. Si c'est ce qu'on entend par progrès, je crois que nous avons certainement fait un pas important en avant.

Pour ce qui est d'un modèle qui fonctionne, je peux vous dire que nous sommes régulièrement sollicités, dans notre programme — je jure que ce n'est pas de la publicité —, en particulier par des pays du Moyen-Orient qui nous considèrent comme un modèle; ils ne savent pas comment élaborer des politiques à cet égard. Parfois, nous leur donnons des conseils, parfois ils envoient des gens suivre nos cours pour apprendre à connaître le système canadien et son fonctionnement. Dans certains cas, il s'agit de choses aussi simples que l'élaboration d'une politique entre divers ordres de gouvernement. Nous pouvons aborder ces questions.

Je ne veux pas laisser entendre que notre modèle est le meilleur, mais cela ne veut pas dire pour autant que nous devrions toujours craindre qu'il soit le pire, parce qu'en réalité, d'autres pays nous prennent comme exemple.

M. Chapnick : Très brièvement, M. Martin Rudner m'a enseigné; la relation est donc évidente.

I agree that we might have been passive pre-2010, but I think that we are more active now; I believe this committee is evidence that we are more active now than we were. I think reactive is somewhat inevitable in a liberal democracy that hasn't experienced the type of catastrophic events that galvanize the combination of the public and the political level to act aggressively. I think it's unfortunate and lucky at the same time.

The place that we looked to in my class quite often when we talked about cyber resilience is Estonia, which happens to have been the victim of a brutal cyberattack. They seem to have their act quite well together when it comes to cyber, but I wouldn't want to have the incentive that Estonia had to get it right.

The Chair: Colleagues, it is 4:30. I want to thank Mr. Chapnick and Ms. Carvin for coming to the committee. We very much appreciate what you had to say.

As we continue our look at threats to Canada's critical infrastructure, we're pleased to welcome Kevin Quigley, Associate Professor and Director, MacEachen Institute for Public Policy and Governance at Dalhousie University. Mr. Quigley currently teaches strategic management in the public sector. His research interests include public sector risk, crisis management and critical infrastructure protection. He has been an investigator on several critical infrastructure protection projects, including supply chain risk analysis and management in New Brunswick; strengthening the resilience of the Canadian water sector; adapting to vulnerabilities in the transportation systems' critical infrastructure; and terrorism, security and society, among others. He holds a PhD from Queen's University Belfast.

Next to Mr. Quigley is Andrew Graham, Adjunct Professor of Public Administration, Queen's University. He is the National Editor of the Case Study Program at the Institute of Public Administration of Canada. Professor Graham has over 30 years of public service experience, including 14 years as an assistant deputy minister with different departments, such as Agriculture and Agri-Food Canada; Senior Deputy Commissioner of Correctional Service Canada; and Warden of the Kingston Penitentiary. He has written a textbook entitled *Canadian Public Sector Financial Management*. In 2011 he edited a publication entitled *Canada's Critical Infrastructure: When is Safe Enough Safe Enough?* for the Macdonald-Laurier Institute's National Security Strategy for Canada series.

Welcome. I understand you each have an opening statement. We will begin with Dr. Graham.

Andrew Graham, Adjunct Professor, School of Policy Studies, Queen's University, as an individual: Good afternoon. I appreciate this invitation to participate in this important discussion. Over the years of my career as a public servant and subsequently, I always

Je conviens que nous étions peut-être passifs avant 2010, mais je pense que nous sommes maintenant plus actifs. À mon avis, ce comité est la preuve que nous sommes plus actifs que nous l'étions. Je pense qu'il est inévitable d'être réactif lorsqu'on vit dans une démocratie libérale qui n'a pas fait l'expérience d'événements catastrophiques qui galvanisent à la fois le public et la classe politique et qui les incitent à agir de façon agressive. Selon moi, c'est un mal pour un bien.

Dans ma classe, lorsque nous discutions de cyberrésilience, nous citions souvent en exemple de l'Estonie, qui a été victime d'une cyberattaque massive. Les Estoniens semblent avoir une synergie plutôt bonne pour les questions liées au cyberespace, mais je dirais qu'il ne faut pas attendre d'être confronté à ce que l'Estonie a connu pour trouver une solution.

Le président : Chers collègues, il est 16 h 30. Je tiens à remercier M. Chapnick et Mme Carvin d'être venus au comité. Nous vous sommes très reconnaissants de vos commentaires.

Nous poursuivons notre étude sur les menaces aux infrastructures essentielles canadiennes. Nous avons le plaisir d'accueillir M. Kevin Quigley, qui est professeur agrégé et directeur du MacEachen Institute for Public Policy and Governance, à l'Université Dalhousie. M. Quigley enseigne actuellement la gestion stratégique dans le secteur public. Ses recherches portent notamment sur le risque dans le secteur public, la gestion des crises et la protection des infrastructures essentielles. Il a été enquêteur pour plusieurs projets de protection des infrastructures essentielles : Analyse et gestion du risque dans la chaîne d'approvisionnement au Nouveau-Brunswick; Renforcer la résilience du secteur des eaux au Canada; S'adapter aux vulnérabilités des infrastructures essentielles du système de transports; Le terrorisme, la sécurité et la société, entre autres. Il est titulaire d'un doctorat de la Queen's University de Belfast.

À ses côtés, nous avons M. Andrew Graham, qui est professeur auxiliaire d'administration publique à l'Université Queen's. Il est rédacteur en chef du programme d'études de cas de l'Institut d'administration publique du Canada. M. Graham compte plus de 30 ans d'expérience de la fonction publique, notamment 14 comme sous-ministre adjoint dans divers ministères comme Agriculture et Agroalimentaire Canada; il a été sous-commissaire principal au Service correctionnel du Canada et directeur du pénitencier de Kingston. Il a écrit un manuel intitulé *Canadian Public Sector Financial Management*. En 2011, il a dirigé la rédaction d'une publication intitulée *Canada's Critical Infrastructure : When is Safe Enough Safe Enough?* dans le cadre de la série sur la stratégie nationale en matière de sécurité du Macdonald-Laurier Institute.

Bienvenue à tous. Je crois savoir que vous avez tous une déclaration préliminaire. Nous commençons avec M. Graham.

Andrew Graham, professeur auxiliaire, École des études sur les politiques publiques, Université Queen's, à titre personnel : Bonjour. Je vous remercie de l'invitation à participer à cette importante discussion. Tant au cours de ma carrière de

looked forward to discussions in the other place because they tended to have much longer-term perspective than what would be the headline tomorrow. It's always a pleasure as a public servant to appear as a witness.

I understand that the base of my invitation is the publication that I did several years ago, which you just referenced and which is available in PDF form on my website. We will get it for you. This was published as part of two reports, the second part of which I would also bring to your attention, by the Macdonald-Laurier Institute. The second was a series of short pieces on solutions to some of the problems that I've identified, which may in fact be of some use to you.

I conducted this research through a thorough review of published material, including, obviously, Professor Quigley's material, which is seminal and very important to thinking in Canada today; a series of interviews with some government officials; a number of industry representatives from some sectors, most notably the electrical sector; and discussions with certain police services across the country. One of the other areas of research and activity I'm involved in is police oversight and governance. I continue to work after my many years in criminal justice with police services across the country. My observations will go to those towards the end.

While I came to this research with relatively fresh eyes in terms of both the security of infrastructure issue and its relationship to terrorist threats, I base my work on my extensive experience, which has already been referenced, and on my continuing interaction with police. I propose to briefly summarize my research findings on the first report and conclude with some brief commentary on issues senators may wish to consider in terms of the direction for policy and practice in this area following from this committee's previous work, which I think has been very important in moving the goal posts.

Perhaps the rub of my findings was that we have a massive decentralized complex of critical infrastructure, which you've heard many times, for which there are many residual forms of risk but for which we have scant evidence that there are specific risks associated specifically with terrorism that we can respond to. In other words, we could foresee all kinds of problems, but what's the evidence that we are having all kinds of problems? That has to be the first question asked.

I do not mean to say this is simply a "Don't worry, do nothing, be happy" sort of conclusion. Rather, it was an effort to take what I see as a realistic review of risk, studying that and teaching it, as I have, to what should be done. I think it's very easy in this area to foresee all kinds of unforeseen risks. I think it's very easy in this area to create more fear and anxiety than resolve to mitigate real risk. There are so many triggers in this field, some of

fonctionnaire et que pendant les années subséquentes, j'ai toujours eu hâte de participer à des discussions à l'autre endroit, car elles étaient habituellement menées dans une perspective à bien plus long terme plutôt que d'être axées sur ce qui ferait la manchette le lendemain. En tant que fonctionnaire, c'est toujours un plaisir de comparaître à titre de témoin.

Je crois comprendre que j'ai été invité en raison de mon rôle dans la rédaction de la publication que vous venez de mentionner. Elle est disponible en format PDF sur mon site web. Nous vous la ferons parvenir. Elle a été publiée dans le cadre d'une série de deux rapports du Macdonald-Laurier Institute. J'aimerais aussi attirer votre attention sur la deuxième partie, qui est une série de courts documents dans lesquels on présente des solutions aux problèmes que j'ai cernés, ce qui pourrait aussi vous être utile.

J'ai mené cette étude en faisant un examen exhaustif de documents publiés, ce qui inclut, évidemment, les travaux précurseurs de M. Quigley, qui sont très importants pour les idées dans le Canada d'aujourd'hui; en réalisant une série d'entrevues avec des fonctionnaires et un certain nombre de représentants de certains secteurs, particulièrement celui de l'électricité; et en discutant avec des services de police partout au pays. L'un de mes autres domaines de recherche et d'activités, c'est la surveillance policière et la gouvernance. Après avoir passé de nombreuses années dans le secteur de la justice pénale, je continue à travailler avec des services de police partout au pays. Certaines de mes dernières observations porteront là-dessus.

Bien que j'aie fait cette recherche en portant un regard relativement nouveau sur la question de la sécurité de l'infrastructure et ses liens avec les menaces terroristes, mes travaux sont fondés sur une vaste expérience, dont on a déjà parlé, ainsi que sur mes contacts constants avec la police. Je propose de résumer rapidement les résultats de mes travaux de recherches sur le premier rapport et de terminer mon exposé par de brèves observations sur des questions d'orientation des politiques et des pratiques dans ce domaine que les sénateurs voudront peut-être envisager et qui découlent des travaux antérieurs du comité qui, je crois, contribuent énormément à changer les choses.

Le hic, c'est que je constate que nous avons un grand ensemble décentralisé d'infrastructures essentielles — on vous l'a dit à maintes reprises — qui comportent de nombreuses formes résiduelles de risques, mais que nous avons peu de preuves de risques précis liés au terrorisme que nous pouvons atténuer. Autrement dit, nous pourrions prévoir toutes sortes de problèmes, mais qu'est-ce qui prouve que nous avons toutes sortes de problèmes? C'est la première question qu'il faut se poser.

Je ne veux pas dire qu'il ne faut pas s'inquiéter, que tout va bien et qu'on ne doit rien faire. J'ai plutôt voulu essayer d'effectuer ce que je considère comme un examen réaliste des risques — ce qui correspond à mes travaux et à mon travail d'enseignant —, pour déterminer les mesures à prendre. Je crois qu'il est très facile de prévoir toutes sortes de risques imprévus dans ce secteur. Il est très facile de semer plus de crainte et

which have already been discussed in the short time I was here this afternoon, that can create an elevated sense of risk without evidence to back it up.

Coming to a ready conclusion that we are doing enough, even if we knew what enough actually looks like, is fraught, I think, with real danger. I can readily see that this whole issue fits into what we have come to call a wicked problem or complex issue. This complexity, in itself, can create confusion and fear with the public and is readily open to manipulation, most notably by the media.

After taking a closer look at the various forms of critical infrastructure that we have in this country, I realize we don't have a system of critical infrastructure in this country. We have a complex of infrastructures. That complexity, in and of itself, lends itself to both confusion and the potential for people feeling that we are more at risk than we are. Further, within that complex, there are certain well-defined systems, such as the electrical distribution system and oil pipelines, that function very well as systems. They function very well on their own, but mostly on their own, having developed over the years to respond to specific challenges in their own specific areas.

So I can talk to the head of security for Ontario Hydro, which I did as part of this research, and they have a very specific sense of the threats that they are facing. I really believe you have to talk to the front line in any of these organizations and not simply to the people at the head office, and they have a very specific, concrete set that don't necessarily fit into a terrorist Armageddon-type of worldview. I'm going to describe later what I think it's founded on, which is a knowledge of the local community in which they're operating and a knowledge of how the systems actually work.

Where we do face some threats is in how the systems either interact or have mutual dependencies, which is what's further growing. Critical infrastructure in Canada is complex, and it's getting more so. It's geographically dispersed and owned by many different players with different agendas and concern for those threats, real or perceived. By its very nature, much of it is vulnerable. The question that arises is if so much of it is vulnerable, why haven't a whole bunch of bad things happened? While we can cite some bad things that have happened, we are not seeing a consistent pattern that would suggest it, even though there are some of those vulnerabilities, like an electrical line crossing northern Quebec in a very isolated way, physically inspected maybe once every six weeks or two months, monitored with electronic monitoring systems that could be overridden by a cyberattack. Why haven't things gone wrong? Because there's a lot of good work being done at the front end of organizations.

d'anxiété plutôt que de décider d'atténuer les risques réels. Dans ce secteur, tellement d'éléments déclencheurs — et vous avez déjà discuté de certains d'entre eux pendant le court moment où j'étais présent cet après-midi — peuvent créer une forte impression de risques sans que ce soit corroboré par des données probantes.

Il est très dangereux de conclure que nous en faisons assez, même si nous savons ce qu'« assez » signifie. Je peux facilement constater que toute cette question cadre avec ce que nous appelons maintenant un problème pernicieux ou une question complexe. Cette complexité peut en soi susciter la confusion et la peur dans la population et peut facilement être manipulée, particulièrement par les médias.

Après avoir examiné plus en profondeur les différentes formes d'infrastructures essentielles qui existent au pays, je me rends compte que nous n'avons pas de système d'infrastructures essentielles, mais bien un ensemble complexe d'infrastructures. Cette complexité, en tant que telle, favorise la confusion et laisse place à la possibilité que des gens aient l'impression que nous sommes plus exposés à des risques que nous le sommes en réalité. De plus, cet ensemble complexe comprend des systèmes bien définis, comme le réseau de distribution d'électricité et les oléoducs, qui fonctionnent très bien en tant que systèmes. Ils fonctionnent très bien individuellement, mais surtout individuellement, puisqu'au fil des ans, ils ont été conçus pour résoudre des problèmes précis liés à leurs propres secteurs.

Je peux donc parler au responsable de la sécurité d'Hydro Ontario, comme je l'ai fait dans le cadre de cette recherche, qui a une idée très précise des menaces existantes. Je crois vraiment que dans n'importe laquelle de ces organisations, il faut parler aux gens de première ligne et non seulement aux membres de l'administration centrale. Ils ont un point de vue d'ensemble concret très précis qui ne correspond pas nécessairement à une vision du monde apocalyptique. J'expliquerai plus tard sur quoi cela repose soit, à mon avis, une connaissance de la collectivité dans laquelle ils mènent leurs activités et du fonctionnement des systèmes.

Ce qui représente une menace, c'est la façon dont les systèmes interagissent ou leurs dépendances mutuelles, ce qui ne cesse de croître. Au Canada, les infrastructures essentielles sont complexes, et elles le sont de plus en plus. Elles sont dispersées sur le territoire et elles appartiennent à différents acteurs dont les programmes et les préoccupations concernant ces menaces, réelles ou perçues, diffèrent. Par définition, elles sont en majeure partie vulnérables. On peut alors se poser la question qui suit : si une bonne part d'entre elles sont vulnérables, pourquoi ne se passe-t-il pas plein de mauvaises choses? Bien que nous puissions en nommer certaines qui se sont produites, aucune tendance constante ne semble l'indiquer, même s'il y a des vulnérabilités : par exemple, une ligne électrique qui traverse le Nord-du-Québec dans une zone isolée et qui fait l'objet d'une inspection toutes les six semaines ou tous les deux mois est surveillée à l'aide de systèmes électroniques qui pourraient être neutralisés par une

Powerlines and pipelines that cross vast, sparsely inhabited areas of land are, by definition, more vulnerable than those in more populated areas due to isolation. However, the intensity of critical infrastructure in more populated areas often represents an inherent risk due to its complexity and due to its proximity to large populations. The degree to which such risk can be mitigated is defined by the interests at stake, not necessarily by the degree of the risk. For instance, the costs of mitigation for privately held critical infrastructure are very real. They're very real to their owners, and they affect the profit margin of those organizations. Are they incentivized to do something only if they feel they have to? Is their line going to be different than for someone perceiving it from a broad systems point of view, say, sitting in Ottawa, from a government point of view, doing analysis? Yes. There are going to be quite different views about what they should be doing, and getting to some common ground is really, I think, a challenge.

I have heard private sector people quite rightly assess such risks with an eye to how credible the risk is and what it would cost to fully mitigate it. Is that right? I'm simply reporting what I have heard.

Such calculations weigh heavily in this field, even when regulatory oversight comes into play. I want to speak to that later.

My broadly based conclusion was that what we really lack are the metrics or measurements to determine an adequate level of response to threats and that this is a systemic, endemic and global problem. It's a dynamic process. I give the federal government credit for trying to herd this bunch of kittens, but it is a bunch of kittens. As we all know, some kittens have claws. By that I mean that there are so many jurisdictions and sectors involved that having the ability to say that everything is under control would be fanciful fiction at best.

My overview conclusion, however, was that the actual threats to critical infrastructure, most notably from the terrorist source, are unstated but also subject to exaggeration based on what we call, in the risk-analysis field, the available heuristic. In other words, if this bomb blew up in Ankara last week, it could blow up in Burlington tomorrow. That's just taking an example and moving it into your own environment, and that's a real tendency that happens in the world of risk.

But I would also add that good and effective risk assessment does not happen on global levels; it happens in communities and at the front end of how systems operate. There are a lot of interesting things going on, but one of the things that I observed was a seeming disconnect in that conversation between those who cyberattaque. Pourquoi les choses ne tournent-elles pas mal? Parce que le personnel de première ligne des organisations fait beaucoup de bon travail.

Les lignes électriques et les pipelines qui traversent de vastes zones peu densément peuplées du territoire sont, par définition, plus vulnérables que celles qui traversent les zones plus peuplées, et ce, parce qu'elles sont isolées. Toutefois, la présence importante d'infrastructures essentielles dans les zones peuplées représente souvent un risque inhérent en raison de leur complexité et parce qu'elles se trouvent à proximité d'un nombre important d'habitants. La mesure dans laquelle les risques peuvent être atténués est définie par les intérêts en jeu, et pas nécessairement par le niveau de risque. Par exemple, les coûts des mesures d'atténuation pour des infrastructures essentielles qui appartiennent à des intérêts privés sont bien réels. Ils le sont pour les propriétaires et ont des incidences sur la marge de profit de ces organisations. Sont-ils motivés à faire quelque chose seulement s'ils sentent qu'ils doivent le faire? Leur perspective sera-t-elle différente par rapport à une personne qui conçoit les choses en fonction de grands systèmes; qui, disons, siège à Ottawa; et qui analyse les choses d'un point de vue gouvernemental? Oui. Leur point de vue sera bien différent quant à ce qu'ils devraient faire, et il est vraiment difficile de trouver un terrain d'entente, à mon avis.

J'ai entendu des gens du secteur privé évaluer assez correctement de tels risques en examinant à quel point un risque existe effectivement et combien coûtera son atténuation réelle. Est-ce exact? Je ne fais que dire ce que j'ai entendu.

Dans ce secteur, de tels calculs pèsent très lourd, même lorsque la surveillance réglementaire entre en jeu. J'en parlerai plus tard.

Ma conclusion générale, c'était que ce qu'il nous manque vraiment, ce sont les instruments qui permettent de déterminer le niveau adéquat de mesures à prendre contre les dangers, et qu'il s'agit d'un problème systémique, endémique et global. C'est un processus dynamique. Je reconnais le mérite du gouvernement fédéral, qui essaie de rassembler tous les acteurs, mais comme nous le savons tous, il y a tellement d'administrations et de secteurs différents qui sont concernés que dire que tout est sous contrôle relèverait de la fantaisie.

Cependant, ma conclusion générale, c'était que les menaces contre les infrastructures essentielles, surtout celles liées au terrorisme, sont implicites, mais aussi exagérées selon ce que nous appelons l'analyse des risques, les éléments heuristiques. Autrement dit, si une bombe a explosé à Ankara la semaine dernière, il pourrait se produire la même chose à Burlington demain. On ne fait que prendre un exemple et l'incorporer dans son propre environnement, et c'est une tendance réelle dans le monde du risque.

Or, j'ajouterais qu'une bonne évaluation du risque efficace ne s'effectue pas à l'échelle globale, mais bien dans les collectivités et au début des processus des systèmes. Il se passe beaucoup de choses intéressantes, mais ce que j'ai observé entre autres, c'est qu'il y avait une discordance apparente entre la tendance qu'ont

tend to try to generalize at the national level, try to make it all one system, and the fact that we are living in a complex world with a lot of pointed ends. There are great people doing great work down there. The communication between the two isn't great.

I would just add four critical observations and then turn it over to Kevin.

I saw a real disconnect between those taking the national, macro view, with a strong focus on terrorism, and those engaged at the front end of critical incident systems and local police, with a great concern for vandalism leading to major systems breakdown. A gang of bikers taking out an electrical distribution system to steal the copper wire can shut down the system just as much as someone driven by terrorism. Local police working with their communities over time produce a level of intelligence, awareness of these systems, that the macro systems are not necessarily equipped to do.

What we are now seeing emerging as an alarming threat is the single radicalized actor working on his or her own, who has been inspired, as in this previous discussion, to do something by such groups as IS. These are the ones that only local and ongoing conversations can, in fact, deal with.

I have long believed that we need to listen to those at the front end of organizations. I'm not sure that their voices are being heard enough. That observation came out of my research basically very viscerally when you talk to people, saying, "We're identifying these things; we're talking certain danger; we're hearing another agenda at the national level." Interesting observation.

A couple of broader observations: I think that there's a very real human resource capacity issue at play with respect to critical infrastructure and the threats that they face. By that I mean the need to grow the skill sets for people working in the system, the need to develop, as we saw with the Carleton example from your previous witness, courses to understand and develop skills in this area. Developing areas of expertise within the various critical infrastructure systems and across them is a human resources challenge. I know that this isn't sexy, but, in fact, having the right people with the right skills in the right place is kind of important in this area. This is a new and emerging set of knowledge.

There are people with considerable skills in this area, and I'm impressed by them. They often work either in isolation or within one of the system's stovepipes. Therefore, someone in the pipeline is a pipeline person; they would never talk to someone in cyber. Yet, today, these things are becoming integrated. There's no

des gens à essayer de généraliser, de créer un seul système national, et le monde complexe dans lequel nous vivons. Des gens formidables font de l'excellent travail. La communication entre les deux n'est pas très bonne.

Je vais seulement ajouter quatre observations critiques et je céderai la parole à Kevin par la suite.

J'ai constaté qu'il y a un véritable fossé entre les gens qui adoptent une optique nationale, qui ont une conception large, et se concentrent fortement sur le terrorisme; et ceux qui sont mobilisés au début du processus pour ce qui est des systèmes d'incidents et les policiers locaux qui se préoccupent grandement des actes de vandalisme pouvant causer une panne majeure des systèmes. Tout comme dans le cas d'une personne qui commettrait un acte terroriste, un groupe de motards qui met un réseau de distribution d'électricité hors service pour voler un fil de cuivre peut paralyser le système. Au fil du temps, un service de police local qui travaille auprès de sa collectivité produit des renseignements et une connaissance des systèmes que les macrosystèmes ne sont pas nécessairement en mesure d'égaler.

Nous voyons maintenant surgir une menace inquiétante, soit celle d'acteurs qui se radicalisent, qui agissent seuls et qui, comme on l'a mentionné dans la discussion précédente, sont inspirés par des groupes comme le groupe armé État islamique. Seuls des contacts réguliers menés par des acteurs locaux peuvent, en fait, mener à quelque chose dans ce cas.

Je crois depuis longtemps que nous devons écouter les membres du personnel de première ligne des organisations. Je ne sais pas s'ils se font assez entendre. Cette observation est ressortie très viscéralement de mes travaux. On parle à des gens. « Nous déterminons ces choses; nous parlons de certains dangers; nous entendons parler d'un autre programme à l'échelle nationale ». C'est une observation intéressante.

Je vais faire deux ou trois observations générales. Je pense qu'il y a vraiment une question de capacité des ressources humaines en jeu concernant les infrastructures essentielles et ce qui les menace. Je parle ici de la nécessité d'accroître l'ensemble des compétences des gens qui travaillent dans le système, le besoin d'élaborer — comme nous l'avons vu avec l'exemple de l'Université Carleton qu'a donné votre témoin précédente — des cours dont l'objectif est de connaître et de développer des compétences dans ce secteur. Développer des domaines d'expertise dans les différents systèmes d'infrastructures essentielles et entre ceux-ci constitue un défi sur le plan des ressources humaines. Je sais que ce n'est pas attirant, mais en fait, dans ce domaine, il est plutôt important que les bonnes personnes ayant les compétences qu'il faut soient au bon endroit. Il s'agit d'un nouvel ensemble de connaissances.

Des gens ont des compétences considérables dans ce secteur, et ils m'impressionnent. Ils travaillent souvent de façon isolée ou dans l'un des vases clos du système. Par conséquent, une personne qui travaille dans le secteur des pipelines est considérée comme telle; elle ne parlera jamais à une personne qui travaille dans la

human resource strategy in a field that demands a human eye and instinct to understand potential risk and validate it.

I would advocate for a sector human resources council, such as have been in existence, although it was unfortunately suspended in the police area for a number of decades. The police sector council was an attempt to develop police human resource capacity, and it did some amazing work over the period of its existence.

There's a knowledge capacity issue at play here, one that Canada can make a major contribution to given who the players are in the field right now. In some respects, we really do not know what we do not know in terms of the nature of the risk, what can be done, who is doing things that we can learn from, and how we can develop transferable knowledge of solutions, techniques and risk mitigation that can transcend these stovepipes.

I would suggest more research capacity. I'm sounding like an academic, but it would be really nice to talk from an evidence base on a lot of these things. Unfortunately, in this field, while there's a lot of evidence, there's also a lot of non-evidence walking around the issue. Therefore, thinking about how we develop knowledge in this area is very important going into the future.

The speed of change in the cybernetic area is of concern for two reasons. Obviously the hacker phenomenon writ large remains a growing concern. We now see a nation stage attacks and their victims responding. What can this mean for the future? The need to ensure our defence systems are up to date is a key concern. The other side of these phenomena with respect to critical infrastructure is the growth of remotely monitored control and observation systems being put in place in our critical infrastructure in the name of improving safety. These are not immune from manipulation. We have to worry about the potential for attack.

Over the past decade, I have seen our police services — nationally of course through the RCMP, but most notably in our large urban police services — engage more and more in investigations, operations and community-based interventions associated with the detection and prevention of terrorist activities. They have been compelled to skill up to respond to these and have done some amazingly good work, both at the point of investigation and on the part of trying to develop community interactions that ensure we never see a situation where a problem has arisen and it becomes a cold call between the community and the police. They have to be interacting.

The police services, in responding to these circumstances and doing this work, have incurred major costs. This has become a major cost driver in the area of policing as resources are deployed.

cybernétique. Pourtant, ces choses commencent à être coordonnées. Il n'y a pas de stratégie des ressources humaines dans un domaine qui nécessite un regard humain et de l'instinct pour comprendre les risques potentiels et confirmer.

Je recommande l'établissement d'un conseil des ressources humaines du secteur, comme celui qui est en place, bien qu'il ait été malheureusement suspendu dans les services policiers pendant un certain nombre de décennies. La création du conseil sectoriel de la police visait à établir une capacité en ressources humaines. Il a accompli un travail extraordinaire.

Une question des capacités du savoir est en jeu ici, et le Canada peut jouer un rôle important compte tenu des acteurs qui sont sur le terrain à l'heure actuelle. À certains égards, nous ne savons vraiment pas ce que nous ignorons sur le plan de la nature du risque, quelles mesures peuvent être prises, qui peut nous apprendre des choses et comment nous pouvons créer des connaissances transférables sur des solutions, des techniques et l'atténuation des risques pouvant transcender les vases clos.

Je suggère le renforcement des capacités de recherche. Je parle comme un universitaire, mais il serait vraiment bien de pouvoir discuter en se basant sur des faits concernant bon nombre de ces choses. Malheureusement, dans ce domaine, même s'il y a beaucoup de données, il y a aussi absence de données. Par conséquent, il sera très important de réfléchir à la façon dont nous développerons des connaissances dans ce secteur.

Le rythme des changements dans le domaine de la cybernétique est inquiétant pour deux raisons. Évidemment, le phénomène des pirates informatiques, de façon générale, est de plus en plus préoccupant. Nous voyons maintenant une nation organiser des attaques et les victimes y réagir. Qu'est-ce que cela laisse présager pour l'avenir? La nécessité de nous assurer que nos systèmes de défense sont à jour constitue une préoccupation importante. L'autre aspect de ces phénomènes en ce qui concerne les infrastructures essentielles, c'est la croissance des systèmes de contrôle et d'observation à distance qui sont mis en place dans nos infrastructures essentielles au nom du renforcement de la sécurité. Ils ne sont pas à l'abri de manipulations. Nous devons nous soucier des risques d'attaque.

Au cours de la dernière décennie, j'ai constaté que nos services de police — la GRC, évidemment, à l'échelle nationale, mais surtout nos grands services de police urbains — participent davantage à des enquêtes, à des opérations et à des interventions communautaires en vue de détecter et de prévenir les activités terroristes. Ils ont dû perfectionner leurs compétences en conséquence et ont accompli un travail remarquable, tant au niveau des enquêtes que des interactions avec les collectivités. Nous ne voudrions surtout pas qu'un événement grave survienne sans que les services de police aient pu créer des liens avec les collectivités au préalable. Ils doivent donc interagir les uns avec les autres.

Les services de police ont dû engager des dépenses considérables pour être en mesure de faire face à ces circonstances et de mener ces activités. L'affectation de

New analytic capacity is added, and greater interoperability adopted between and among police services. These costs have not been given the recognition they deserve.

So these are some trends that my research has identified. A number of remedies are available. I've suggested some to you. I see three broad areas where we need to improve, as well as those specifics I've just mentioned. We need to improve how government and industry assess risk and communicate it; we need to grow our knowledge base through research, centres of excellence, sharing of leading practice through documented cases and forums for professionals in this field to interact; and finally, we need to develop more incentives for industry to invest in critical infrastructure resiliency and resource new players within the public sector, as well as increase the regulation by government and the setting of standards for this through the government's regulatory capacity. Thank you.

Kevin Quigley, Associate Professor and Director, MacEachen Institute for Public Policy and Governance, as an individual: I'd like to talk about risk regulation to limit the possibility of low-probability, high-consequence events, disasters, crises, so-called black swan events, to our critical infrastructure. I'm talking about natural disasters, industrial failures and terrorist attacks. I'm not going to limit myself to terrorist attacks.

My recent research is focused on two critical sectors in particular, the Canadian transportation sector and the chemical manufacturing sector. I've done a fair bit of work on the food sector as well. I study risk regulation in a broad context looking at the law, markets, media, public opinion, organized interests and organizational culture.

Markets, left to their own devices, do not always prepare for black swan events. In fact, markets can increase the probability of black swan events by rewarding risk-taking behaviours. We saw this in in the Lac-Mégantic tragedy in which regulatory standards and business practices designed to improve efficiencies and reduce costs contributed to a failure that ended in disaster. Small and medium-sized enterprises, companies like Montreal, Maine and Atlantic Railway, are increasingly important to global supply chains, but they don't often have adequate risk management staff, expertise or insurance. They respond to profit motives and don't give much attention to preventing disasters they feel are unlikely to occur. This makes perfect market sense. Markets are central to our society. They are the foundation of our economic system, but they reward behaviours and ways of thinking that don't always contribute to effective critical infrastructure protection.

ressources est devenue un inducteur de coûts important dans le domaine des services de police. Que ce soit pour améliorer la capacité analytique ou l'interopérabilité au sein des services de police, ces coûts n'ont pas reçu l'attention qu'ils méritent.

Voilà donc ce qui ressort de mes recherches. Il y a plusieurs solutions possibles. Je vous en ai proposé quelques-unes. Je considère qu'il y a trois grands secteurs où nous devons apporter des améliorations, mis à part les cas précis dont je viens de vous parler. Nous devons améliorer la façon dont le gouvernement et l'industrie évaluent les risques et les communiquent; accroître notre base de connaissances grâce à la recherche, la création de centres d'excellence, la mise en commun de pratiques exemplaires à la lumière de cas documentés et au moyen de tribunes où les professionnels du domaine peuvent interagir; et enfin, mettre en place des mesures pour inciter les entreprises à investir dans la résilience des infrastructures essentielles et à susciter l'engagement de nouveaux joueurs au sein du secteur public, ainsi que renforcer la réglementation et l'établissement de normes connexes grâce à la capacité de réglementation du gouvernement. Merci.

Kevin Quigley, professeur agrégé et directeur, MacEachen Institute for Public Policy and Governance, à titre personnel : J'aimerais vous parler de la réglementation des risques visant à réduire au minimum les possibilités d'événements, de désastres et de crises peu probables, mais très lourds de conséquences, c'est-à-dire ce qu'on appelle les « cygnes noirs » concernant nos infrastructures essentielles. Je parle ici des catastrophes naturelles, des défaillances industrielles et des attaques terroristes. Je ne vais pas me limiter aux attaques terroristes.

Mes récents travaux de recherche portaient principalement sur deux secteurs essentiels, soit le secteur des transports et le secteur de la fabrication de produits chimiques au Canada. Je me suis aussi longuement penché sur le secteur de l'alimentation. J'étudie la réglementation des risques dans un vaste contexte qui comprend le droit, les marchés, les médias, l'opinion publique, les intérêts organisés et la culture organisationnelle.

Les marchés, laissés à eux-mêmes, ne sont pas toujours préparés à l'éventualité de cygnes noirs. En fait, ils peuvent même accroître la probabilité de ces événements en récompensant les comportements à risque. Nous l'avons vu à Lac-Mégantic. Les normes réglementaires et les pratiques commerciales, qui avaient été mises en place pour améliorer les gains d'efficience et réduire les coûts, ont entraîné une défaillance qui a tourné au désastre. Les petites et moyennes entreprises, comme la Montreal, Main and Atlantic Railway, jouent un rôle de plus en plus important au sein des chaînes d'approvisionnement mondiales, mais souvent, elles n'ont pas assez d'effectifs, d'expertise et d'assurance en matière de gestion des risques. Elles sont guidées par la recherche du profit et n'accordent pas suffisamment d'attention à la prévention des incidents qui, à leurs yeux, sont improbables. Cela est logique du point de vue commercial. Les marchés sont au cœur de notre société. Ils sont le fondement de notre système économique, mais ils récompensent les comportements et les mentalités qui n'assurent pas toujours la protection des infrastructures essentielles.

In particular, while some critical infrastructure organizations have a safety culture, with the exception of larger airports and larger rail companies, few organizations have a security culture. Not having a security culture creates vulnerabilities for companies but also for supply chains and everyone who depends on critical infrastructure. This is a failure of market forces which governments must address.

Yet governments are ill-equipped to address these market failures in critical infrastructure. Since the 1980s, the dominant narrative in Canada has been that private industry with the profit motive is better at managing critical infrastructure than government. As a result, most critical infrastructure has been privatized or outsourced and, at a minimum, afforded considerable regulatory flexibility.

At the same time, governments have been hollowed out. They have been unable to keep pace with the technical sophistication of critical infrastructure. As a result, government officials now arguably lack the knowledge, skill, time, flexibility and credibility to keep an eye on the CI owners and operators who manage risks to critical infrastructure.

Government finds itself in a conundrum. Polling data suggests Canadians do not consider security a high priority, certainly not compared to health care and economic concerns. Yet the public holds government partly, if not completely, responsible for critical infrastructure failures, despite the fact that government has less and less control over it. The public expects their governments to act and will blame them if they do not. In response, governments assume a cooperative stance with industry and use euphemisms to mask unclear accountability, terms like "information sharing," "trust building," "partnership," "stakeholder," "leadership at all levels" and "federal family."

Meanwhile, media fails to keep a watchful eye on critical infrastructure risk regulation. Black swan events generate a lot of media coverage and a ruthless hunt for someone to blame, more so with industrial failures than natural disasters. However, disasters and crises are complex and require thoughtful and prolonged examination. Despite this, most media coverage ends the same month it starts and focuses more on personalities than on rational risk assessment. When a seemingly healthy boy in Ottawa died of H1N1 in 2009, for example, that event generated 15 times more media coverage in *The Globe and Mail* than the Canada Revenue Agency 2007 computer glitch that limited government's ability to collect or disseminate funds online, which, unlike the boy's death, had very serious and far-reaching economic implications.

Autrement dit, même si certaines organisations du secteur des infrastructures essentielles ont une culture de la sécurité, à l'exception des grands aéroports et des grandes sociétés ferroviaires, très peu d'organisations en ont une, ce qui rend les entreprises, les chaînes d'approvisionnement et tous ceux qui comptent sur les infrastructures essentielles vulnérables. Les gouvernements doivent remédier à cet échec du marché.

Il reste que les gouvernements sont mal outillés pour faire face à ces lacunes. Depuis les années 1980, on a toujours dit qu'au Canada, le secteur privé, qui est motivé par les profits, parvenait à mieux gérer les infrastructures essentielles que le gouvernement. Par conséquent, la plupart des infrastructures essentielles ont été privatisées ou confiées à des sous-traitants et, à tout le moins, elles bénéficient d'une grande souplesse en matière de réglementation.

En même temps, les gouvernements sont dépassés. Ils n'ont pas pu s'adapter à la complexité technique des infrastructures essentielles. Par conséquent, les fonctionnaires n'ont sans doute pas aujourd'hui les compétences, les connaissances, le temps, la souplesse ni la crédibilité nécessaires pour surveiller les propriétaires et les exploitants d'infrastructures essentielles qui gèrent les risques de ces infrastructures.

Le gouvernement se retrouve donc dans une impasse. D'après les sondages, les Canadiens ne considèrent pas la sécurité comme une grande priorité, certainement pas au même titre que les soins de santé ou l'économie. Pourtant, le public tient le gouvernement en partie, pour ne pas dire entièrement, responsable des défaillances des infrastructures essentielles, alors que le gouvernement a de moins en moins de contrôle sur les infrastructures. Le public s'attend à ce que leur gouvernement agisse et il le blâmera pour son inaction. Les gouvernements collaborent avec l'industrie et utilisent des euphémismes pour masquer le manque de clarté de la reddition de comptes. On parle de « communication de renseignements », d'« établissement de liens de confiance », de « partenariat », de « partie prenante », de « leadership à tous les niveaux » et de « famille fédérale ».

Entretemps, les médias ne surveillent pas de près la réglementation des risques des infrastructures essentielles. Les événements improbables qui ont des répercussions très importantes sont très médiatisés et nous amènent à blâmer impitoyablement les responsables, encore plus dans le cas des défaillances industrielles que des catastrophes naturelles. Cependant, les catastrophes et les crises sont complexes et nécessitent une analyse réfléchie et en profondeur. Il n'en demeure pas moins que la plupart des médias cessent de s'y intéresser au cours du même mois et se concentrent davantage sur les personnalités que sur l'évaluation rationnelle des risques. Lorsqu'un jeune garçon en bonne santé est décédé des suites de la grippe H1N1 à Ottawa, en 2009, par exemple, cet événement a généré 15 fois plus de couverture médiatique dans le *Globe and Mail* que le pépin informatique de l'Agence du revenu du Canada en 2007 qui a empêché le gouvernement de percevoir ou de verser de l'argent en ligne, ce qui, contrairement à la mort tragique du garçon, a eu de très graves et lourdes conséquences économiques.

Despite the rhetoric of markets and competition, many large CI organizations are protected from market competition. After all, to borrow and modify an American catch phrase, they are too critical to fail. This dynamic increases government's incentives to restore CI companies after CI failures. Under the guise of competition or security considerations, companies can withhold information from the public. As a result, government often doesn't know how seriously companies take it and how effectively they are managing risks. We do know, however, there are few incentives for most CI sectors to spend time or money on security.

En dépit de la théorie des marchés et de la concurrence, de nombreuses organisations du secteur des infrastructures essentielles sont à l'abri de la concurrence. Après tout, pour reprendre et modifier un slogan américain, elles sont trop essentielles pour échouer. Cette dynamique incite davantage le gouvernement à rétablir les entreprises après une défaillance des infrastructures essentielles. Pour des raisons de concurrence ou des considérations liées à la sécurité, les entreprises peuvent cacher de l'information au public. Par conséquent, le gouvernement ne sait souvent pas dans quelle mesure les entreprises prennent ces risques au sérieux et les gèrent efficacement. En revanche, nous savons qu'il y a certaines mesures en place qui incitent la plupart des organisations du secteur des infrastructures essentielles à consacrer du temps ou de l'argent à la sécurité.

Market failures, ill-informed media coverage, governments' diminished capacity for risk policy and management, and companies that are too big and too critical to fail — these forces converge to empower already powerful critical infrastructure institutions, which the public trust less and less.

Les échecs du marché, les médias mal renseignés, le rôle amoindri des gouvernements dans les politiques et la gestion des risques, et les entreprises qui sont trop importantes et trop essentielles pour échouer — toutes ces forces convergent pour donner du pouvoir aux organisations d'infrastructures essentielles déjà puissantes, en qui le public a de moins en moins confiance.

While some careers end abruptly after critical infrastructure disasters, for the most part, organizations maintain power after black swan events, and sometimes even gain power. The governance system in place privileges stability, efficiency and political expediency. It is concerned less with transparency and accountability. Its commitment to learning over blame shifting could be improved.

Même si certaines carrières prennent fin de façon abrupte à la suite de ces défaillances, la plupart des organisations conservent leur pouvoir après de tels événements, et parfois, elles acquièrent encore plus de pouvoir. Le système de gouvernance en place privilégie la stabilité, l'efficience et l'opportunisme politique. Il est moins préoccupé par la transparence et la reddition de comptes. Son engagement visant à privilégier l'apprentissage plutôt que le blâme pourrait être renforcé.

It is increasingly important that we learn and adapt so that we can address risks associated with climate change, security, aging infrastructure and emerging cyber-threats. To strengthen our critical infrastructure, we must strengthen and extend independent audits, and I welcome the work of this committee in that area; report more frequently on performance, as Andy Graham just mentioned; share information more widely, including to the general public — we need an informed public on these issues; manage the risks associated with small and medium-sized enterprises; deconcentrate single points of failure; enforce appropriate standards and behaviour in a timely manner; increase mindfulness of security; and enhance fairness in our distribution of risks.

Il est de plus en plus important que nous apprenions et que nous nous adaptions de façon à réduire les risques associés aux changements climatiques, à la sécurité, au vieillissement des infrastructures et aux nouvelles cybermenaces. Pour renforcer nos infrastructures essentielles, nous devons resserrer les vérifications indépendantes et en élargir la portée, et d'ailleurs je me réjouis du travail du comité dans ce domaine; faire davantage rapport sur le rendement, comme Andy Graham vient de le mentionner; diffuser l'information à plus grande échelle, y compris au grand public — le public doit être au courant de ces enjeux —; gérer les risques associés aux petites et moyennes entreprises; déconcentrer les points de défaillance uniques; appliquer les normes pertinentes et adopter les comportements appropriés en temps opportun; accroître la sensibilisation à la sécurité; et améliorer l'équité dans notre distribution des risques.

Critical infrastructure protection is not exclusively about government or security; it is about the assets that enable our civilization. We all have a stake in critical infrastructure protection.

Lorsqu'on parle de la protection des infrastructures essentielles, il ne s'agit pas uniquement du gouvernement ou de la sécurité; il s'agit des actifs qui assurent la survie de notre civilisation. Nous avons donc tous intérêt à ce qu'on les protège.

The new government plans to spend considerable sums of money on our critical infrastructure. These investments can enable a significant step forward toward a more desirable society — smarter, greener cities, for example. Critical infrastructure investments can reflect the values and communities we wish to build. The planning we do today will take years to come to

Le nouveau gouvernement compte dépenser des sommes considérables à cette fin. Ces investissements représentent un grand pas vers une société plus enviable — des villes plus vertes et plus intelligentes, par exemple. Les investissements dans les infrastructures essentielles peuvent refléter les valeurs et les collectivités que nous souhaitons édifier. La planification que

fruition. We must consider security, climate change, trade, and the economic challenges and opportunities of the future to maximize the benefits of today's CI investments.

Thank you again for the opportunity to comment on this subject.

The Chair: Thank you. We'll begin our questions.

Senator Mitchell: These were very interesting presentations. Thank you.

Dr. Graham, I'm very interested in your building-of-skills issue. You did give us some context and some you flushed out a bit, but could you give me some more? How would you do that? Are you talking about programs in university — master's degrees, technical programs, subspecialties in computer science or all of the above?

Mr. Graham: All of the above. I don't have an inventory of the current level of offerings in this area across the country, and I think it's time we took a look at what's available.

When you talk to practitioners in the field, one the questions I would ask — and I've usually become quite impressed about what they know and what they've learned — I've sort of said, "Who is going to replace you?" And the answer is, "Well, we'll find somebody, and I'll train them." That's fine; that's a real knowledge-transfer way, and sometimes that's the only way you can do it.

But something struck me: I did a very cursory look around about how many degrees we have in engineering and critical infrastructure assessment. They have a degree between the engineering department at Carleton — and I don't mean to advertise for another university, but you have to give them praise where it's due — between Carleton's engineering department and the Paterson School. They're trying to bring that stuff together.

I think our community colleges and technical levels need to find ways to begin to teach certain areas systematically, at a tactical level: risk in equipment and all the cyberskills that are going to be needed in the future.

I don't have that inventory, but those are the kinds of things we'll have to build.

Senator Mitchell: Dr. Quigley, I don't know whether this was an implication of your statement, but it captured me, because I'm very interested in climate change, as are most Canadians — the threat to critical infrastructure because of climate change. We have a dam that doesn't have water any more. Is that an implication of what you're talking about?

Mr. Quigley: When we interviewed people at seaports, for instance, their number one concern was climate change. We frequently ask people: "What's your top-of-mind critical

nous faisons aujourd'hui prendra des années avant de se concrétiser. Nous devons tenir compte de la sécurité, des changements climatiques, du commerce, des défis et des possibilités économiques à long terme afin de maximiser les investissements d'aujourd'hui dans les infrastructures essentielles.

Je vous remercie, encore une fois, de m'avoir donné la possibilité de m'exprimer sur ce sujet.

Le président : Merci. Nous allons maintenant amorcer la période de questions.

Le sénateur Mitchell : Vos exposés étaient très intéressants. Je vous remercie.

Monsieur Graham, je m'intéresse beaucoup à la question du renforcement des compétences. Vous nous avez mis en contexte et vous nous avez donné quelques précisions, mais pourriez-vous nous en dire davantage à ce sujet? De quoi s'agit-il exactement? Parle-t-on de programmes universitaires — de maîtrises, de programmes techniques, de sous-spécialités en informatique ou de tous ces éléments?

M. Graham : De tous ces éléments. Je ne sais pas exactement quel est le niveau actuel des possibilités qui s'offrent partout au pays, mais je pense qu'il est temps qu'on se penche là-dessus.

Lorsque je discute avec des spécialistes du domaine — et je suis souvent très impressionné par ce qu'ils savent et ce qu'ils ont appris —, je leur demande : « Qui va vous remplacer? » Et ils me répondent : « Nous allons trouver des gens et les former. » C'est logique; le transfert des connaissances est souvent le seul moyen d'assurer la relève.

Toutefois, il y a quelque chose qui m'a étonné. J'ai examiné rapidement le nombre de diplômes offerts en ingénierie et en évaluation des infrastructures essentielles. On offre un diplôme au département d'ingénierie de l'Université Carleton — et je ne veux pas faire de la publicité pour une autre université, mais je crois qu'on doit les féliciter puisqu'ils le méritent — en collaboration avec l'École Paterson.

Je considère que nos collèges communautaires et techniques doivent trouver des façons d'enseigner certains domaines systématiquement, à un niveau tactique : les risques liés à l'équipement et toutes les compétences cybernétiques qui seront nécessaires à l'avenir.

Je n'ai pas l'inventaire, mais je pense que c'est là où il faut renforcer nos compétences.

Le sénateur Mitchell : Monsieur Quigley, je ne sais pas si j'ai bien compris ce que vous avez dit, mais comme la majorité des Canadiens, je me soucie beaucoup des changements climatiques, et vous avez parlé de la menace qu'ils peuvent représenter pour les infrastructures essentielles. Nous avons un barrage qui n'a plus d'eau. Est-ce ce dont vous parlez?

M. Quigley : Lorsque nous avons interrogé des gens dans les ports maritimes, leur première préoccupation était les changements climatiques. Nous demandons souvent aux gens

infrastructure threat? Low-probability, high-consequence sort of stuff." While there is this frequent reference to terrorism, and it gets a lot of media coverage, et cetera, to maybe reinforce the point that Andy was making, at the street level, that's not necessarily what people are as concerned about. At the seaports, there was a lot of concern around climate change — rising sea levels and what that meant for seaports. The Hurricane Sandy event was very troubling for people at seaports.

Senator Mitchell: There's a really important study, chair: climate change and critical infrastructure.

Mr. Quigley: If I may extend on that one point, I am almost reluctant, though, to pick a danger, because it's like casino-activity type stuff. So you need to bake it into the infrastructure, reduce the vulnerabilities around single points of failure and have some adaptive capacity.

I know the committee has talked about resilience before. There are different ways to talk about resilience. There's the organic concept where you modify the bounce back. The problem with the bounce back is that you bounce back to where you were when you were vulnerable in the first place. Why would you want to go back there?

You might actually want to bounce back better, which is a new way of talking about resilience, or use, as I say, a kind of organic process where you're kind of trying to survive, so you adapt according to your threats.

But I think it's a bit of a fool's game to zero in on the terrorism one, the natural disasters or the industrial failures — the accidents sort of thing. Rather, try to build better infrastructure that tries to take into account what the climate is going to be — not the climate change, but the threat environment, let's say, in the future.

For these critical infrastructure investments we're going to be making shortly, it will take a long time to roll that out, and then we will be living with that for the next decade or two. So we need to start thinking about what it will look like 10 or 15 years from now, and ask, how do we build strong, resilient, dependable critical infrastructure that allows us to take advantage of trade deals, be prosperous and efficient — and also manage the security environment where these trade deals will open up?

Senator Mitchell: This question probably more directed to Dr. Graham, but it might apply in both cases: Are you aware of Kanishka and the government-funded project, and is it something that could be focused on these issues?

Mr. Quigley: I've been funded through Kanishka. I wrote three papers. It was enormously beneficial for me, because I had collected quite a bit of data. I interviewed about 80 or so people

quelle est, selon eux, la principale menace aux infrastructures essentielles et ils nous répondent que ce sont les événements peu probables qui sont susceptibles d'avoir des conséquences désastreuses. Même si on pense souvent au terrorisme, puisque cela retient beaucoup l'attention des médias, et cetera, pour revenir à ce qu'Andy disait, ce n'est pas nécessairement ce qui inquiète le plus la population. Dans les ports, on se préoccupait beaucoup plus des changements climatiques, de l'élévation du niveau de la mer et de la menace que cela représentait pour les ports. L'ouragan Sandy a été un événement très troublant pour ces gens.

Le sénateur Mitchell : Monsieur le président, voilà une étude très importante que le comité pourrait entreprendre : les changements climatiques et les infrastructures essentielles.

M. Quigley : Si je peux me permettre, à cet égard, j'hésite à choisir une menace, parce que c'est comme jouer à la loterie. Par conséquent, vous devez tenir compte des infrastructures, réduire les vulnérabilités aux points de défaillance uniques et avoir une certaine capacité d'adaptation.

Je sais que le comité a parlé de la résilience plus tôt. Il y a différentes façons d'aborder la question. Il y a le concept organique où on modifie le rebond. Le problème, c'est que lorsqu'on rebondit, on retourne à notre état initial vulnérable. Pourquoi voudrait-on rebondir dans ce cas?

En fait, ce qu'on veut, c'est mieux revenir. C'est une nouvelle façon de percevoir la résilience ou, comme je l'ai dit, une sorte de processus organique où on essaie de survivre et où on s'adapte en fonction des menaces.

Toutefois, je pense qu'il serait ridicule de se concentrer uniquement sur le terrorisme, les catastrophes naturelles ou les défaillances industrielles — tous les types d'accidents. Nous devons plutôt essayer de construire de meilleures infrastructures qui tiennent compte du climat — non pas des changements climatiques, mais plutôt de l'environnement de la menace à l'avenir.

Nous avons beau investir tout de suite dans les infrastructures essentielles, ces investissements se concrétiseront au cours des deux prochaines décennies. C'est pourquoi nous devons réfléchir à ce à quoi ressemblera la situation dans 10 ou 15 ans. Il s'agit de savoir comment créer des infrastructures essentielles solides, résilientes et fiables qui nous permettront de tirer avantage des accords commerciaux, d'être prospères et efficients — et de gérer l'environnement de sécurité dans lequel de nouveaux marchés pourraient s'ouvrir.

Le sénateur Mitchell : Cette question s'adresse probablement davantage à M. Graham, mais elle pourrait s'appliquer aux deux cas : connaissez-vous le projet Kanishka? Cette initiative financée par le gouvernement devrait-elle se concentrer sur ces enjeux?

M. Quigley : J'ai reçu des fonds dans le cadre du projet Kanishka. J'ai rédigé trois documents. Ce financement m'a été très bénéfique, parce que j'avais recueilli beaucoup de données.

on critical infrastructure in agriculture, transportation and dangerous chemicals. The Kanishka funding allowed me to get that data and flip them into three working papers, which are now on my website and have been handed in to Public Safety Canada.

So it was enormously beneficial. They built on funding I already had, and I could flip them into usable papers for everybody, mine that data and hire research assistants to do the work. It will be put into a manuscript, also. So it was enormously beneficial. I thought it was very worthwhile.

Senator White: Professor Quigley, I always go back to nuclear power, because when they look at their facilities, they look at the myriad of problems they could have rather than the one that's most likely to happen. So you're saying we should be doing that in infrastructure, looking at the myriad of problems that may happen with the dam system, whether climate change, terrorism, power outage, et cetera?

Mr. Quigley: It's worthwhile. If you're talking about what kind of scenario planning you do and what kind of exercises — I pointed out one of the limitations of some of the scenario exercises sizes that organizations sometimes do. They can sometimes pick friendly and convenient partners when they do these scenarios; they come up with these implausible scenarios, because those are the four or five departments that want to work together. But disasters don't come at you in a jurisdictional way. As Andy said, it straddles all three levels and orders of government, a lot of the private sector, and it requires a certain community response. So I think these over-orchestrated learning opportunities are highly constrained in that sense.

Then, are we actually transparent about what we genuinely learned that that exercise?

Just on that point in terms of how we learn, that's a really important one we have to be more creative about.

My sense would be that these are extremely low-probability events, and how we could focus all of our attention on — and also just the kind of the additional risks and threats we take on by overemphasizing terrorism as opposed to saying, "Do we have a genuinely institutionalized learning culture in place where we can bring forward mistakes and errors, and learn from those and build on them?"

The "lessons learned" phrase always kills me. It's "lessons identified." It's not clear to me that we ever learn lessons; our organizational cultures resist it. How do we internalize genuine challenges to organizational culture and adapt? I think we need to do more work in that area.

Whether we learn from an industry failure or otherwise, it might help us to deal with a low-probability, high-consequence event. It will play out differently in the popular culture or media,

J'ai interrogé près de 80 personnes au sujet des infrastructures essentielles dans les domaines de l'agriculture, des transports et des produits chimiques dangereux. Les fonds, accordés au titre du projet Kanishka, m'ont permis de combiner ces données en trois études, qui se trouvent maintenant sur mon site web et qui ont été transmises à Sécurité publique Canada.

Ce financement m'a énormément aidé à poursuivre mes recherches. J'ai pu embaucher des assistants, extraire les données et produire des documents pratiques qui seront également compilés dans un manuscrit. J'estime donc que ce projet est très utile.

Le sénateur White : Monsieur Quigley, je reviens toujours aux centrales nucléaires, parce que lorsqu'elles examinent leurs installations, elles songent à la multitude de problèmes auxquels elles pourraient être confrontées plutôt qu'à celui qui est le plus susceptible de se produire. Vous dites que c'est ce que nous devrions faire dans le contexte des infrastructures, c'est-à-dire se pencher sur tout ce qui pourrait menacer les barrages, que ce soit les changements climatiques, le terrorisme, les pannes d'électricité, et cetera.

M. Quigley : C'est exact. Si vous voulez savoir quel scénario retenir — j'ai mentionné l'une des limites des scénarios qu'évoquent parfois les organisations. Au moment d'envisager ces scénarios, les entreprises choisissent souvent des partenaires amicaux et commodes, et on se retrouve avec des scénarios peu plausibles, étant donné que ce sont les quatre ou cinq ministères qui veulent travailler ensemble. Toutefois, les crises ne tiennent pas compte des champs de compétence. Comme Andy l'a dit, elles touchent les trois ordres de gouvernement et une grande partie du secteur privé et elles nécessitent une certaine intervention de la part des collectivités. Par conséquent, j'estime que les occasions d'apprentissage trop orchestrées sont très limitées à cet égard.

Ensuite, sommes-nous suffisamment transparents au sujet de ce que nous avons véritablement appris?

À cet égard, je considère qu'il faudrait faire preuve de davantage de créativité.

À mon avis, ce sont des événements très peu probables, et la façon dont nous pourrions concentrer tous nos efforts sur... Nous prenons des risques en accordant trop d'importance au terrorisme. Nous devons plutôt nous demander si nous avons une culture d'apprentissage en place qui nous permet de tirer parti de nos erreurs pour aller de l'avant.

Je n'ai jamais aimé l'expression « leçons retenues ». Il s'agit plutôt de « leçons relevées ». Je ne suis pas certain qu'on ait déjà tiré des leçons; notre culture organisationnelle s'y oppose. Comment intégrer les véritables défis à notre culture organisationnelle et nous adapter? Je pense que nous devons intensifier nos efforts dans ce domaine.

Que nous apprenions d'une défaillance industrielle ou autrement, cela pourrait nous aider à faire face à un événement peu probable et lourd de conséquences. Cela va se dérouler

but there's a lot to be said — we could concentrate a lot more minds if we can get some buy-in across a spectrum of low-probability, high-consequence events instead of saying, "Let's focus on terrorism," in which case you might get a certain degree of skepticism.

Senator White: Professor Graham, if I may, you talked about educational opportunities. Back about 15 years ago, concerns were raised about departmental security officers in every department in the country, primarily because they started at a different level. Often they were about administration and passes and things like this, and post-9/11 they became much bigger. But certainly from 9/11 to 2010-11 there hasn't been a dramatic change in the educational opportunities for those people. There may be some more training, but that is rote-based and not about learning new things. It's often about repeating the same thing over and over.

Are we in a better place now? You're trying to think of a place that you might be able to recommend without going outside of your university, I'm sure, but I can't think of a place. There are some programs, but they're all small.

Mr. Graham: Just to build on your comments, because I think they're right on, the security was, as you say, somebody who was looking after the administration. They have to now apply skills that they never had to apply if they're going to get into a safety culture.

Senator White: To gain skills they've never had.

Mr. Graham: They're going to have to do analysis of events. One of the things they have to get involved in is looking at patterns and advising around operations and understanding things going on. I've spoken to people in security and who may wear this moniker of the risk officer, and I hear, "What do I do?" One thing that struck me continuously is how isolated they are from the overall process of running the organization.

Going back to your point about education, some good stuff is going on. I would suggest that there's not enough, and there's not enough that moves them into being effective at the new job of security officer. I would say a lot of these people before just got on with their experience and minimal education, and now they have to deal with analytics and a whole bunch of capacities that they never had. Degrees make a lot more sense in that regard.

différemment au sein de la population ou des médias, mais on pourrait en dire long... Ce qu'il faut surtout, c'est obtenir l'adhésion générale, plutôt que de se concentrer sur le terrorisme, car cela pourrait susciter un certain degré de scepticisme.

Le sénateur White : Monsieur Graham, vous avez parlé des perspectives d'apprentissage. Il y a une quinzaine d'années, on s'interrogeait quant à la compétence des agents responsables de la sécurité dans tous les ministères au pays. Ces inquiétudes étaient principalement dues au fait que les agents en question avaient amorcé leur carrière à un autre niveau, que ce soit dans l'administration, la gestion des laissez-passer ou des secteurs semblables, avant d'accéder à ce poste qui a pris beaucoup plus d'importance depuis le 11 septembre. Les perspectives d'apprentissage de ces agents ne se sont toutefois guère améliorées, en tout cas, certainement entre le 11 septembre et 2010-2011. Il y a peut-être certaines activités de formation, mais elles visent davantage la consolidation des acquis via la répétition que l'apprentissage de nouvelles notions.

Sommes-nous en meilleure posture actuellement? Vous tentiez de penser à un programme à recommander sans sortir des cadres de votre université, mais je n'arrive pas à voir où on pourrait en trouver. Il existe certains programmes, mais ils sont tous de petite taille.

M. Graham : Je vais poursuivre dans le sens de vos observations, car vous aviez tout à fait raison; la sécurité était en effet confiée à quelqu'un qui s'occupait des aspects administratifs de la chose. Si l'on veut implanter une véritable culture de la sécurité, ces agents doivent désormais compter sur des compétences qu'ils n'ont jamais eu à utiliser auparavant.

Le sénateur White : Ils doivent acquérir de nouvelles compétences.

M. Graham : Ils doivent être capables d'analyser les événements. Ils doivent notamment étudier les tendances, formuler des conseils sur les modes de fonctionnement et être en mesure de comprendre ce qui se passe. J'ai parlé à certains de ces agents de gestion du risque qui ne savent pas en quoi consiste leur rôle. Je m'étonne sans cesse de constater à quel point ces gens-là sont isolés de la gestion de l'organisation.

Pour revenir à votre question concernant l'éducation, certains bons programmes sont offerts. Je dirais toutefois qu'il n'y en a pas assez, et qu'ils sont trop peu nombreux à permettre d'acquérir les compétences nécessaires pour s'acquitter efficacement du nouveau mandat d'agent de la sécurité. Auparavant, bien des gens accédaient à ce poste en s'appuyant sur leur expérience et un niveau de scolarisation minimum. Ils doivent maintenant effectuer un travail d'analyse et utiliser un large éventail de compétences totalement nouvelles. Il est donc désormais beaucoup plus logique de rechercher des candidats diplômés.

Some universities and colleges are doing some things, but I don't think we're funding a lot of that sort of thing on a systemic basis. That actually drives it into the provinces, not just the federal government.

The Chair: That was the one thing that I would like to raise. Probably 80 per cent or 90 per cent of the infrastructure that we're talking about will be provincial, if not in the private sector, as to what is perhaps expected in terms of giving some care and attention to the question of critical infrastructure and what you can do to prevent it from being damaged or attacked.

I don't think we can concentrate just on the question of the terrorist attack. There are so many other elements to this that we have to understand. This is a very broad issue.

One aspect that we can take as an opportunity, I would say, and I'd like to hear Dr. Quigley's comment on this, is that from the point of view of what is happening globally and within the terrorism activity that's happening around the world and in Canada, it gives us an incentive to take a hard look at what we have and have this conversation. We can then promote a constructive look at how we're running our various systems so that we prevent ourselves from getting into a situation that we don't want to be in. That's primarily to have those individuals, companies and others, take it very seriously and take a second look, and look at how we can prevent someone or some people from damaging this particular type of infrastructure.

Perhaps you want to comment on that.

Mr. Quigley: Sure, I'm happy to. Thank you for that question.

I'll make a couple of points. First of all, I've done a fair bit of work with the U.S., the U.K. and Australia on critical infrastructure also. When I mentioned earlier that these documents are peppered with phrases like "trust building," "information sharing" and whatnot without any kind of reference to standards or appropriate behaviour change, Canada is not alone in this. These phrases are in the U.K., American and Australian documents. The documents seem very similar in many respects.

However, I would say — and this is maybe a reference to an earlier comment from one of the earlier sessions — that security is a cultural issue and is deeply embedded in who we are and how we respond to it. I don't think it's all that easy to look at the British, Australian and American experiences. You just call that a best practice, let's say, and pick it up and bring it here. Even if you took the same strategies and put them here, it would be operationalized differently, because it would be operationalized in a Canadian context — maybe in terms of the Canadian identity, but also Canadian institutional arrangements. The fact that we have a strong federal system, that most of the assets are at the provincial and municipal levels and in the private sector, that might be different from the cultural and institutional

Il y a des universités et des collèges qui offrent certains programmes, mais je ne pense pas qu'il existe de financement systématique à cet égard. Dans ce contexte, le dossier ne relève plus uniquement du gouvernement fédéral; les provinces ont aussi un rôle à jouer.

Le président : C'est justement l'un des éléments que je souhaitais soulever. Quand il s'agit de déterminer les mesures à prendre pour faire en sorte que les infrastructures essentielles soient à l'abri des dommages ou des attaques, il faut considérer qu'entre 80 p. 100 et 90 p. 100 de ces infrastructures sont du ressort des provinces, lorsqu'elles n'appartiennent pas carrément au secteur privé.

Je ne crois pas que nous puissions concentrer uniquement nos efforts sur les risques d'un attentat terroriste. C'est une problématique très vaste qui comporte de nombreuses autres facettes qu'il nous faut arriver à bien comprendre.

Quand on voit ce qui se passe actuellement avec l'activité terroriste à l'échelle planétaire comme au Canada, je crois que nous devrions être incités, et j'aimerais savoir ce que M. Quigley en pense, à examiner d'un œil critique nos processus en place et à tenir ce genre de débat. Tout cela irait dans le sens d'une analyse constructive du fonctionnement de nos différents systèmes de manière à éviter de nous retrouver dans une situation fâcheuse. Il faudrait d'abord et avant tout que les intervenants, les entreprises et les autres parties prenantes envisagent les choses sous un angle différent pour voir comment nous pouvons éviter que ces infrastructures névralgiques soient endommagées.

Peut-être pourriez-vous nous dire ce que vous en pensez.

M. Quigley : Avec plaisir. Merci pour cette question.

J'aurais quelques réflexions. Disons d'abord que je me suis beaucoup intéressé également à la situation des infrastructures essentielles aux États-Unis, au Royaume-Uni et en Australie. Je parlais tout à l'heure de ces documents truffés d'expressions comme « renforcement de la confiance » et « partage de l'information », sans qu'il soit question de normes ou de changements de comportement souhaités, mais le Canada n'est pas le seul à le faire. On peut retrouver les mêmes expressions dans les documents britanniques, américains et australiens. À bien des égards, ces documents présentent de nombreuses similitudes.

Je dirais toutefois — c'est peut-être en référence à une observation entendue tout à l'heure — que la sécurité est une question de culture qui est étroitement liée à la nature d'un peuple et à la manière dont il réagit à certaines choses. Je ne pense pas qu'il soit si facile de s'inspirer des expériences vécues au Royaume-Uni, en Australie et aux États-Unis. Il ne suffit pas nécessairement de déterminer qu'il s'agit d'une pratique exemplaire pour ensuite la mettre en œuvre chez nous. Ainsi, des stratégies identiques ne seront pas appliquées de la même manière, car il faudra tenir compte du contexte canadien, notamment pour ce qui est de notre identité propre, mais aussi de la structure de nos institutions. Nous avons ici un régime fédéral fort au sein duquel la plus grande partie des actifs se

arrangements in the U.K. I'm not really sure it's as easy to lift those experiences and plant them, even if you have the same language. I think it would be operationalized a little differently.

To your point about how we protect critical assets and how we prepare front-line staff, to go back to Mr. Graham's point about how we listen to front-line staff, I would really emphasize that with a lot of the critical infrastructure interviews we did, front-line staff don't take the terrorism threat that seriously. They just don't think it will happen here. "Not to me, not on my watch, not on my system." It seems like something for television.

That's why I would say that broadening the spectrum of possibilities and talking about low-probability, high-consequence events, sure, talk about terrorism on the menu, and the fact is that terrorism, if it happens, will have a different impact in terms of public response than a natural disaster or industrial failure; they play out differently in the media. In terms of practical application, there is benefit to thinking about these black swan events, talk about it that way, because you'll get more buy-in on the front-line level.

They're saying to us that they're worried about rising sea levels. As psychologists say, why not start with where the client or patient is? If that's what they're worried about, start there and try to introduce different kinds of scenarios that might include terrorism also. But I believe it has to be put in that broader context in order for it to be credible. It's such a low-probability event and so dramatized on television and in popular culture that I don't think people connect with it in their day-to-day living. That would be my observation.

Senator Mitchell: You make the point, Dr. Quigley, and I accept it implicitly because I'm an independent Liberal, that markets left to their own devices don't always prepare for black swan events, but I also believe that markets drive things, as you do. You're not saying that they don't.

It just dawned on me that there's a huge amount of investment risk in the potential for critical infrastructure attack and/or erosion in one form or another due to climate change. We have begun to require that public companies report on their assessment of risk due to climate change. I wonder if we need to require

retrouvent aux échelons provincial et municipal ainsi que dans le secteur privé, ce qui peut être différent de la culture et de la structure institutionnelle au Royaume-Uni. Je ne suis donc pas vraiment certain qu'il soit si facile d'importer ces expériences pour les implanter chez nous, et ce, même si nous parlons la même langue. Je crois que le tout devra se concrétiser de manière un peu différente.

Quant à la façon dont nous protégeons nos infrastructures névralgiques et dont nous pouvons former les employés travaillant sur place, je reviendrais aux commentaires de M. Graham quant à l'importance d'écouter ces employés. À ce titre, je tiens à souligner qu'il est ressorti des nombreuses entrevues que nous avons tenues pour l'étude des infrastructures critiques que les employés de première ligne ne prennent pas vraiment au sérieux la menace terroriste. Ils ne croient tout simplement pas que cette menace puisse se concrétiser au Canada. « Cela ne peut pas m'arriver à moi, pas tant que je serai là, pas dans mon système. » C'est comme s'il s'agissait d'histoires uniquement bonnes pour la télé.

C'est la raison pour laquelle il m'apparaît bénéfique d'élargir le spectre des possibilités en parlant de ces événements peu probables à forte incidence. Il faut en effet traiter de terrorisme et du fait qu'un éventuel acte terroriste aura sur la population des répercussions différentes de celles d'une catastrophe naturelle ou d'une défaillance industrielle, notamment parce que les médias en font un tout autre traitement. Dans la pratique, il est donc avantageux d'envisager ces événements peu probables ayant de fortes incidences, car cela permet une plus grande mobilisation des employés de première ligne.

Si ces gens-là nous disent s'inquiéter de l'élévation du niveau de la mer, alors nous devrions imiter les psychologues en les rejoignant là où ils sont rendus. Si c'est leur principale préoccupation, commençons par cette question en essayant de faire progressivement intervenir différents types de scénarios pouvant inclure le terrorisme. Je crois cependant qu'il convient de présenter le phénomène dans ce contexte plus général afin qu'il soit crédible. Comme c'est un événement qui risque très peu de se produire, et qui est très dramatisé à la télévision comme dans la culture populaire, il devient plus difficile pour les gens de faire le lien avec leur vie de tous les jours.

Le sénateur Mitchell : Monsieur Quigley, vous avez soulevé un argument que j'accepte d'emblée en ma qualité de libéral indépendant. Vous avez dit que les marchés laissés à eux-mêmes ne se préparent pas toujours en fonction d'événements peu probables à forte incidence. Je crois également que les marchés peuvent accroître les risques que de tels événements se produisent, et vous n'avez pas dit le contraire.

Je viens tout juste de réaliser que les menaces qui planent sur nos infrastructures essentielles, tant sous la forme d'une attaque que d'une dégradation quelconque due aux changements climatiques, font grimper en flèche les risques liés aux investissements. Nous avons commencé à exiger des entreprises

companies to report on their assessment of risk due to critical infrastructure vulnerabilities.

Mr. Quigley: I think we could be looking at a much more rigorous program in critical infrastructure. To give the players the benefit of the doubt, I think we've been in a maturing process, and a lot of it is about information gathering and getting the right people to the table. We're several years after 9/11 now. It's taken a bit of time, but I think we're getting there.

One the points I've tried to make before is that information gathering and sharing alone will not control the system. Not to suggest you want ultimate control over the system, but if you're trying to exert a level of control we need to talk about standards and appropriate behaviour. These are the critical assets upon which society depends, so maybe we need to have more discussions about more transparency and accountability, about how these assets are being managed, and have some confidence in the public.

Senator Mitchell: If we looked at it from the additional perspective of financial investment risk, it would draw in a whole different realm of intensity.

Mr. Quigley: I'm not sure what you mean by that. Could you clarify?

Senator Mitchell: If I'm investing in a bank, maybe I want to know which bank is taking best care of the potential for infrastructure cyberhacking.

Mr. Quigley: Indeed. I would add one nuance to it, but I agree. When I talk about fair distribution of risk in my statement, whether I invest in the bank or not, I depend on the bank, and even if I don't have money to invest in the bank I want to know the bank is safeguarding my money appropriately because these are critical assets for this whole community, not just the shareholders. I wonder if we shouldn't be thinking in those terms.

Let me make one other point.

Senator Mitchell: It would be one way to catalyze them.

Mr. Quigley: You're correct. I think that's true. One other point that I would make is do people trust the owners and operators of critical infrastructure? I was quite interested in hearing the discussion about cyber that's been occurring this afternoon. People don't trust banks generally, and government doesn't do much better, actually. Canadians tend to trust their bankers and government more than our allies trust theirs, but it's still a bit low. However, people trust the technology sector. They have incredible optimism, and they're very positive, yet there is quite a bit of vulnerability. You spent a good bit of the day talking about the vulnerabilities in the technology sector, but it

publiques qu'elles fassent état de leur évaluation des risques attribuables aux changements climatiques. Je me demande si nous ne devrions pas faire de même pour ce qui est des risques associés à la vulnérabilité des infrastructures névralgiques.

M. Quigley : Je pense qu'il faudrait envisager des mesures beaucoup plus rigoureuses à l'égard des infrastructures critiques. Pour laisser à chacun le bénéfice du doute, je dirais que nous avons vécu un processus de maturation, et qu'il faut surtout s'employer à recueillir les données nécessaires et à mobiliser les intervenants concernés. Plusieurs années se sont écoulées depuis les attaques du 11 septembre. C'est un long processus, mais je crois que nous cheminons dans la bonne direction.

J'essayais de faire valoir précédemment que le niveau de contrôle requis ne peut pas s'appuyer uniquement sur la cueillette et la mise en commun de l'information. Sans prétendre vouloir tout contrôler, il convient d'établir des normes et des critères de comportement pour pouvoir exercer un niveau de contrôle acceptable. Comme il s'agit d'actifs essentiels dont la société dépend, il serait peut-être bon que nous parlions davantage de transparence et de reddition de comptes ainsi que de la manière dont ces actifs sont gérés si on veut renforcer la confiance des citoyens.

Le sénateur Mitchell : Si l'on examine la question également dans l'optique du risque financier lié aux investissements, on passe à un niveau d'intensité bien différent.

M. Quigley : Je ne vois pas trop ce que vous voulez dire par là. Pourriez-vous préciser?

Le sénateur Mitchell : Si je souhaite investir dans une banque, peut-être que je vais vouloir savoir quelle banque est la mieux préparée à l'égard des risques de cyberpiratage.

M. Quigley : Effectivement. Je suis d'accord, mais j'apporterais une nuance. J'ai parlé dans ma déclaration d'une répartition plus équitable des risques et, que je dispose ou non des fonds nécessaires pour investir dans une banque, je compte sur elle pour qu'elle protège bien mon argent. Il s'agit en effet d'actifs essentiels pour tous les épargnants, et pas seulement pour les actionnaires. C'est peut-être la façon dont nous devrions voir les choses.

Il y a une autre question que je pourrais poser.

Le sénateur Mitchell : Ce serait une manière de catalyser le tout.

M. Quigley : Vous avez raison. Je crois par ailleurs qu'il convient de se demander si les gens font confiance aux propriétaires et aux exploitants des infrastructures essentielles. J'ai écouté avec grand intérêt les échanges sur la cybersécurité plus tôt cet après-midi. D'une manière générale, les gens ne font pas confiance aux banques, et les gouvernements ne s'en tirent guère mieux. Le niveau global de confiance des Canadiens envers leurs banquiers et leurs dirigeants gouvernementaux est plus élevé que celui des citoyens de nos pays alliés, mais demeure tout de même un peu faible. En revanche, les gens font pleinement confiance au secteur technologique. L'optimisme est incroyable et les gens sont

doesn't resonate with Canadians. We talk about media coverage of cyber stuff, but cyber doesn't come anywhere near the other disasters I've been talking about — the industrial failures, the natural disasters, the pandemics. This blows cyber out of the water. People think highly and positively about their technology and very optimistically. They don't feel there is a danger or threat. However, when we get together as a security community, we talk about it, and we all agree that it is a big threat, a big vulnerability, but the general public does not connect with it in that way. They're very positive about that sector. An education program is required — not to scare them, but to bring them along and to say that there is a lot of vulnerability. We're in an unregulated space here, and there is risk associated with that.

Senator Mitchell: Some time ago, we did a study in the Energy Committee on transportation of petroleum safety, including pipelines. We met with Mark Fleming from Saint Mary's University, who is big on safety culture. A lot of what you're talking about, Dr. Graham, is culture. You referred to security culture.

Mr. Graham: Right.

Senator Mitchell: I don't know that I need an answer as much as I'd like to encourage that thought, because Professor Fleming makes some powerful points that what we think is safety culture really isn't. It's not just counting slips and near misses. And security culture is even more complicated. It took us years to get to the place we are now with safety culture to the extent that we got there at all.

Mr. Graham: One of the pillars of both the safety culture and the security culture is actually dealing with real problems. I would go back to Senator White's reference to the nuclear industry as one that has had a pretty good record of identifying and doing two things. First, it has identified real problems, not potential unreal or pretended problems. You mentioned near misses, but part of that culture is that you encourage and find ways in which the cracks are identified and you don't go to blame so quickly. The nuclear industry has done a really good job at that in terms of developing that kind of culture, and there is a lot to be learned from it. It is really quite shocking.

We have a rolling pipeline system called the railway. Is the safety culture as strong there? Well, I don't know what the answer is, but I don't know that we have the metrics or that it has been studied enough to know, but it needs to be.

très positifs, malgré que ce soit un secteur plutôt vulnérable. On peut parler sans relâche des risques associés au secteur technologique sans parvenir à convaincre les Canadiens. Les médias font état des infractions à la cybersécurité, mais celles-ci sont bien loin de susciter le même niveau d'intérêt que les autres situations de crise dont j'ai parlé, comme les défaillances industrielles, les catastrophes naturelles et les pandémies. Les gens ont une opinion très favorable de leurs outils technologiques et ils sont très optimistes à cet égard. Ils n'ont pas l'impression qu'il y ait de menace ou de danger. Lorsque nous nous réunissons entre spécialistes de la sécurité, nous discutons de la question et convenons tous que la menace est importante et que le secteur est très vulnérable, mais ce n'est pas la façon dont le grand public voit les choses. Les gens n'ont aucune inquiétude relativement à ce secteur. Des mesures de sensibilisation sont requises, non pas pour faire peur aux gens, mais pour leur faire prendre conscience des risques importants à ce chapitre. C'est un secteur réglementé qui ne va pas sans certains risques.

Le sénateur Mitchell : Il y a quelques années, nous avons mené au Comité de l'énergie une étude sur la sécurité du transport des hydrocarbures, notamment via le pipeline. Nous avons alors rencontré Mark Fleming de l'Université Saint Mary's qui accorde beaucoup d'importance à la culture de la sûreté. Monsieur Graham, une grande partie de votre argumentation s'articule autour de cette notion de culture, et vous avez parlé de culture de la sécurité.

M. Graham : Tout à fait.

Le sénateur Mitchell : Peut-être davantage pour vous inciter à réfléchir à la question que dans l'espoir d'obtenir une réponse, je vous signale que M. Fleming nous avait alors bien fait comprendre que notre perception de la culture de la sûreté était quelque peu faussée. Il ne s'agit pas simplement de compter les erreurs et les accidents évités. Et la notion de culture de la sécurité est encore plus complexe. Il nous a fallu des années pour parvenir à la situation actuelle en matière de culture de la sûreté, si tant est que nous y soyons vraiment parvenus.

M. Graham : Tant la culture de la sûreté que celle de la sécurité s'appuient notamment sur la volonté de s'attaquer aux vrais problèmes. Je dirais que l'industrie nucléaire à laquelle le sénateur White a fait référence se tire très bien d'affaire pour ce qui est tout d'abord de détecter les véritables problèmes, plutôt que les situations que l'on prétend problématiques ou qui pourraient éventuellement le devenir. Vous avez parlé des accidents évités de justesse, mais cette culture vise entre autres à encourager les gens à trouver des façons de détecter les failles sans que l'on cherche spontanément à blâmer qui que ce soit. L'implantation d'une culture semblable est très avancée dans le secteur nucléaire, et nous aurions beaucoup à apprendre de ce côté-là.

Il est vraiment consternant de voir comment les choses peuvent se passer par ailleurs. Nous avons un système de pipeline sur roues que l'on appelle le train. Est-ce que la culture de la sûreté est aussi bien ancrée dans ce secteur? Je ne sais pas quelle est la

Mr. Quigley: If I may add to that point, first, Andy's earlier reference to the risk officer could be a bureaucratization of security rather than a genuine engagement with safety culture. If you put somebody in charge, and if there is a template and a form to check off, that's an organizational culture of bureaucracy responding the way bureaucracies do. Put someone in charge and give them the forms, but that's not generally engaging in safety and security.

What I found in my research is regulatory simplicity, if I can say such a thing can exist in critical infrastructure. What I mean by that is that with telecoms, for instance, where you've got one government that largely regulates the sector, that makes it a lot easier. However, when you get into the messy business of the federal, provincial and municipal all having a stake in one sector, there is an overlap, and it becomes a lot harder to get a national standard. Telecoms make more progress; also, areas where the U.S. makes progress, Canada tends to make progress, for instance, in aviation. We found that regulatory simplicity, where customers thought the risk was real and where the owners and operators had a financial interest in it, for example with airports, you tended to get more progress. But where there was more complex federal and provincial interaction on the issue, where people didn't think the threat was real, customers didn't believe it. Seaports, for instance, are out of sight and out of mind, so no one deals with the threats at seaports regularly, whereas at airports you see it and feel it. There is a genuine emotional engagement from the customers, and they accept it because of the searing images of 9/11. But the seaports are off to the side.

The Chair: I have a general question here on your research. Perhaps you can tell us what is Canada's definition of "critical infrastructure," and have we also identified, as a government, the question of the key assets so that we understand what we have identified to be able to take the necessary steps to protect it? Have we got a list?

Mr. Quigley: The U.S. always had a short, sharp definition which I didn't think was too bad. I don't know if Canada picked up the same one. It was the cyber and physical assets upon which our society depends. Something like that.

The problem is that "critical," "infrastructure" and "protection" — each of those words — are totally explosive. What is critical? Who is on the list, and who is off the list?

réponse, et j'ignore si nous avons recueilli les données nécessaires ou effectué les études suffisantes pour vraiment le savoir. Il faudrait pourtant que ce soit le cas.

M. Quigley : J'ajouterais que la création du poste d'agent de gestion des risques dont Andy parlait tout à l'heure pourrait correspondre davantage à une bureaucratisation de la sécurité qu'à un véritable engagement envers une culture de la sûreté. Si vous désignez un responsable qui doit suivre un gabarit et cocher un formulaire, vous obtenez une culture organisationnelle de la bureaucratie qui va dans le sens de ce que les bureaucrates font habituellement. Ce n'est pas la manière dont se manifeste généralement un engagement en faveur de la sécurité.

Mes travaux m'ont permis de constater qu'il peut y avoir simplification de la réglementation, dans la mesure où cela est chose possible, dans le contexte des infrastructures essentielles. Je veux dire par là que s'il est possible de faire en sorte qu'un seul gouvernement réglemente la plus grande partie d'un secteur, comme celui des télécommunications, cela facilite grandement les choses. Par contre, lorsqu'il y a enchevêtrement chaotique entre les responsabilités fédérales, provinciales et municipales, il y a chevauchement entre ces différentes instances et il devient beaucoup plus difficile d'obtenir une norme nationale. On note des progrès plus marqués dans le secteur des télécommunications de même que dans ceux, comme l'aviation, où les progrès canadiens suivent ceux réalisés aux États-Unis. Nous avons constaté que le progrès est généralement plus senti dans les secteurs où la réglementation a été simplifiée, quand les consommateurs estiment que la menace est réelle et lorsque les propriétaires et exploitants ont un avantage financier à agir. Les choses sont beaucoup moins faciles lorsqu'il y a davantage d'interactions complexes entre le gouvernement fédéral et une province et lorsque les gens ne croient pas que la menace est réelle. À titre d'exemple, personne ne pense aux ports de mer, si bien que l'on ne se penche pas régulièrement sur les risques auxquels ils sont exposés, alors que la menace est directement ressentie dans les aéroports dont les utilisateurs sont véritablement engagés du point de vue émotif. Les gens acceptent les mesures qui leur sont imposées parce qu'ils ont encore à l'esprit les images percutantes du 11 septembre, alors que la situation des ports passe totalement inaperçue.

Le président : J'ai une question d'ordre général concernant vos recherches. Peut-être pourriez-vous nous dire comment sont définies au Canada les « infrastructures essentielles » et nous indiquer si le gouvernement a déterminé quels étaient les actifs clés exigeant des mesures de protection particulières. Avons-nous établi une liste de ces actifs?

M. Quigley : Les Américains utilisent depuis toujours une définition brève et précise que je trouve assez bonne. Je ne sais pas si le Canada s'en est inspiré. Je pense que c'est quelque chose comme les actifs cybernétiques et physiques dont la société dépend.

Il devient difficile de trancher du fait que la définition de chacun des termes « protection », « infrastructures » et « critiques » ouvre la voie à de nombreuses questions. Qu'est-ce

Because if you're not critical, that means you're not critical. That might even have funding implications for you if you're not critical.

The Chair: That's not always a bad thing.

Mr. Quigley: No, it's not maybe from our perspective, but sometimes you want to be on the critical infrastructure list if you —

The Chair: You don't just want to be there to get financed.

Mr. Quigley: Who wants to say you're working on something that's not critical?

The Chair: Somebody has to make a determination, don't they?

Mr. Quigley: That's right. What I heard from government departments at the provincial level is their anxieties over determining what's critical, because once you label it critical, then you will have to protect it, and you will have to take on responsibilities, and there might be liabilities associated with that. That's why there is anxiety about committing that pen to paper and saying what is critical around here.

The interdependence issue is highly complex. One small failure — we talked about the trees knocking down the power grid — where does it end? It is a highly interdependent and fragile system. My colleague mentioned earlier about which parking lots become critical when she was talking about the hospitals. Where does that discussion end? I think if you start identifying that, then you have a long inventory that is probably changing every day anyway. That is another risk: having an out-of-date list. That is, doing the list one year, and then the next year it has changed and then you have an out-of-date list.

I know with computer modellers they tried to have some complex, interdependent modelling. It is a huge undertaking, and it can pass its shelf life quickly because the systems are always changing. It's a tough one.

Senator White: Professor Quigley, you raised the seaport issue. In northern Australia there is an issue around a Chinese company — owned by China, obviously — that is trying to purchase a seaport in Darwin, I think it is. In Canada, I'm not sure that we would actually raise the same concerns if they were looking at purchasing the port at Sydney in Cape Breton, although it is a deep seaport. I know a Chinese company is actively looking at it. Do you think we need to do more around that issue and the issue from a perspective of the infrastructure of our national security — not so much natural disasters or terrorism but an infrastructure and national security perspective?

qui est essentiel? Qu'est-ce qui doit figurer sur la liste et qu'est-ce qui ne doit pas s'y trouver? Si un bien n'est pas considéré essentiel, il faut en tirer certaines conclusions qui peuvent même avoir des incidences du point de vue financier.

Le président : Ce n'est pas toujours une mauvaise chose.

M. Quigley : Non, peut-être pas de notre point de vue, mais il arrive que l'on souhaite se retrouver sur la liste des infrastructures essentielles si...

Le président : Vous ne voulez pas y figurer simplement pour obtenir du financement.

M. Quigley : Qui veut se faire dire que son travail n'est pas essentiel?

Le président : Quelqu'un doit trancher, n'est-ce pas?

M. Quigley : Tout à fait. Des gestionnaires de ministères provinciaux m'ont fait part de leurs appréhensions lorsqu'il s'agit de déterminer ce qui est essentiel ou non, car tout ce qui est désigné essentiel exige des mesures de protection et s'accompagne de responsabilités, notamment du point de vue financier. Ils hésitent donc à désigner officiellement leurs infrastructures essentielles.

La question de l'interdépendance est extrêmement complexe. Tout peut débuter avec une panne sectorielle — nous avons parlé de ces installations électriques abattues par des arbres — mais où est-ce que cela se termine? C'est un système fragile et totalement interdépendant. Ma collègue en a traité tout à l'heure en parlant des stationnements qui peuvent devenir des infrastructures essentielles dans le cas des hôpitaux. Mais jusqu'où pouvons-nous aller en ce sens? J'ai l'impression que si l'on commence à désigner de tels actifs, on va se retrouver avec un long inventaire qui va probablement changer d'une journée à l'autre de toute manière. C'est d'ailleurs un autre risque. La liste peut devenir désuète. Vous dressez une liste et l'année suivante la situation a changé de telle sorte que votre liste n'est plus valable.

Je sais que l'on s'efforce d'en arriver à des modèles complexes et interdépendants grâce à la modélisation mathématique. C'est une initiative d'envergure dont les résultats pourraient devenir rapidement obsolètes, car les systèmes évoluent sans cesse. C'est un des aspects problématiques.

Le sénateur White : Monsieur Quigley, vous avez parlé des ports de mer. Dans le nord de l'Australie, un problème se pose du fait qu'une entreprise chinoise tente d'acheter un port de mer à Darwin, si je me rappelle bien. Je ne suis pas certain que l'on soulèverait autant de préoccupations au Canada en envisageant l'achat du port de Sydney, au Cap-Breton, bien qu'il s'agisse d'un port en eau profonde. Je sais d'ailleurs qu'une entreprise chinoise s'y intéresse de près. Croyez-vous que nous devrions être plus vigilants dans ce dossier, non pas dans la perspective des risques de catastrophe naturelle ou de terrorisme, mais du point de vue d'une infrastructure nécessaire à notre sécurité nationale?

Mr. Quigley: You asked the question about foreign ownership. I've observed it, like others, in the media. I know the Americans have a lot of issues about who should own critical assets. I have written on this subject and can make the paper about seaport security available to the committee.

This is a pretty stressed-out group of people working in seaport security. When I made my own opening statement about markets, this is a group that really finds itself betwixt and between. Are they in market service, trying to get things to market as quickly possible? Or are they about security? We have done a lot of work on seaport security, and they are feeling more and more in the direction of markets and about efficiency, and they are concerned they wouldn't have the support to stop to do the checks they need to do. They don't necessarily feel like they have the support of the security apparatus in the country as well because they feel like they are a quasi-independent organization. Are they government? Are they not? It's a stressed-out group of seaport people.

Senator White: If you don't mind sending that paper, I would appreciate it.

Mr. Quigley: I don't mind at all.

The Chair: We're coming to the end of our time. I'd like very much to thank our witnesses for taking time and sharing their knowledge and experience with us. I'm sure we'll have you here another time in the future. Once again, thank you.

(The committee adjourned.)

M. Quigley : Vous soulevez la question de la propriété étrangère. J'ai suivi le dossier dans les médias. Je sais que les Américains ont de nombreuses réserves quant à la propriété des infrastructures essentielles. J'ai rédigé à ce sujet un document sur la sécurité portuaire que je pourrais transmettre au comité.

Les gens qui travaillent à la sécurité des ports de mer sont passablement nerveux. Ils se retrouvent déchirés entre deux orientations pour ce qui est des considérations liées aux marchés dont j'ai parlé dans ma déclaration préliminaire. Sont-ils là pour desservir les marchés de telle sorte que les produits puissent rejoindre le plus rapidement possible leur marché cible? Ou leur rôle en est-il un de sécurité? Nous avons fait un important travail d'analyse relativement à la sécurité portuaire, et je peux vous assurer que ces gens-là s'intéressent de plus en plus à l'accès aux marchés et à l'efficience. Ils craignent de ne pas obtenir le soutien nécessaire pour pouvoir renoncer aux mesures de contrôle qu'ils sont censés prendre. Ils n'ont pas toujours l'impression d'avoir l'appui de l'appareil de sécurité de notre pays. Il y a aussi le fait qu'ils se voient comme une organisation quasi indépendante. S'agit-il ou non d'une instance gouvernementale? Les responsables de la sécurité des ports sont plutôt inquiets.

Le sénateur White : Si vous voulez bien nous faire parvenir ce document, je vous en serais reconnaissant.

M. Quigley : Avec grand plaisir.

Le président : C'est tout le temps que nous avions pour aujourd'hui. Je tiens à remercier nos témoins pour le temps qu'ils nous ont consacré et les trésors de connaissances et d'expérience dont ils nous ont fait profiter. Je suis persuadé que nous aurons le plaisir de vous accueillir de nouveau. Merci encore.

(La séance est levée.)

Monday, March 21, 2016

Canada Border Services Agency:

Martin Bolduc, Vice President, Programs Branch;

Caroline Xavier, Vice President, Operations Branch.

Communications Security Establishment Canada:

Greta Bossenmaier, Chief.

As individuals:

Stephanie Carvin, Assistant Professor, International Relations, Norman Paterson School of International Affairs;

Adam Chapnick, Professor and Deputy Director, Education, Canadian Forces College, Department of National Defence;

Kevin Quigley, Associate Professor and Director, MacEachen Institute for Public Policy and Governance;

Andrew Graham, Adjunct Professor, School of Policy Studies, Queen's University.

Le lundi 21 mars 2016

Agence des services frontaliers du Canada :

Martin Bolduc, vice-président, Direction générale des programmes;

Caroline Xavier, vice-présidente, Direction générale des opérations.

Centre de la sécurité des télécommunications Canada :

Greta Bossenmaier, chef.

À titre personnel :

Stephanie Carvin, professeure adjointe, Relations internationales, Norman Paterson School of International Affairs;

Adam Chapnick, professeur et directeur adjoint, Éducation, Collège des Forces canadiennes, ministère de la Défense nationale;

Kevin Quigley, professeur agrégé et directeur, MacEachen Institute for Public Policy and Governance;

Andrew Graham, professeur auxiliaire, École des études sur les politiques publiques, Université Queen's.

WITNESSES

Monday, February 22, 2016

Reserves 2000:

Lieutenant-Colonel (Retired) John Selkirk, Executive Director.

Security Intelligence Review Committee:

The Honourable Pierre Blais, Chair;

Michael Doucet, Executive Director.

Office of the Communications Security Establishment Commissioner:

The Honourable Jean-Pierre Plouffe, Commissioner;

J. William Galbraith, Executive Director.

Office of the Auditor General of Canada:

Nancy Cheng, Assistant Auditor General;

Gordon Stock, Principal;

Nicholas Swales, Principal.

Monday, March 7, 2016

Canadian Security Intelligence Service:

Michel Coulombe, Director.

National Defence and the Canadian Armed Forces:

General Jonathan Vance, Chief of the Defence Staff.

Canada Revenue Agency:

Cathy Hawara, Director General, Charities Directorate, Legislative Policy and Regulatory Affairs Branch;

Alastair Bland, Director, Review and Analysis Division, Charities Directorate, Legislative Policy and Regulatory Affairs Branch.

Public Safety Canada:

Monik Beauregard, Senior Assistant Deputy Minister, National and Cybersecurity Branch;

Patrick Boucher, Acting Director General, Critical Infrastructure and Strategic Coordination Directorate;

Suki Wong, Director General, National Security Operations Directorate;

Colleen Merchant, Director General, National Cyber Security Directorate.

(*Continued on previous page.*)

TÉMOINS

Le lundi 22 février 2016

Réserves 2000 :

Lieutenant-colonel à la retraite John Selkirk, directeur exécutif.

Comité de surveillance des activités de renseignement de sécurité :

L'honorable Pierre Blais, président;

Michael Doucet, directeur exécutif.

Bureau du commissaire du Centre de la sécurité des télécommunications :

L'honorable Jean-Pierre Plouffe, commissaire;

J. William Galbraith, directeur exécutif.

Bureau du vérificateur général du Canada :

Nancy Cheng, vérificatrice générale adjointe;

Gordon Stock, directeur principal;

Nicholas Swales, directeur principal.

Le lundi 7 mars 2016

Service canadien du renseignement de sécurité :

Michel Coulombe, directeur.

Défense nationale et les Forces armées canadiennes :

Général Jonathan Vance, chef d'état-major de la Défense.

Agence du revenu du Canada :

Cathy Hawara, directrice générale, Direction des organismes de bienfaisance, Direction générale de la politique législative et des affaires réglementaires;

Alastair Bland, directeur, Division de l'examen et de l'analyse, Direction des organismes de bienfaisance, Direction générale de la politique législative et des affaires réglementaires.

Sécurité publique Canada :

Monik Beauregard, sous-ministre adjointe principale, Secteur de la sécurité et de la cybersécurité nationale;

Patrick Boucher, directeur général par intérim, Direction générale des infrastructures essentielles et de la coordination stratégique;

Suki Wong, directrice générale, Direction générale des opérations de la sécurité nationale;

Colleen Merchant, directrice générale, Direction générale de la cybersécurité nationale.

(*Suite à la page précédente.*)

Available on the Internet: http://www.parl.gc.ca

Disponible sur internet: http://www.parl.gc.ca

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT.
REVISE PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS A L'INFORMATION

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 006 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, March 8, 2016

Chair

Mr. Robert Oliphant

Standing Committee on Public Safety and National Security

Tuesday, March 8, 2016

● (1105)

[*English*]

The Chair (Mr. Robert Oliphant (Don Valley West, Lib.)): I'm going to call this meeting of the Standing Committee on Public Safety and National Security to order.

I thank our witnesses and guests for coming today. This meeting is to consider the supplementary estimates (C) for the year 2015-16. As a reminder, the meeting is televised.

We're very pleased to have the Honourable Ralph Goodale, Minister of Public Safety and Emergency Preparedness with us, as well as many senior officials. It is a great honour for us to see you once again.

We're going to have two rounds of questioning. I want to leave about five minutes at the end of the meeting for the vote on the supplementary estimates, which I understand should happen fairly easily. That is my hope.

We are going to begin with a 10-minute presentation from the minister. Thank you for being with us.

Hon. Ralph Goodale (Minister of Public Safety and Emergency Preparedness): Mr. Chair, thank you very much. I offer my sincere apologies to you and members of the committee. I was stranded in another meeting that ran a few minutes over time and I apologize for not being here exactly on time.

It is a pleasure to appear before this committee for the first time as Minister of Public Safety and Emergency Preparedness, and specifically to discuss the estimates.

I want to say that with respect to the estimates process, as members who study old speeches from the House of Commons will know, I very much support the efforts that Minister Brison at Treasury Board is leading to try to improve the ability of parliamentarians both to have effective oversight with respect to the spending plans of the government and to connect the budget process to the estimates process and the public accounts process, so that everyone can follow the money and make intelligent decisions about controlling the public purse. I hope that over the course of this Parliament we will be able to make substantial progress towards greater transparency with respect to government spending.

Today, I am joined by a number of familiar faces. I will introduce my deputy minister, François Guimont, who heads the public service within Public Safety Canada. I would ask François to introduce the other officials at the table, many of whom I know this committee already knows.

Mr. François Guimont (Deputy Minister, Department of Public Safety and Emergency Preparedness):

Thank you, Minister. Good morning to all of you. I present Don Head, whom most of you probably know from Correctional Service Canada; Nada Semaan, executive vice-president with the Canada Border Services Agency; Commissioner Paulson, with us this morning as well, from the RCMP; Michel Coulombe, director of Canadian Security Intelligence Service, CSIS; and Mr. Harvey Cenaiko who is the chairperson of the Parole Board of Canada.

● (1110)

Hon. Ralph Goodale: Thank you, François.

As committee members already know from your previous encounters with officials and heads of the various agencies within the public safety portfolio, this mandate in this portfolio is both large and complex. It encompasses a vast array of responsibilities: national security, emergency management, law enforcement, corrections, crime prevention, and border security.

I am continually impressed by the work that is being done by the dedicated public servants who make up this portfolio in fulfilling the basic mandate that we have from the Prime Minister. It's a mandate that is inherent in this portfolio: keep Canadians safe, and do so in a way that respects their rights, their freedoms, and the values of this country.

No matter how assiduous public servants are, there is always more work to do.

At the outset today, I'd like to address two or three of the top-of-mind issues that we're working on, issues that Canadians are concerned about and on which they are expecting leadership and progress.

First, as members will know, we have moved ahead with real purpose and intent on the issue of post-traumatic stress injuries, or what people now refer to as operational stress injuries. They are disproportionately high among first responders due to the nature of the jobs that first responders are asked to do.

Every day police officers, firefighters, border officers, and others in high-stress situations are risking their lives for the safety of other Canadians. At the end of the day, very often they do not have access to the resources and the support systems they need to help them cope with the trauma they experience in their jobs.

We held an excellent national round table on PTSD, or OSI, in Regina, back in January. It was a first step toward an inclusive national conversation about how we can better support front-line responders.

I understand this committee is going to be studying this important issue, and I will certainly follow your deliberations on that topic with a great deal of care.

Another topic of urgency is the whole question of workplace harassment in the national police force. That was referred to explicitly in my mandate letter from the Prime Minister. We want healthy workplaces that are free from harassment and sexual violence.

RCMP members perform an absolutely critical role in our communities. Canadians expect a high standard from them in terms of professional and exemplary behaviour. I am committed to taking whatever action is necessary to help RCMP members, trainees, and employees feel safe and respected among their colleagues and superiors. I know the commissioner has been hard at work on that challenge over the last period of time as well.

In that regard, I wrote to the chair of the Civilian Review and Complaints Commission for the RCMP on February 4 this year to ask him to undertake a comprehensive assessment of RCMP policies and procedures in the workplace about harassment, and to evaluate the implementation in the force of the recommendations that the commission made back in 2013.

I note as well that RCMP Commissioner Paulson has asked Paul Kennedy, a former chair of the commission for public complaints against the RCMP, to act as an independent observer and monitor on the investigation that's currently under way with respect to certain allegations of misconduct at the police college. This is a topic that has been of concern to Canadians, and we need to ensure that we're responding on all fronts.

Finally, I want to mention the greatest challenge to our national security as another topic of important concern to me, and I'm sure to members of the committee, and that is the twofold threat of terrorism and radicalization to violence.

As committee members know, we are undertaking broad consultations about Canada's national security framework with stakeholders that include parliamentarians, subject matter experts, the general public, and our foreign partners.

I welcome and actively seek the input of members of all parties to contribute to this review process. Indeed, a number of MPs and a number of senators have already come forward to make offers.

● (1115)

Mr. Chair, I would welcome the advice of this committee about how this committee would want to participate in the consultative process, both hearing from other members of Parliament, but also hearing from the general public about our national security framework.

Among our top priorities is the establishment of a designated Canadian office on community outreach and counter-radicalization coordination. The goal is to find, promote, and share the best ways with communities to prevent and combat radicalization and to build resilient communities and resilient individuals.

The Aga Khan, a very respected citizen of the world, a global activist for peace, and a great friend of Canada, has described our country as the finest expression of pluralism the world has ever seen. If we wish to continue that success, we need to work very hard to share, instill, celebrate, and practise our precious Canadian values of openness, diversity, inclusion, respect, and accommodation, and I hope our new office of community outreach will contribute to that effort.

I'm also working, as you know, with the Leader of the Government in the House of Commons to create a statutory committee of parliamentarians that will help scrutinize government departments and agencies that exercise national security responsibilities. That was a fundamental election promise that we made. Canada is an anomaly at the present time in not having a parliamentary review mechanism with respect to security and intelligence operations. All of our major allies, including those in the Five Eyes—the U.S., the U.K., New Zealand, and Australia—have such a parliamentary vehicle. We intend to fill the gap in Canada and provide that kind of review mechanism in Canada, too.

In the process we will also review what other kinds of vehicles and mechanisms we need in order to properly overview and scrutinize the activities of our security and intelligence operations. Other countries typically have a number of different vehicles including a parliamentary one. We at present don't have that parliamentary one and we will fill that gap.

The objectives are twofold here. Number one is to make sure that our security and police operations are effective in keeping Canadians safe. Number two is to make sure that in the process of doing so they are safeguarding the values, the rights, the freedoms, and the fundamental character of our country.

Mr. Chair, specifically about estimates and supplementary estimates (C), as you will see for the portfolio overall, the total authorities that we are seeking will result in a net increase of $176 million, which is relatively modest from a government pan-Canadian point of view. It represents a 1.98% increase over the total authorities to date.

The largest request, probably not a surprise to the committee, is with respect to the RCMP. Commissioner Paulson in the past has been very candid with the committee indicating where the financial pressures, stresses, and strains are, and he's had to make some internal reallocations from other areas to national security, which has been difficult for the force to accommodate. We can't deal with all of that pressure in this one set of estimates, but we are beginning the process of trying to make sure that on a go-forward basis the A-base contribution to the RCMP is sufficient for the work that Canadians expect the RCMP to do. You can't give them a mandate and demand they perform miracles and then not provide the resources necessary to get the job done. The increase for the RCMP is $110 million, most of which is going to the contract policing side of the equation. There's also funding here for counterterrorism work and the fight against cybercrime.

With respect to the CBSA, there's an increase of $59.2 million, largely related to its mandate for securing the borders. It's the integrity of its front-line operations, the critical work that it has performed in respect to the Syrian refugees, and improving its capacity with respect to biometrics.

For the Correctional Service of Canada, the request is a total of $4 million, the majority of which goes to fulfilling the requirements of the Canadian Victims Bill of Rights. The same is true with respect to the Parole Board of Canada, a request of $300,000 in order to implement measures in relation to the Canadian Victims Bill of Rights.

● (1120)

With respect to CSIS, you will find a number of transactions in the estimates with money moving back and forth, all intended to increase its capacity with respect to software and its work with Global Affairs Canada, which is taking on increasing importance.

I have one final specific point on the $2.6 million for Public Safety Canada itself. That is largely to recognize the additional responsibilities the department is taking on for the national search and rescue secretariat. That used to be vested in the Department of National Defence, and it will now be vested in the Department of Public Safety.

That's a quick overview, Mr. Chair.

I want to close by thanking all the dedicated public servants who toil in this department and in this portfolio in very critical jobs that relate to the safety of their fellow citizens. They do a remarkable job, subject to the human frailties that we all experience, but they are a terrific group of public servants who work very hard for their fellow citizens.

I also want to say, Mr. Chair, thank you and a farewell to my deputy minister, François Guimont. He will retire from the public service at the end of this month after a remarkable career in the service of Canada in Public Safety, Public Works, Environment Canada, PCO, and elsewhere. François, I wish you well in your retirement, and I extend the gratitude of the Government of Canada for your lifetime of accomplishment in the service of Canadians. Thank you, sir.

Mr. François Guimont: Thank you, Minister.

The Chair: We begin our questioning with Mr. Di Iorio.

[*Translation*]

Mr. Nicola Di Iorio (Saint-Léonard—Saint-Michel, Lib.): Thank you, Mr. Chair. Good morning, Mr. Minister.

Minister, the world has known different epochs, and Canada has had its share of terrorist threats in its history. However, there is one that is weighing on us currently, and it concerns the threat posed by the radicalization of foreign combatants. We are meeting in a splendid room, Minister, but this room has also been the setting for some tragic moments in the history of this Parliament and of this country.

Could you explain to us how you intend to deal with that threat?

[*English*]

Hon. Ralph Goodale: There are two ways to address it. The challenge is large and significant, and it's a challenge that's shared worldwide.

Many other countries face much bigger problems than we do, but the tragic events of October 2014 demonstrate that Canada is not immune, and we need to treat this with the full seriousness it deserves, in partnership with our colleagues and allies around the world.

Among the activities aimed at dealing with violent extremism and radicalization, the front-line efforts to combat the immediate consequences are directed by the RCMP and by CSIS and by the Canada Border Services Agency. They work with National Defence. They work with PCO. In fact, there are 17 departments or agencies of the Government of Canada that discharge national security functions and obligations.

Those people are on the job doing an amazing job for Canada constantly all the time. They are absorbing all the necessary information. They are taking the appropriate actions to deal with that information. They constantly assess and reassess the threat level that's applicable to Canada.

I would pause here to say that, while this is constantly under review and nothing is ever taken for granted, the threat level that exists today is the same as it was in October 2014, which is assessed at medium. There has been no cause for Canada to adjust the threat level since October 2014, and that remains the case today.

In terms of being more proactive about the future, we are focusing, as you know, on the creation of this new office of community outreach and counter-radicalization coordination. This is to find the very best Canadian ways to reach out to communities, to understand their vulnerabilities, and to identify the best means to intervene before a tragedy occurs.

We have some good research through the Kanishka project, which the previous government initiated. It has given us some useful and helpful insights into the process of radicalization. Some provinces, for example, the Province of Quebec has been very proactive in developing its own counter-radicalization strategy. Cities and police forces such as those in Montreal, Edmonton, Calgary, Toronto, and others have developed their own outreach initiatives. The RCMP has an outreach program. So does the Department of Public Safety.

What we want to do is pull all of this together in a coordinated national office for outreach and for counter-radicalization, with best practices, to make sure we are doing everything we can to build resilient individuals and resilient communities while avoiding the lure of radical and violent propaganda. We're going to do our very best to make the values of Canadians something for everyone in this country, those who have been here a long time and the newcomers, to celebrate.

● (1125)

[*Translation*]

Mr. Nicola Di Iorio: Thank you, Minister.

You just spoke of the threat due to human actions, ill-intentioned actions directed against Canada and its citizens. However, there are also unfortunate events that occur because of natural disasters.

The Parliamentary Budget Officer recently announced that the costs related to natural disasters was increasing. Could you share with us the reasons behind that?

[*English*]

Hon. Ralph Goodale: There are many reasons for it, but one obvious one is the impact of a destabilized climate and the greater risk of natural disasters because of more frequent, more violent, and more consequential weather events, the floods, droughts, and the other types of problems that have befallen Canadians, and cost municipalities, the private sector, and individual Canadians literally tens of millions and billions of dollars. I think of the flood in southern Alberta a few years ago. In southern Saskatchewan and southern Manitoba, in two out of the last five years, there have been major floods. There was the flooding in Quebec three years ago, I believe.

The parliamentary budget officer has added up the consequences of all of this and taking predictable factors into account, the officer has tried to project what we can expect in terms of cost. He is saying that typically what we budgeted in the past will simply not be adequate to deal with the consequences in the future. There are two things about that. No doubt in future estimates we will need to make more cautious preparations for what the real dollar costs are going to be, but we also need to invest in prevention. There you will see something from our campaign platform that I think is very encouraging. In the streams of infrastructure investment that we intend to make in the future, there is specific reference to building resilience against the consequences of climate change. How do we better prepare for floods? How do we better manage those unpredictable water flows? What kind of infrastructure can we invest in that will make us better able to handle the disasters when they occur and avoid the downstream costs as much as possible?

The Chair: Thank you, Mr. Minister.

We'll go to Mr. O'Toole.

Hon. Erin O'Toole (Durham, CPC): Thank you very much, Mr. Chair.

Welcome, Minister, thank you for attending and thank you to your deputy for his service. It's appreciated. I'd also like to thank your department.

We were very happy to see the conclusion of the Syrian refugee program on the modified timeline, and I know a lot of effort went into that. Many of my questions will relate to that, Minister. Under your portfolio which departments were involved in the Syrian refugee response?

Hon. Ralph Goodale: The primary front-line department, Mr. O'Toole, was obviously CBSA, but a great deal of expertise and effort was also devoted by the RCMP and by CSIS. The RCMP and CSIS in particular were helpful to Immigration, Refugees and Citizenship Canada in devising the screening process.

● (1130)

Hon. Erin O'Toole: Your own department, Public Safety and Emergency Preparedness, obviously would have had some involvement as well.

Hon. Ralph Goodale: Oh, yes, absolutely.

Hon. Erin O'Toole: Okay.

I liked your remarks at the beginning about studying old speeches and following the money. That's what I intend to do with my time today.

On December 9, in committee of the whole on Bill C-3, which was supplementary estimates (B), Minister McCallum said the overall cost of the Syrian refugee program, which was the need for Bill C-3 in the supplementary estimates, was $700 million. He told the House that day that $500 million of that was the total spending for Immigration, his department. Minister Brison said that other departments.... They did not allocate where the other $200 million would be spent, but Minister Brison said that most other departments involved would cash manage their involvement in the Syrian program. Is that what your departments did, they cash managed it?

Hon. Ralph Goodale: Let me ask Nada to comment specifically from the point of view of CBSA. I would note that I did mention an amount earlier of $13.6 million for the critical role the agency played in those efforts. That's part of these estimates now. But Nada can provide more detail.

Ms. Nada Semaan (Executive Vice-President, Canada Border Services Agency): Absolutely. This money will be received, once approved. However, as you know, we worked on it quite a bit before, so there was a bit of cash management in anticipating receiving the funds through supplementary estimates (B).

Hon. Erin O'Toole: So the $13.6 million, Minister, that you mentioned for CBSA, of the four departments you mention that's the only department that will be receiving additional allocation. CSIS, RCMP, and Public Safety, none of them require it?

Hon. Ralph Goodale: That's correct.

Hon. Erin O'Toole: Do we have a breakdown on how the cash management may have affected other priorities or operations of the government?

Mr. François Guimont: At least in the case of Public Safety, and I'll let my colleagues speak to their specific portfolio responsibilities, we manage that as a priority within our ongoing programs. We did not specifically earmark an individual or a team. This was part of our ongoing activities and we just absorbed it. Very often, frankly, we do that when emerging priorities do come up.

Hon. Ralph Goodale: Could I ask Commissioner Paulson or Mr. Coulombe if they have anything to add?

Commr Bob Paulson (Commissioner, Royal Canadian Mounted Police): I would just say in a similar fashion that the total cost to our organization was minimal and it was manageable within our existing reference levels.

Hon. Erin O'Toole: Specifically, Minister, the government operations centre, which I understand was the hub of the entire operation, has not received additional funds in supplementary estimates (B) or (C), so did it cash manage the entire additional work?

Hon. Ralph Goodale: It did, and that's the nature of its function, to be able to respond to emerging situations quickly.

Mr. O'Toole, you do raise a point about the future capacity of the government operations centre, and I think that's something we will have to look at very carefully. This is a very important nerve centre within the Government of Canada when something goes wrong somewhere in the country. This is a place where all of the participants—not just federal departments, but provinces, municipalities, NGOs, and members of the private sector—can come together. We're dealing with a national crisis, and we're all in the same room, and we can make sure—

Hon. Erin O'Toole: Absolutely, Minister, and that's why I'm asking. In the 2015-16 plans and priorities for your department, one of the risks identified was, and I quote, "That the...GOC...may be unable to support a coordinated response to a large-scale...event." That was identified by the department before the Syrian refugee program, but you're saying they needed no additional resources and were able to coordinate this?

Hon. Ralph Goodale: That's correct, but let me ask the deputy minister to comment.

Mr. François Guimont: When that risk was identified, we wanted to differentiate between the individuals within the capacity of the team and the actual building. The building does have limitations, if you will, which is something that I have discussed with the minister. We are taking steps to address that building issue, because the capacity of the GOC to coordinate in response to a major issue is a function of the team, but also of the location, the structure of the building, and its capacity. That risk is tied more to that component than to what I would refer to as human resources, their training and their capacity to work together and deliver a coordinated response.

● (1135)

Hon. Erin O'Toole: Would we be able to get a breakdown by department of how much spending was required and how that cash management affected additional operations?

Hon. Ralph Goodale: Do you mean in relation to the overall Syrian refugee initiative?

Hon. Erin O'Toole: Yes, because the supplementary estimates (B) did not have details apart from CIC's commitment to the program. I think even our new members of the family, our new permanent residents want to make sure that we spend and allocate accordingly. There's been a lot of concern that certain programs like the private sponsorship route for refugees and a number of other programs have been shelved to accommodate the timeline set during the election. Cash management is a broad term. I'd like to see how much it affected the budgets of your departments and what priorities were shifted to accommodate that.

Hon. Ralph Goodale: Mr. O'Toole, I will undertake to raise that with Mr. McCallum and my other cabinet colleagues to see if we can present to MPs and to Canadians publicly a final report on the Syrian initiative so that people can have all the facts and figures on how it went.

Hon. Erin O'Toole: Because in fairness, $13.6 million is all we're seeing, and I'm sure it was more than that.

Hon. Ralph Goodale: Let me see if we can put it together. I agree with your point.

The Chair: Thank you.

Monsieur Dubé.

[*Translation*]

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Mr. Chair.

I thank the minister and our other guests for being here with us today. Mr. Guimont, as my colleagues have also done, I want to take this opportunity to thank you for your services.

My question is on Bill C-51.

The following issue is still of great concern to the NDP—especially after listening to Mr. Coulombe yesterday, and also in thinking about his testimony before our committee a few weeks ago. I am referring to the fact that the powers are currently being used, even though the oversight mechanisms that are considered essential to ensure that those powers are well used have still not been put in place. The NDP is still of the opinion that this act should be repealed.

My question is about the role opposition parties should play in this regard. Minister, you have had some fine words to say on this, but the fact remains that Mr. McGuinty was appointed without any consultation of the opposition parties. You went to London. Yes, there were conferences, but you also wanted to review the best practices of the United Kingdom committee which is the counterpart of the one you want to set up. Once again, no members of the opposition were invited.

Following the letter Mr. Mulcair sent to the Prime Minister, will opposition members and parties finally really be formally included in this process?

Could you also provide us with an update on the process? Where do things stand? There is some urgency now. The powers are being used and the oversight is not adequate.

[*English*]

Hon. Ralph Goodale: I fully appreciate your point, Monsieur Dubé. I want to give you the absolute reassurance from me as the responsible minister but also on behalf of the government that this is very much intended to be a process in which parliamentarians will play an exceedingly important role in two ways.

First of all, it's by participating in the consultation about what needs to be done in specific legislative terms to fix the problems that were presented by Bill C-51. We have identified a number of those issues in the past, the definition of "terrorist propaganda", for example, the problem with the no-fly list, various other ways that have been enumerated in which the legislation has presented difficulties and has been rightly criticized by a great many Canadians. We are at the beginning of what I think is likely to be the most inclusive consultation process about national security that the country has ever seen.

[*Translation*]

Mr. Matthew Dubé: With your permission, Minister, I would like to ask the following question.

With regard to the creation and operation of that committee, do you commit to formally including opposition parties?

[*English*]

Hon. Ralph Goodale: Yes, the commitment is clear. Now, when you say "this committee" you mean the committee of parliamentarians to scrutinize....

● (1140)

Mr. Matthew Dubé: The McGuinty committee, as Mr. O'Toole likes to refer to it.

Hon. Ralph Goodale: It's a legislated statutory committee of parliamentarians to scrutinize the security intelligence operations of the Government of Canada.

As I said earlier, there are probably 17 different departments and agencies that have some security function. The committee will be a committee representing all parties in the House of Commons. We are still considering the interface with the Senate. That hasn't been decided yet. I'll be meeting with senators later on to discuss that, but on the specific question of whether members of the opposition will be on that committee, yes, absolutely. If they weren't, the committee wouldn't work.

[*Translation*]

Mr. Matthew Dubé: I would like to specify that my concern is not about the presence of members on the committee, but about the participation of the opposition in the setting up and operations of the committee. We can talk about this again, because my time is limited.

With your permission, I am going to move on to another topic.

[*English*]

There was a *Globe and Mail* story yesterday, with the Prime Minister going to visit his counterpart in Washington, on the question of streamlining border services and how that's all operating. Some concerns were raised by the Privacy Commissioner with regard to removing red tape and the consequences that this can have on how information flows.

The other problem is that often when we have these agreements with Americans, it's important to remind folks that our laws and American laws are quite different especially when it comes to protecting the privacy of Canadians. Where is that process at? What's going on, and can you guarantee to this committee that the private information of Canadians will be protected according to Canadian law and not American law?

Hon. Ralph Goodale: Any agreement between two countries with respect to matters of information about citizens would need to respect the laws of the jurisdiction within which the information originated. So the short answer to your question is yes.

As discussions about the border proceed, we have been very careful to engage the office of the Privacy Commissioner, to seek guidance from that office to make sure that the best practices are followed. We will continue to seek that advice, and of course, after the fact we're obliged to produce a privacy impact statement, so we will make sure that is done—

[*Translation*]

Mr. Matthew Dubé: Thank you, Minister.

As my time is almost up, I have one last question for you and it follows upon the one my colleague Mr. Garrison put to you in the House concerning the Police Officer Recruitment Fund, which was abolished by the previous government.

Will you, yes or no, commit to re-establishing that fund?

[*English*]

Hon. Ralph Goodale: That is not in the fiscal frame at the present time. What is within the fiscal frame is a commitment that we made during the election to establish a new fund, specifically directed at the battle against guns and gangs, in the amount of $100 million on an annual basis that would flow through provinces to police forces in order to assist those forces with the very difficult on-the-ground work they need to do in combatting illegal guns and gangs.

The Chair: Mr. Mendicino.

Mr. Marco Mendicino (Eglinton—Lawrence, Lib.): Thank you very much, Mr. Chair.

I want to thank the minister for coming today to talk about the supplementary estimates.

I also want to take the opportunity to thank the deputy minister for his years of service. How many years did you say it was?

Mr. François Guimont: It was 34 years and—

Mr. Marco Mendicino: It must have gone by like the blink of an eye.

Hon. Ralph Goodale: He's a lot older than he looks.

Mr. Marco Mendicino: There's a compliment.

I want to try to cover two topics today, Mr. Minister. I want to talk a little about the oversight committee, and then I want to talk a little about the no-fly list, and if you'll permit, I'd like to ask some very targeted questions regarding oversight.

You talked about our fundamental commitment to creating a national oversight committee. You talked about Canada being an anomaly among our partners, and particularly with respect to the Five Eyes. You talked as well about the creation of that committee as a creature of statute. There'll be a piece of legislation that basically strikes a national security oversight committee. Is that right?

Hon. Ralph Goodale: That's correct.

Mr. Marco Mendicino: Will this be an all-party committee?

Hon. Ralph Goodale: Yes.

Mr. Marco Mendicino: Will it be made up of parties from all sides of the House?

Hon. Ralph Goodale: That's right.

Mr. Marco Mendicino: Will it be made up as well of both Houses? Is that what we're contemplating right now?

● (1145)

Hon. Ralph Goodale: That remains an open question. We haven't yet had that conversation with the Senate, but we're open to a good discussion of it.

Mr. Marco Mendicino: Is it safe to say that we'd like to see progress so that we could include the Senate as part of this committee?

Hon. Ralph Goodale: I'd like to see it be comprehensive, but we haven't really crossed that policy bridge yet.

Mr. Marco Mendicino: Will membership of the committee exclude ministers and parliamentary secretaries?

Hon. Ralph Goodale: You said "exclude"? Yes.

Mr. Marco Mendicino: Okay. Will these be order in council appointments, which is to say, will the people be appointed by the Prime Minister's Office or by cabinet?

Hon. Ralph Goodale: The method of selection has not yet been determined. What will be required is an extraordinary level of security clearance, because obviously these members of Parliament will have access to very sensitive information and will need to be appointed on a basis that respects that very critical dimension of public safety and security.

Mr. Marco Mendicino: Is it possible that as part of the process the screening may contemplate an order in council appointment?

Hon. Ralph Goodale: That's possible, yes.

Mr. Marco Mendicino: Okay.

You mentioned earlier to some of my colleagues on the other side about appointing members from the opposition. Is it the government's plan to consult with leaders of the opposition parties before including members of their party?

Hon. Ralph Goodale: There obviously needs to be very thorough consultation with party leaders and with members of Parliament in order to get this appointment process right. The exact methodology has not been settled, but we will seek advice on all sides of the House to make sure we have a satisfactory way of assembling the committee.

Mr. Marco Mendicino: Regarding powers that are contemplated for the national security oversight committee, is it your vision that the committee will have the power to compel witnesses to attend and give evidence?

Hon. Ralph Goodale: That policy question has not yet been determined.

Mr. Marco Mendicino: Has it been determined whether or not we'll have the ability to compel individuals to bring information that might otherwise be categorized as privileged under the national security provisions?

Hon. Ralph Goodale: That's in the same category of compelling witnesses or compelling documents. Those issues have not been resolved yet, but I do repeat the objective here. This committee has to be real. It has to be credible. It has to be trustworthy so that when it does its work and offers comments to Canadians on the nature of its work, Canadians will be able to trust that they are being told the truth. Credibility is absolutely essential here, and we need to make sure the committee has the tools necessary and the resources and the research capacity to do its job.

Mr. Marco Mendicino: I have one last question on a national security oversight committee. Will we find any references to it in the supplementary estimates, or is it safe to say that because we're not at the stage yet where presenting the legislation is imminent with regard to this committee, it's not in the current supplementary estimates?

Hon. Ralph Goodale: It's not in the current numbers. This again gets back to my first point about the strange way in which Parliament deals with estimates. The main estimates that have been tabled are actually based on last year's budget, not the budget we'll get on March 22, so we have to change the order of things here to make it logical.

Mr. Marco Mendicino: With regard to the no-fly list, Mr. Minister, you were recently quoted in the papers as expressing some frustration on the part of certain children who continue to be flagged by the no-fly list, erroneously, it would appear. Can you tell this committee what steps your department is taking to ensure this doesn't happen in the future, or at least that we are continuing to reduce the likelihood of children being erroneously flagged by the no-fly list?

Hon. Ralph Goodale: The point is clearly this. Those children who have been erroneously caught up in the no-fly process are not on the no-fly list. The problem is that there are some adults who have exactly the same names who are on the no-fly list, and it's the confusion between the two that is causing the problem.

When the system was designed a few years ago, it did not include an interactive, internal database that would allow false positives to be easily flagged and then resolved. In fact, it relied on physical identification at the gate, and within 5, 10, 15 minutes, the problems could be resolved. But that still presents an awkward situation at the gate, so we have to find a way to improve the database and the computer system. There may be some lessons that we can learn here from the American side of the operation, because they do have an interactive system that resolves false positives faster than we do.

● (1150)

Mr. Marco Mendicino: May I just use the few seconds remaining to ask whether or not you've contemplated some sort of appeals process so that there is transparency for those individuals who have been erroneously flagged?

Hon. Ralph Goodale: Yes, and that was a specific commitment in our platform.

Mr. Marco Mendicino: Thank you.

The Chair: Thank you, Minister.

Mr. O'Toole.

Hon. Erin O'Toole: Thank you very much, Mr. Chair.

Minister, a number of my colleagues have been asking about the committee of parliamentarians for security intelligence review. We've been affectionately calling it the McGuinty committee, for lack of any other description.

Hon. Ralph Goodale: Your affection is overflowing, Mr. O'Toole.

Hon. Erin O'Toole: Well, you see that pragmatically last week after consultations with the NDP, and the lack of consultations from the government, I sent you a letter with recommendations. Mr. Mendicino clearly read it because several of his questions to you were contained in my letter.

You were saying the exact methodology is to be resolved, and you need this to be credible. You're clearly still putting parameters on it. Why appoint a chair before even the parameters are done?

Hon. Ralph Goodale: Well, we're reaching out to have a very inclusive process, and Mr. O'Toole, I would, quite frankly, apologize to members of Parliament around the table here for not being able to move as quickly on this as I would have liked to. I've said on other occasions that this department is like riding a fire hose, and trying to get up to speed on every issue is a big challenge, but we're getting there.

Hon. Erin O'Toole: Certainly.

Hon. Ralph Goodale: I welcomed your letter, as I did Monsieur Mulcair's letter. It is helpful input into the process. Mr. LeBlanc and I will be meeting shortly with members of the Senate to get their input. We will have a more fulsome discussion of this.

The suggestions that you and others have made about how to structure this committee, and what power and authority it needs to have, are helpful input. We will weigh all of that very carefully.

Hon. Erin O'Toole: I appreciate those comments. I know MP Rankin and I will wait by our phones for the call.

I have one final question on this subject. You talked about the official secrets that will be involved, the credibility. Mr. Mendicino mentioned this as well.

The Intelligence and Security Committee of Parliament in the U. K. has had some success with discretion over two decades. One of the points I made was that members should have some experience in security, national defence, previous experience chairing a committee, or ministerial experience, to ensure that the quality and effectiveness of the committee is safeguarded. Is that your plan?

There has been some speculation that you've already identified government members for the committee. Can you confirm whether or not that's true?

Hon. Ralph Goodale: The final decisions have not been taken, Mr. O'Toole.

The kinds of qualifications that you referred to in your letter will certainly be helpful. They may not be the only ones, but I take your point that this committee needs to have the horsepower to do a good job. Otherwise, why have it? It's not there to be window dressing. It's not there to be a buffer or a deflection. It's there to give Canadians the assurance of two things; namely, that the agencies are doing what they need to do to keep Canadians safe, and that the values, rights, and freedoms of Canadians are properly respected. I want this to be a very high-calibre group of parliamentarians who will be able to give Canadians that assurance.

Hon. Erin O'Toole: Well, certainly the Conservative Party wants this to be done right. We're prepared to work with the government, particularly to ensure the safety of the operations conducted by our intelligence agencies and their personnel.

My final question relates to the court decision in the case of Mounted Police Association of Ontario v. Canada. We spoke in the House on this subject when the government sought an extension of the court period for that case. I understand that the government will be bringing forward legislation very shortly on the new designated bargaining model, using guidance from the court to ensure that members have the right of collective action. Whether or not it will be in the Public Service Labour Relations Act...

In the estimates we see another $110 million for the RCMP, with about half of that being for contract policing. Has your department, working with the commissioner, looked at the impact on the fiscal framework of the legislation that will be in front of the House in the next few weeks, in terms of how much upward pressure it may put on budgets?

● (1155)

The Chair: Very briefly, Minister.

Hon. Ralph Goodale: The Supreme Court has been very clear that RCMP members not having collective bargaining rights is in violation of their constitutional rights, so the legislation will remedy that constitutional defect. That will result in a bargaining process that, as with the bargaining in all other sectors of the public service, will be handled by Treasury Board.

You will find in the legislation a design to ensure that the unique nature of policing operations is appropriately safeguarded.

Commissioner, do you have some thoughts that you—

The Chair: I'm sorry, we're at the end of the member's time. Thank you, Minister.

It's hard to cut off Mr. Goodale.

Hon. Ralph Goodale: Worse still to cut off the commissioner.

The Chair: Oh, I'm worried about that.

Ms. Damoff.

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Thank you very much for being here and for bringing your officials with you. I'm going to change the subject just a little bit.

I've met with representatives of the Canadian Association of Elizabeth Fry Societies and the John Howard Society. They've talked to me about devastating personal and financial costs to individuals because of changes that were made by the previous government to pardons or record suspensions. I wonder if you could speak to that a little bit.

Hon. Ralph Goodale: I may ask Mr. Cenaiko to comment as well, because he has the task of dealing with these challenges.

There has been a considerable backlog. Through his own good internal management within the Parole Board, he has been able to make progress in resolving the backlog. There is still some of it remaining, but as I understand it, Mr. Cenaiko is expecting to be able to deal with most of that over the course of the next year or so.

There were also changes made in terms of fees that were charged and the time that is taken, and so forth. We will re-examine all of that to ensure it is good, solid public policy, not intended to accomplish an ideological purpose but in fact designed to contribute to the well-being of Canadians and to public safety.

Harvey, do you have some comments to make on the backlog?

Mr. Harvey Cenaiko (Chairperson, Parole Board of Canada): I just have—

Ms. Pam Damoff: Actually, I have only five minutes. What you've told me is good enough that I can take it back to them. I'm sorry to cut you off, but I have a couple of other things I want to ask you about and I don't have much time.

Hon. Ralph Goodale: Okay.

By the way, after I leave, the officials will be able to stay for a while.

Ms. Pam Damoff: Okay, so we can follow up on that afterwards.

Hon. Ralph Goodale: Yes.

Ms. Pam Damoff: When Mr. Head appeared before the committee, he said, and I'm quoting him here, "I cannot stress enough how important that" occupational stress injury support is. He went on to say, "The way we talk about it now is on how we build and sustain the mental resilience of our staff...".

I've talked about this at all of our meetings. It's something I'm very passionate about. I applaud what you've done so far. I think we need to be removing the stigma around this in the workplace. Our public safety officers need to be on the top of their game, both physically and mentally.

Can you talk briefly about the financial cost as well as the potential need for additional funding for this issue within your department?

Hon. Ralph Goodale: Well, the cost of occupational stress injuries and disabilities is difficult to quantify, but I think Canadians are coming to recognize that they take a huge toll in terms of the efficiency of people being on the job, the capacity to do the job, the time they need to be away from work, and lost talent, altogether.

Do we have an internal calculation of the cost consequences of PTSD? Quite frankly, I'd like to—

● (1200)

Ms. Pam Damoff: We can get that later.

Hon. Ralph Goodale: Yes, we could take a stab at putting together some estimates.

Bob, within the RCMP, what is the toll?

Commr Bob Paulson: It is $162 million—that's why we have a $6 million ask in the supplementals—and it's on a 12% increase, year on year.

Hon. Ralph Goodale: So it's expensive.

And we need to make sure when public safety officers suffer a mental health issue because of their job that they get the kind of support they need, that there is not a stigma attached to asking, that their friends and colleagues and superiors know the danger signs to look for, and that the treatment capacity is readily available not two years from now or six months from now, but now, when you have the opportunity to relieve that person's stress and maybe head off a bigger tragedy.

That's why we're putting such emphasis on PTSD treatment and responses for public safety officers.

Ms. Pam Damoff: That's why I push so hard for us as a committee to look at it as well. I think it's a really important issue to shed some light on.

I don't think I have any time left. Have I?

The Chair: You have 14 seconds.

Ms. Pam Damoff: Okay. I can say thank you very much.

I could have let you speak after all.

The Chair: Thank you, Ms. Damoff.

Ms. Gallant.

Mrs. Cheryl Gallant (Renfrew—Nipissing—Pembroke, CPC): Mr. Chairman, this is through you to the minister.

Just prior to Christmas last year there was a worker inside an electricity control centre. He was preparing to leave, and he noticed a cursor on his computer suddenly slide across the screen on its own. One after another, circuit breakers were turned on until substations were turned off—30 in all—for 230,000 residents, two days before Christmas, in western Ukraine, with no electricity and no heat.

The concern is that this type of sophisticated, planned, synchronized attack could occur in North America.

What measures are in place to ensure that such a coordinated attack, or perhaps a more sophisticated one, does not impede our electricity system and all the items attached to the grid that we depend on?

Hon. Ralph Goodale: That is a very good question.

I share the concern of members of Parliament about Canada's capacity to deal effectively with cybersecurity issues, the whole issue of our critical infrastructure, which you've referred to as potentially vulnerable. The incident in Ukraine, by the way, was a very active topic of discussion at the last meeting of the Five Eyes alliance in Washington a few weeks ago. It's a matter of international anxiety.

There's simply a loss to businesses and enterprises from having their systems hacked and interfered with. That probably cost businesses globally $400 billion last year. By the end of this decade, that cost is probably going to surpass $2 trillion U.S. per year. The dimensions of this, not to mention privacy issues and so forth, are huge.

Toward the end of last year the RCMP launched a whole new initiative with respect to being more effective in dealing with cybercrime. The Business Council of Canada, formerly the Canadian Council of Chief Executives, has launched a new exchange of information system in order to prepare business to deal with this more effectively. Federal, provincial, and territorial security ministers have had this conversation, as well.

I have been asked by the Prime Minister to lead a review of everything in the Government of Canada that relates to cybersecurity, in collaboration with the industry department and many other departments of government, to make sure that we are on top of this kind of situation and that the problem that hit Ukraine will be properly defended against in Canada. We think that is the case today, but the review will ask that critical question: are we sure? We want to be sure.

● (1205)

Mrs. Cheryl Gallant: The criticism I hear about the Canadian cyber incident response centre is that it's passive. There are plans and tips given, but in the event of a cyber-attack, be it commercial or otherwise, there is not an instant response.

Do the supplementary estimates reflect any efforts to stand up a coordinated command and response to these types of incidents?

Hon. Ralph Goodale: Let me ask the deputy minister to comment.

Mr. François Guimont: Thank you, Minister.

The CCIRC, the capacity we have in public safety, is co-located with the government operations centre and it would be helpful if we were successful in relocating it. This group is very capable. It has augmented its capacity over the last budget, so there are more people in the group. That's the first observation.

The second one is that they're pretty active. Their responsibility is one of getting information from the operator when they face a situation. They literally keep a laboratory of viruses that they study to understand. They're very quick at disseminating information to other constituents in Canada to help them take action to protect themselves. They are at that pivot point. There is information flowing to them from inside and outside government which they pass back to the industrial sector of Canada. This is one of their key features, their key role.

We want to work more closely with the industry. The industry is giving itself a similar capacity. It's all about information sharing. It's all about the speed of the information sharing, so that people can then take action to protect themselves.

They have now invested in tools where this response will be automated. We've made investments. Therefore, instead of relying only upon individuals to pass on the information, there will be an automated system whereby this information will fan out across Canada.

Progress has been made, but I'll tell members of the committee that the cyber file, unlike other files, if you will, is always evolving. It's a little bit like all your devices that have new functionality and new applications. All that reality, which is quickly moving, is also moving on us.

I'm tempted to say that we're all only as good as we are, and therefore the idea of carrying out a comprehensive review of our cyber strategy is a very timely thing. The strategy is not that old, but the file is moving so quickly. It's time to step back, see where we are, and carry out actions where we think we may have weaknesses.

The Chair: Thank you very much, Mr. Guimont.

Hon. Ralph Goodale: Mr. Chair, could I ask if every member of the committee has changed their password today. You're supposed to do it frequently.

The Chair: Thank you.

We're going to suspend the meeting for a few minutes. Mr. Goodale is leaving to go to another meeting. The officials are going to stay. I'm going to suggest to the committee that we finish round one. We would go with Mr. Spengemann, then Mr. Dubé, and then start back at the top of the list for round two.

We'll suspend for two minutes.

Hon. Ralph Goodale: Mr. Chair, thank you for the opportunity to be here. I appreciated your questions. I even look forward to coming back another time.

The Chair: You'll be invited.

Hon. Ralph Goodale: Might I suggest to you on the cyber centre that was the subject of the last question, it might well be possible to arrange an opportunity when members of this committee, if you're interested, could pay a visit to the cyber centre and see it functioning. That might help with some of the background information.

The Chair: Excellent. Thank you very much.

We'll suspend for a few minutes.

● (Pause)

●

● (1210)

The Chair: We're missing a few members. As I suggested, we're going to finish round one. That will be five minutes for Mr. Spengemann, three minutes for Mr. Dubé and then we will start back with the seven-minute round and the first one will be Mr. Erskine-Smith in the second round.

Mr. Spengemann, for five minutes.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Thank you, Mr. Chair.

Thank you to our six distinguished senior public servants for being here. Thank you for your service to the nation, and my thanks also to your colleagues, the women and men who are in the field keeping us safe day after day who are not here today but through you are represented here.

I have two questions. One of them is specific and the other is more general. I'll start with the more specific one.

In our ridings I think many of us parliamentarians around the table and colleagues who are not here will have received questions over the past months on the issue of marijuana. I've had folks come to me from the production side, people who are interested in holding licences to produce medical marijuana, people from the consumer side, people who are beneficiaries of medical marijuana. Also there are the pros and cons of the recreational side.

I'm wondering if you could give the committee, and through the committee the Canadian public an update on the current legal status of marijuana.

● (1215)

Commr Bob Paulson: Me?

Voices: Oh, oh!

Mr. Sven Spengemann: That's for anybody who would like to comment, anybody who has relevant information to give.

Commr Bob Paulson: I can say that the current legal status is unchanged from where it was before the new government came into power.

I can say that we've had a struggle in the police community broadly in terms of being discretionary in recognizing the stated objectives of the government, while having to recognize the existing laws. In other words, the medical marijuana regime, and frankly, the explosion of dispensaries in many cities across the country present a number of technically challenging legal conundrums.

Certainly, we in the RCMP have applied our discretion to enforce where circumstances are exceeding the scope of the existing legislation around medical marijuana, in other words, aggressive marketing, on the street, near schools, and so on. In some communities they're even contemplating taxing and licensing.

I might point out, just technically, not as a stated intention, there's an argument to be made that licensing some of these illegal dispensaries amounts to receiving the proceeds of crime.

It's a bit of a mess right now, to be honest. Our approach has been to use our discretion at the front line to make decisions while the government sorts out their stated platform.

Mr. Sven Spengemann: Is it fair to say that you have changed your enforcement strategy in the wake of recent platform policy announcements, or is it the same as it was a year and a half ago, let's say?

Commr Bob Paulson: No. I would say it's fair to say that we've changed. We understand the platform. We understand the existing laws, but we also see a proliferation of patently unlawful behaviours that need to be held in check while we get to a point where a more coherent legislative regime is in place.

Mr. Sven Spengemann: Thank you for that.

My second question, as I said, is a more general one. I'd like to address it to as many of you as would like to comment. I think, if we look back on this conversation this morning, what connects all our questions and the answers that many of you gave is the idea of trust in our public institutions.

The minister said we're balancing the provision of effective security against or with our charter rights, and when we do that well, we earn the trust of Canadians. So the maintenance of trust, the strengthening of trust in our public institutions is not unique to public safety and security, but it is perhaps something that we should look at emphatically with respect to the area of public safety and security.

I'm wondering if each of you could comment briefly on how you are working to maintain and strengthen the trust of Canadians in the various organizations that you oversee.

Mr. François Guimont: Maybe I could say a few words to start. Trust is important for sure in the institution and Canadians can step back and look at the portfolio partners and be convinced, and I mean that truthfully, that we are professional and we do our best.

We wake up in the morning, and come to work to do a good job. A good job means we're on all the time, because this business that we're in doesn't stop at five o'clock or six o'clock.

The second point is that people are very lawful, very mindful of the legal framework in which we work. I would say as well it's a function of teamwork. We work very closely with the commissioner's people when we need to, Commissioner Paulson, and Michel Coulombe, the director of CSIS. We have ongoing discussions, relationships, built on trust, and that trust inside projects outside in the sense of Canadians. I think they can feel that we're doing our best to earn and keep their trust.

As I said, we work within the legal framework and we work within the policies and the operational procedures that we give ourselves.

● (1220)

The Acting Chair (Hon. Erin O'Toole): Thank you very much, Mr. Guimont.

Three minutes for Mr. Dubé.

[*Translation*]

Mr. Matthew Dubé: Thank you, Mr. Chair.

My question is addressed to Mr. Head. In fact, I would like to go back to the topic I raised the last time he came before the committee.

The Ontario Human Rights Commissioner has spoken out about solitary confinement. That is not the preferred term, but I am going to continue to use it nonetheless. She mentioned that this practice should be brought to an end in provincial prisons or should at the very least be restricted. I continue to insist that this committee should study this matter. I know that my colleague Murray Rankin shares my opinion.

What do you think of the commissioner's statement? Does it reflect reality in federal penitentiaries?

[*English*]

Mr. Don Head (Commissioner, Correctional Service of Canada): Thank you for the question.

As I briefly mentioned at the last appearance, we've made a lot of progress at the federal level in terms of how segregation, or solitary confinement, as some people call it, has been used. We have put in place a series of additional, internal, oversight processes. We have also put in place different alternatives for housing offenders other than in the institution where they're being segregated or held in special confinement conditions.

I have to say that in comparison to the provinces we have a little more in terms of resources to do some of the work that we've been doing. Even in the last year, we've been able to reduce the segregation population by almost half. We've gone from just under 800 down to 396 people who are in segregation on any given day. The challenge that the provinces have is in relation to resources and a population which is not comprised of individuals who have longer-term sentences with whom they can work to deliver programs. The provinces have a little more of a challenge than we do at the federal level.

[*Translation*]

Mr. Matthew Dubé: Mr. Chair, do I have a little time left?

The Chair: You have one minute left.

[*English*]

Mr. Matthew Dubé: I have a quick question for Mr. Paulson.

I am wondering about the criminal database backlog which the Auditor General has raised a few times. I think we're closing in on seven years since this has been brought to our attention.

Can you give us an update on where that is, or do we have to wait for the Auditor General to report on it again?

Commr Bob Paulson: No, I don't think you have to wait for the Auditor General again.

We have implemented a plan to reduce the backlog on a cascading priority level, while recognizing that the transition to electronic reception into the system, the taking of fingerprints and biometric data, is a tough transition, not necessarily just for the RCMP, but also for other police services. That transition is making it difficult, but we are trying to prioritize our updates to the record database so that courts are properly informed as to what they're facing when criminal records are presented, and so that police officers, perhaps more importantly, are aware of who they're facing when they are doing their jobs.

The plan is in place and it's a massive undertaking to digitize that whole approach. I'll undertake to provide an update in more detail if you'd like.

The Chair: Thank you, Mr. Paulson.

Mr. Erskine-Smith, for seven minutes.

Mr. Nathaniel Erskine-Smith (Beaches—East York, Lib.): Thank you very much.

I'd like to deal with the estimates themselves. I'd like to start with the Canada Border Services Agency. There's a line item of $21 million in funding to improve the integrity of the CBSA front-line operations. It's one of the largest line items we have before us.

Could you give us an explanation as to where those monies would go?

Ms. Nada Semaan: Absolutely.

This is money that has been provided since 2011. It serves to help with the program integrity in three areas. First, once we became an armed workforce we could no longer utilize students on the land borders, so we now need to supplement that in peak periods with regular officers, which is an increased cost. Second, with small and remote ports, we needed to double up our officers for safety and security purposes. That required an additional workforce in all of our small and remote ports. Third, when we became a department or an agency, we came from a number of other agencies, one being the CRA, the Canada Revenue Agency. The conversion of their status at CRA to a border force officer also required additional money. That's basically all it is.

● (1225)

Mr. Nathaniel Erskine-Smith: Thanks very much.

My next question is for the Correctional Service of Canada.

I note that since March 2005, the federal inmate population has increased by 17.5%. Could you comment, Mr. Head, with respect to whether funding levels have matched the increase in federal inmates?

Mr. Don Head: There are a couple of components to that.

Actually, over the last year or so the population has been coming down. As of this morning, the incarcerated population sits at 14,613. This is down from a peak when it was at just over 15,200, so it has been coming down over the last year.

We did receive money over the last three or four years for the building of additional cells and additional accommodation space; however, we did not receive additional monies to increase programming capacity. We had to find some measures and implement some streamlining efficiencies to keep the level of programming going.

Mr. Nathaniel Erskine-Smith: If I can, I'll jump in there.

On programming specifically related to the aboriginal inmate population, which is excessively high, the Truth and Reconciliation Commission recommendations called upon the federal government to provide more supports for aboriginal programming, halfway houses, and parole services. Under your current funding model, are you able to provide those services?

Mr. Don Head: Under the current funding model, in order to go forward I would need additional funding.

Mr. Nathaniel Erskine-Smith: My next question is for the Parole Board of Canada.

In your 2015-16 report you note that there's "a risk that key activities and functions could be adversely affected unless the Board is able to recruit, stabilize, strengthen competencies and capacity, and retain its workforce while ensuring employee wellness". I note that there's not a significant amount of new funding. In fact, the funding is going to implement the Canadian Victims Bill of Rights.

I wonder if you could comment on whether you are receiving sufficient funding to do your job.

Mr. Harvey Cenaiko: That's a good question. The funding we're receiving in the supplementary (C)s is really to assist us with the web portal that the Correctional Service of Canada is going to be providing us.

With that, we'll be able to provide victims with an electronic means to register and to get information for themselves. In addition, though, on our own, for those individuals who don't have the Internet or for remote communities or indigenous communities where no Internet is available, we want to ensure that victims who cannot attend a hearing personally can have the ability to access a digital recording of the hearing so they can in fact hear it themselves.

Mr. Nathaniel Erskine-Smith: As we move forward with the legalization of marijuana and perhaps move forward to increase pardons for those who have records related to possession and perhaps low-level trafficking offences, would you envision needing significant additional resources to process those pardons?

Mr. Harvey Cenaiko: Well, we'd have to see what the legislation brings forward before we could actually make a determination on how that might impact us.

First of all, there are no pardons. They're record suspensions. If the term is going to be changed, then the legislation would have to be changed. However, I understand what you're saying.

Mr. Nathaniel Erskine-Smith: Sure.

My next question is for the RCMP. I note that there's $6 million in funding related to government advertising programs. Could you fill us in as to where those monies go?

Commr Bob Paulson: Well, to recruiting, mostly to recruiting. In fact, we're on a bit of a campaign to up our numbers. The force is challenged to meet attrition and growth and attract the right people to the organization, so we've embarked on a very targeted and focused recruitment effort to bring good young people of all backgrounds into the force.

Mr. Nathaniel Erskine-Smith: Thanks very much.

My next question is for the Canadian Security Intelligence Service. There's a line item of $1,160,000 for software tools to process digital information. Are these software tools created in-house? Is that the reason the line item is so large?

Mr. Michel Coulombe (Director, Canadian Security Intelligence Service): Yes, that's it.

Mr. Nathaniel Erskine-Smith: Does CSIS use these software tools as part of its own investigations?

● (1230)

Mr. Michel Coulombe: Yes.

Mr. Nathaniel Erskine-Smith: Moving to SIRC, I note there's $240,000 in funding to support an increase in the complexity and volume of workload related to SIRC's review of the expanded operations of CSIS. What specifically are these expanded operations that require $240,000 more to go to SIRC?

Mr. Michel Coulombe: Could you repeat that?

Mr. Nathaniel Erskine-Smith: Sure. I'll take you to the line item. It shows $240,000 for funding to support an increase in the complexity and volume of workload related to SIRC's review of the expanded operations of CSIS.

Mr. Michel Coulombe: Yes, as SIRC is expanding the number of reviews they're doing—

Mr. Nathaniel Erskine-Smith: Oh, sorry. It said "expanded operations" of CSIS, so that may be incorrect, then.

Mr. Michel Coulombe: Well, that's it, but as we're expanding our operations, SIRC might increase the number of reviews they're doing of our operations and we need more people to actually support the work that SIRC is doing in terms of those annual reviews.

Mr. Nathaniel Erskine-Smith: Is the expanded work the new disruption powers, the new information sharing, and the new powers under Bill C-51 specifically?

Mr. Michel Coulombe: That's part of it, but it's also the expansion of our operation overseas and the expansion of operations here in Canada.

Mr. Nathaniel Erskine-Smith: That makes sense. Thanks very much.

The Chair: Thank you.

Mr. O'Toole.

Hon. Erin O'Toole: Thank you very much, Mr. Chair.

Thank you to our witnesses for remaining with us.

Mr. Coulombe, you are not as busy as you were yesterday before a committee, so I'm going to spend a little time with you. The minister outlined in his remarks the focus on counter-radicalization and stopping those threats before they gather. I think all sides want to proceed on that. We've been trying to look at that from day one as a committee.

Yesterday in front of the Senate committee you mentioned the disruption powers that have been used two dozen or so times. Without revealing any specifics, could you in general terms discuss what type of disruption it was and what the risks were of a general nature? I know this might be hard for you, but I'd like to understand the type of disruption that has been engaged for public safety reasons.

Mr. Michel Coulombe: As I mentioned in my last appearance in front of this committee, the threat reduction measures used so far did not require Federal Court warrants. That's the first thing that needs to be understood.

Generically, the type of activities we're talking about go from conducting an interview and overtly letting the subject of the investigation know that they are under investigation, to asking family members, friends, and community leaders to intervene when somebody is on the path to radicalization. Trying to bring a counter-narrative to stop that radicalization would be another example; it could be about preventing a terrorist target of investigation from accessing a potential target facility.

Those are the types of measures we've used so far. The risk is minimal because again, we're not talking about warranted threat reduction measures.

Hon. Erin O'Toole: You've mentioned working in some cases with family members or community members to halt the risks of radicalization. Have there been any instances you can speak of, without specifics, where there has been foreign influence, either through connections through an organization or through the flow of money to an organization on the ground in Canada?

Mr. Michel Coulombe: Well, most of the time actually there is, if you want to qualify it as a foreign influence. It's usually through the Internet and social media, from organizations such as Daesh, the Islamic State in Iraq and the Levant.

Hon. Erin O'Toole: About the money piece, is there an ability to watch the flow of money to see if that's supplementing what can start as radicalization online but can lead to a cluster, as we've seen in Ottawa and Calgary? Has money flowed?

Mr. Michel Coulombe: Money flow is something that the service is looking into as a subject of investigation. Money flow is certainly something that is of importance. It's part of our investigation in collecting intelligence on the activities of the target.

Hon. Erin O'Toole: The minister has mentioned the counter-radicalization coordinator and a national office. We've read a lot about it in the media, but we haven't received any specifics on it in Parliament. Are some of your operations and outreach within the counter-radicalization community and the groups tackling this informing the minister as he creates this position and the scope for the department?

● (1235)

Mr. Michel Coulombe: Yes, the role of the service and the work we've done so far, for example, being part of the Kanishka project and the analysis the service has done itself in terms of factors leading to radicalization, are certainly informing Public Safety as they're working on this project.

Hon. Erin O'Toole: Thank you.

Commissioner Paulson, thank you. You've both been here within a few weeks of previous appearances, so we appreciate your time. I have a question for you.

Mr. Spengemann outlined somewhat the uncertainty with respect to marijuana, in that there was an election promise with regard to legalization, yet there's a period before legislation or a regulatory review is coming forward. There's a kind of wild west being created by people who want to push the envelope forward.

The discretion that you noted, Commissioner, appears to be similar to the position that the chiefs of police of Canada took, in that the best way to approach this might be to empower law enforcement with the ability to issue a ticket in the circumstances where use is recreational and there's no impact on youth or things like that, or to lay charges for more serious incidents near schools or for someone who might be trafficking or dealing and that sort of thing.

That was a recommendation as opposed to legalization. Is that in effect what is happening now in this sort of grey zone between the election promise and future legislation?

Commr Bob Paulson: Yes, I don't think we should overstate the greyness of it. I would draw a parallel to coming across someone with a still who is making whisky for commercial purposes. We wouldn't issue a ticket, right? There are ample other statutory paths to prosecuting them. That's somewhat analogous to this situation.

The people who are exploiting.... Maybe I shouldn't say exploiting, but there's a misunderstanding, it seems to me, in the Canadian consciousness about what the state of the law is. People are trying to take advantage, frankly, and make some money. Where those people are identified as organized crime figures or serious criminals with criminal enterprise intentions, or where they are doing that around schools, or marketing that overtly and affecting children, we're taking action. I think that's a reasonable course.

Hon. Erin O'Toole: We're three or four months past the election when the promise was made. Do you find that the aggressiveness of some players in this space is becoming more pronounced as time passes?

Commr Bob Paulson: No, it seems to be pretty steady.

The Chair: Thank you very much.

Monsieur Dubé.

[*Translation*]

Mr. Matthew Dubé: Thank you, Mr. Chair.

Mr. Paulson, I would like to discuss another aspect of the criminal activity intelligence database. We know that the situation may have changed and perhaps you could provide us with more detail on this.

In Quebec, according to what the Auditor General said, processing times are longer for requests in French than in English. According to the information I have, the wait time is 14 months for requests in English, whereas in Quebec it is 36 months. Is this due to a lack of sufficient resources to meet official languages commitments? Is that what explains that difference?

Commr Bob Paulson: Unfortunately, Mr. Dubé, I am not in a position to explain what is going on. What could explain this difference is that in Quebec there are several police forces, whereas elsewhere in Canada, the RCMP does this type of frontline police work. I do not have the figures, but there are hundreds of police corps in Quebec and each one has to adjust its policy to manage—

Mr. Matthew Dubé: Forgive me for interrupting you, but my time is limited.

Ontario has a provincial police force like the one in Quebec, and yet the situation is not the same. Do you have a shortage of resources to meet official language commitments in Quebec? I understand what you are saying, but once again, the situation is the same in Ontario, but it does not have the same problem.

● (1240)

Commr Bob Paulson: There are also challenges in Ontario. Even though they may not be as serious as the ones in Quebec, we still have to meet the challenge which consists in changing the processes to provide information.

Mr. Matthew Dubé: Very well. I have taken note of this.

[*English*]

Mr. Head, if I may come back to you, once again I'm going to come back to the topic of solitary confinement.

I heard what you said, and I appreciate that the situation is different provincially and federally. That being said, I will ask once again, given that I think it's an important topic to study, do you still believe that this committee should undertake a study on the use of solitary confinement, and how we can see that going forward?

Mr. Don Head: It's a really good question. When I talk to my colleagues around the world, probably the common theme that is coming up at their management tables is the issue of segregation. Part of the reason it's at the table is there is a misunderstanding about what's going on, so I think that even having someone appear before you to talk about what segregation is, and what happens federally, provincially and around the world would be a good start to getting some facts out there.

As we go forward, looking at the whole issue, I think there is going to be an opportunity to consider possible policy, legislative and regulatory changes that will address some of the issues you see in the newspaper and playing out in our facilities.

M. Matthew Dubé: All right. Thank you.

[*Translation*]

I have a question for all the witnesses. Mr. Paulson may also want to answer.

Several members raised the issue of the legalization of marijuana. I think the government is beginning to realize that there is a difference between an electoral commitment and actually changing the laws involved. There is a certain vagueness at the moment, no matter what your opinion is on this topic, and this is causing a problem with regard to your work. We need some concrete action and more information as to the direction the government is going to take. Would you say that is an accurate statement? That seems to be the gist of your comments.

Commr Bob Paulson: In my opinion, changing the legislation and the regulations is very complex work.

[*English*]

It's a complex area. I think folks are going to be challenged to make that transition, and we want to help to the extent that we can.

[*Translation*]

Mr. Matthew Dubé: The situation remains uncertain because we do not know what direction the government is going to take. There seems to be more reluctance than there was before. This seems to be causing problems for you with regard to—

Commr Bob Paulson: The government's anticipated direction is clear enough, but with such a complex project, you have to expect that it will take some time.

Mr. Matthew Dubé: Fine.

Mr. Coulombe, given your line of work, you are a man of few words, often quite rightly so. Yesterday, you spoke of several decades of combatting terrorism. I would like to understand why you made such a statement, which could be worrisome for people.

How do you justify such a statement?

Mr. Michel Coulombe: I will give you an example.

The phenomenon of people going abroad to take part in jihad, in terrorist activities, is not new. We have seen it in Afghanistan, Bosnia and Chechnya. However, even if we add up all of these conflicts, we see that the number of people involved now in Syria and Iraq is probably 10 times higher. But we are still working today on the files of individuals who took part in these conflicts.

At the present time there are between 25,000 and 30,000 foreign combatants in that region who are neither Iraqi nor Syrian. As I mentioned yesterday, even if the Islamic State group is defeated militarily, these 30,000 individuals will leave the region to return to their countries of origin or go elsewhere to take part in jihad. Even if only 10% of them do so, we are talking about 2,000 people who will continue to participate in terrorist activities.

Mr. Matthew Dubé: Concerning the fight against radicalization, do you think that an approach that would include the communities concerned would have more impact than military measures? If I read between the lines, I believe that is what you were saying.

● (1245)

Mr. Michel Coulombe: I do not think the issue is whether one would have more impact than the other. It is really a continuum. We certainly cannot solve this matter simply by collecting information, or enforcing the laws and carrying out military operations. Nor will the issue be solved through deradicalization programs alone. What matters is that there truly be a continuum, with action all along the spectrum.

[*English*]

The Chair: Thank you very much.

We have time for one more seven-minute round. We'll go to Mr. Mendicino and then Ms. Damoff.

Mr. Marco Mendicino: Thanks very much, Mr. Chair.

I'd like to return to the topic of the national security oversight committee. Given that the minister has now taken his leave, I'm going to direct my questions to the deputy minister.

Within the broader context of oversight, we've heard about the distinction between real-time oversight and post hoc or after-the-fact oversight, which is more akin to what SIRC does. It looks historically at whether or not the departments are complying with the balance between the need to protect Canadians and to also safeguard their values under the charter.

We presently get real-time oversight through the national security adviser. Is that a fair statement?

Mr. François Guimont: Well, if by "we" you mean the government—

Mr. Marco Mendicino: I mean that the Prime Minister gets real-time—

Mr. François Guimont: Yes. It is a combination of Public Safety, the agency heads, the deputy minister, the minister, and the national security adviser and the apparatus around that unit.

Mr. Marco Mendicino: It's channelled through the national security adviser. Is that a fair statement?

Mr. François Guimont: For the PM, yes.

Mr. Marco Mendicino: It requires ongoing information and assessments provided to the executive branch, namely, the Prime Minister.

Mr. François Guimont: Yes.

Mr. Marco Mendicino: It also requires coordinating all of the various branches within the broader intelligence community. Is that right?

Mr. François Guimont: Yes.

Mr. Marco Mendicino: In the course of exercising that function, there is some oversight. Is that a fair statement?

Mr. François Guimont: Well, the oversight—I would use the word "review"—is separated along a number of lines at the agency. The director of CSIS has SIRC as a review mechanism. Commissioner Paulson also has the capacity, a review mechanism, to look at the operations of the RCMP. It's separated. It's not integrated. Also, they're not parliamentarians. That's the big difference. It's people who are from the outside, so they're at arm's length. They're not tied to Parliament.

Mr. Marco Mendicino: My question is this: where do you see the national security adviser's role within the national security oversight committee? Do you see this particular official being the most appropriate one to brief the national security oversight committee on ongoing real-time exercises of government authority as provided for under the relevant statutes?

Mr. François Guimont: Mr. Chairman, if I were to look at the dialogue we had in the U.K. when I was there with the minister in January, I would say that they will go where they need to go to get the information they need in carrying out their duties. It could be calling upon the NSA, but I can see the director of CSIS being called forward, and it's the same thing for Commissioner Paulson, me, or anyone.

I will again repeat myself. They will go where their mandate essentially allows them to go to get the information they need to carry out their work.

Mr. Marco Mendicino: This is in keeping with my question earlier to the minister about the ability to compel witnesses to come and provide evidence to the statutory committee.

Mr. François Guimont: That's a question that will need to be discussed.

In the U.K., they have the power to compel, if I remember, but they have been using an approach whereby in calling people to come forward to the committee the individuals contribute or collaborate quite freely.

That point will have to be discussed and decided by the government.

Mr. Marco Mendicino: Thank you very much.

Ms. Pam Damoff: On this International Women's Day, I want to go back to Commissioner Paulson. We talked about putting women in leadership in the RCMP. I appreciated your support that this needs to happen if we're going to change the culture to create a healthy workplace that is free from sexual harassment.

One of the things I had asked, and I might not have been clear about, is that we need women to enter policing. You're doing some promotion on that. We need them to remain in policing and also to take on leadership roles.

I'll give you an example of one of the obstacles I've heard, which is child care. For women, working shift work or working 12-hour shifts when day cares are open from 7 a.m. to 6 p.m. makes it very challenging to get into policing.

I'm wondering whether you need more funding to look at issues like that: why women aren't entering and staying in policing, and are there ways we can make it so they are able to both enter and stay in the RCMP?

● (1250)

Commr Bob Paulson: That's an excellent question, and it's something we've turned our mind to in the last several years as we've tried to advance on the gender and respect issues that we've been working on.

Just quickly, women have a retention rate in the force on par with men up until 25 years. That doesn't answer your question, but it's interesting that once they qualify for a pension, they leave. That affects our ability to advance a greater cohort of women into the executive and senior executive ranks.

Putting that aside for a second and going back to your question, in terms of accommodating families, that's where our concentration is now. In large urban centres where we have a sizeable representation, that's not a problem. We—at least I and the senior executive—are moving towards a more innovative approach to HR. For example, job sharing has been something which women have raised with me, and we're completely open to it. We need to get the mechanics and the practical arrangements done, but the authorities are all there and the support from senior management is there.

The challenge is in the more remote areas. We police, I think, 78% of the geographic land mass of Canada, and in some very remote circumstances. In terms of our postings and our policies around postings, it presents a challenge. We'll have a two-person detachment, and it can be very difficult for families.

We're completely open to innovative approaches. Do we need more money for HR practices? Yes, we absolutely do. We are embarking on our review—the minister referred to it briefly—of our funding demands, and it is being put out to contract as we speak. That will provide an opportunity for the government to understand how to rightsize the RCMP.

Ms. Pam Damoff: I suspect that in remote areas, getting the right people, whether they're men or women, is a challenge because of those families.

Commr Bob Paulson: Right.

Ms. Pam Damoff: So you're really limiting who is able to take those postings because it would only be certain people with certain family situations who could do that.

Commr Bob Paulson: Right.

Ms. Pam Damoff: Okay, thank you. I think that's my time.

The Chair: That's your time, and that will end our questioning.

I have three questions for the committee members.

You have in front of you the list of the 12 requests regarding voting on the supplementary estimates. Do I have unanimous consent that we will agree to them as they are stated, or would you prefer to vote on them one at a time?

Some hon. members: Agreed.

The Chair: It's okay to accept them. Are they accepted then unanimously?

An hon. member: On division.

CANADA BORDER SERVICES AGENCY
Vote 1c—Operating expenditures.....$43,936,130
Vote 5c—Capital expenditures.....$8,960,703

(Votes 1c and 5c agreed to on division)

CANADIAN SECURITY INTELLIGENCE SERVICE
Vote 1c—Program expenditures.....$1

(Vote 1c agreed to on division)

CORRECTIONAL SERVICE OF CANADA
Vote 1c—Operating expenditures, grants and contributions.....$1,788,446
Vote 5c—Capital expenditures.....$2,311,554

(Votes 1c and 5c agreed to on division)

PAROLE BOARD OF CANADA
Vote 1c—Program expenditures $299,150

(Vote 1c agreed to on division)

PUBLIC SAFETY AND EMERGENCY PREPAREDNESS
Vote 1c—Operating expenditures.....$1
Vote 5c—Grants and contributions.....$1

(Votes 1c and 5c agreed to on division)

ROYAL CANADIAN MOUNTED POLICE
Vote 1c—Operating expenditures.....$71,330,241
Vote 5c—Capital expenditures.....$26,020,296
Vote 10c—Grants and contributions.....$6,600,000

(Votes 1c, 5c and 10c agreed to on division)

SECURITY INTELLIGENCE REVIEW COMMITTEE
Vote 1c—Program expenditures.....$270,262

(Vote 1c agreed to on division)

The Chair: The second question is, shall I report the supplementary estimates (C) 2015-16 to the House?

Some hon. members: Agreed.

The Chair: The third question—I was waiting until one of the members requested this—is with respect to lunch. I believe in public disclosure on this. We have not been serving lunch to the committee, even though we are over the lunch hour, and I just wanted....

Is there general agreement that we should have sandwiches and soup available over the lunch hour? Is there unanimous consent for this? Are we all agreed?

Some hon. members: Agreed.

The Chair: I think that is all the business. I'll just remind the committee that we will begin our study on PTSD/OSI on Thursday. We'll have a brief agenda committee meeting before then to go over the witnesses beyond Thursday.

The meeting is adjourned.

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

Published under the authority of the Speaker of the House of Commons

Publié en conformité de l'autorité du Président de la Chambre des communes

SPEAKER'S PERMISSION

Reproduction of the proceedings of the House of Commons and its Committees, in whole or in part and in any medium, is hereby permitted provided that the reproduction is accurate and is not presented as official. This permission does not extend to reproduction, distribution or use for commercial purpose of financial gain. Reproduction or use outside this permission or without authorization may be treated as copyright infringement in accordance with the *Copyright Act*. Authorization may be obtained on written application to the Office of the Speaker of the House of Commons.

Reproduction in accordance with this permission does not constitute publication under the authority of the House of Commons. The absolute privilege that applies to the proceedings of the House of Commons does not extend to these permitted reproductions. Where a reproduction includes briefs to a Committee of the House of Commons, authorization for reproduction may be required from the authors in accordance with the *Copyright Act*.

Nothing in this permission abrogates or derogates from the privileges, powers, immunities and rights of the House of Commons and its Committees. For greater certainty, this permission does not affect the prohibition against impeaching or questioning the proceedings of the House of Commons in courts or otherwise. The House of Commons retains the right and privilege to find users in contempt of Parliament if a reproduction or use is not in accordance with this permission.

Also available on the Parliament of Canada Web Site at the following address: http://www.parl.gc.ca

PERMISSION DU PRÉSIDENT

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante : http://www.parl.gc.ca

House of Commons Standing Committee on Public Safety and National Security (SECU)

GOVERNMENT MEMBERS

Liberal Party of Canada



Pam Damoff
(Oakville North - Burlington, Ontario)
- First–Time MP



Nicola Di Iorio
(Saint-Léonard — Saint-Michel, Quebec)
- First-Time MP



Nathaniel Erskine-Smith
(Beaches – East York, Ontario)
- First–Time MP



Marco Mendicino
(Eglinton – Lawrence, Ontario)
- First-Time MP
- Federal prosecutor against organized crime and terrorism



Robert Oliphant
(Don Valley West, Ontario)
- MP From 2008 – 2011
- Returning MP in 2015



Ben Spengemann
(Mississauga – Lakeshore, Ontario)
- First-Time MP
- Served as a senior United Nations official in Iraq - led a team of experts in support of the Iraqi Parliament

OPPOSITION MEMBERS

Conservative Party of Canada



Larry Miller
(Bruce-Grey-Owen Sound, Ontario)
- MP Since 2004



Erin O'Toole
(Durham, Ontario)
- **Public Safety Critic for the Conservative Party**
- MP Since 2012
- Former RCAF – conducted search and rescue operations



Alain Rayes
(Richmond - Arthabaska, Quebec)
- **Public Safety Deputy Critic for the Conservative Party**
- First-Time MP

NDP



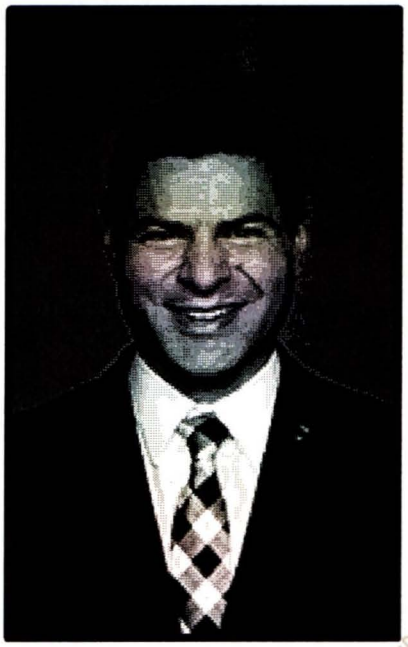
Matthew Dubé
(Beloeil — Chambly, Quebec)
- Deputy NDP House Leader
- MP Since 2011

RDIMS #1745867

PROCESSED BY CSIS UNDER THE PROVISIONS OF THE PRIVACY ACT AND / OR ACCESS TO INFORMATION ACT.
RÉVISÉ PAR LE SCRS EN VERTU DE LA LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET / OU DE LA LOI SUR L'ACCÈS À L'INFORMATION

House of Commons Standing Committee on
Public Safety and National Security (SECU)

Conservative Party of Canada



PUBLIC SAFETY DEPUTY CRITIC

Name: **Alain Rayes**
Riding: **Richmond – Arthabaska, Quebec**

Parliamentary Experience:

- New MP

Activities/Experience of Interest to the Portfolio:

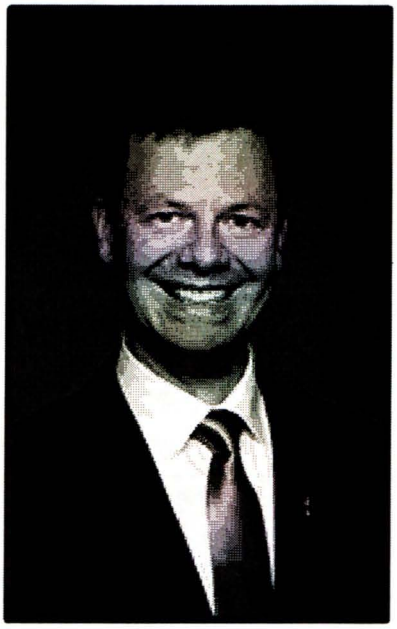
- Member of SECU (February 2016 -)

Biography not available at this time.

Updated February 2016

House of Commons Standing Committee on
Public Safety and National Security (SECU)

Liberal Party of Canada



Name: **Ben Spengemenn**
Riding: **Mississauga – Lakeshore, Ontario**

Parliamentary Experience:

- New MP

Activities/Experience of Interest to the Portfolio:

- Served as a senior United Nations official in Iraq - led a team of experts in support of the Iraqi Parliament
- Worked for PCO

Sven Spengemann was born in Berlin, Germany, and moved to Canada with his family at age 14. He particularly enjoys working with young people who are embarking on their career path and is an active member of the community of Mississauga-Lakeshore. He volunteers at the Compass Food Bank and serves on the Board of Directors of United Way of Peel Region and the UTM Alumni Association. Sven is also an Advisor to the Peel Multicultural Council.

Sven's academic qualifications include degrees from the University of Toronto (Mississauga), Osgoode Hall Law School and the Collège d'Europe. He was a Canada-US Fulbright Scholar and earned his doctorate at Harvard Law School.

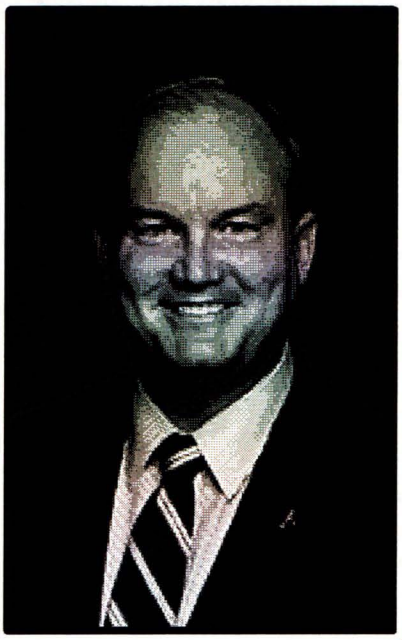
Sven's professional experience spans the private sector, academia, government and international affairs. He served as a senior United Nations official in Iraq, where he led a team of experts in support of the Iraqi Parliament. Sven also worked for a major Canadian bank and in the Privy Council Office in Ottawa. He held affiliations at the Munk School of Global Affairs, the Balsillie School of International Affairs and the Glendon School of Public & International Affairs.

In his spare time, he is an avid mountaineer, motorcyclist and private pilot.

Updated February 2016

House of Commons Standing Committee on Public Safety and National Security (SECU)

Conservative Party of Canada



PUBLIC SAFETY CRITIC

Name: **Erin O'Toole**
Riding: Bruce-Grey-Owen Sound, Ontario

Parliamentary Experience:

- MP since 2012

Activities/Experience of Interest to the Portfolio:

- Former RCAF – conducted search and rescue operations

Erin was raised in Port Perry and Bowmanville. He joined the Canadian Forces, and subsequently graduated from the Royal Military College (RMC) in 1995 with an Honours Bachelor of Arts degree and was commissioned as an officer in the Royal Canadian Air Force. He served briefly at CFB Trenton working as an assistant controller at the Rescue Coordination Centre, and was then posted to Winnipeg, Manitoba where he received his wings in 1996 before choosing to fly on the Sea King Helicopter as a Tactical Navigator. During his time at 423 Squadron in Shearwater, Nova Scotia, Erin participated in operations related to the crash of Swiss AirFlight 111 when he received a Sikorsky Helicopter Rescue Award following his crew's successful rescue of an injured fisherman at sea. He was subsequently promoted to the rank of Captain.

Following his completion of service in the regular forces, Erin transferred to the reserves to attend law school at Dalhousie University. Erin returned to Ontario to practice law in 2003, and retired formally from the Canadian Forces, receiving the Canadian Forces Decoration for 12 years of faithful service to his country.

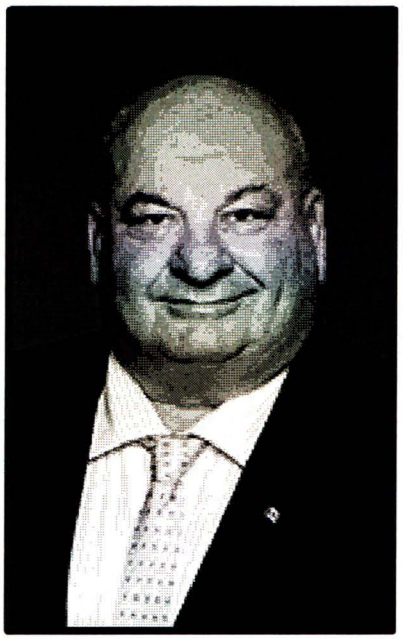
Erin has been an active organizer and supporter of many charitable causes. He was the co-chair of the River Runs Through Us Gala, which through a dinner and online campaign raised over $100,000 for the Valleys 2000 fish passage project on Bowmanville Creek. Erin serves as one of the Rotary Club organizers of the Clarington Youth & Community Leadership Dinner, which for the last few years has recognized local youth leaders at a dinner that also raises funds for the building of a school in Africa for the Michael "Pinball" Clemons Foundation and Free the Children. Erin also remains very active in causes related to veterans and connecting Canadians with their military. He is a Director and one of the founders of the True Patriot Love Foundation, which since 2009 has raised over $10 million for programs supporting members of the military, veterans and their families. Erin also serves on the Board of Governors of the Royal Military College of Canada. For his work with veterans and the Canadian Forces, Erin was awarded a Diamond Jubilee medal in 2012.

Erin lives in Courtice (Clarington) with his wife Rebecca and their children, Mollie and Jack.

Updated February 2016

House of Commons Standing Committee on Public Safety and National Security (SECU)

Conservative Party of Canada



FIRST VICE-CHAIR

Name: **Larry Miller**
Riding: Bruce-Grey-Owen Sound, Ontario

Parliamentary Experience:

- MP since 2004

Activities/Experience of Interest to the Portfolio:

- Member of SECU (January 2016 -)

Larry Miller has been serving as the Member of Parliament for Bruce-Grey-Owen Sound for four consecutive terms. Some of the issues he has been involved with include: health care, seniors, agriculture, ending the long-gun registry, protecting Canada's water and ensuring Federal funding reaches programs and organizations in Bruce and Grey counties.

Larry has been a part of many House of Commons Committees during his time in Ottawa. He sat as a Government Representative on the Standing Committee on Agriculture and Agri-Food from 2004-2012 and was Chair of this committee from 2008 to September of 2012. Larry was also a member of the Standing Committee on International Trade from 2006-2008. In September of 2012 Larry was elected as Chair of the Standing Committee on Transport Infrastructure and Communities and was re-elected as Chair of this committee in February of 2014.

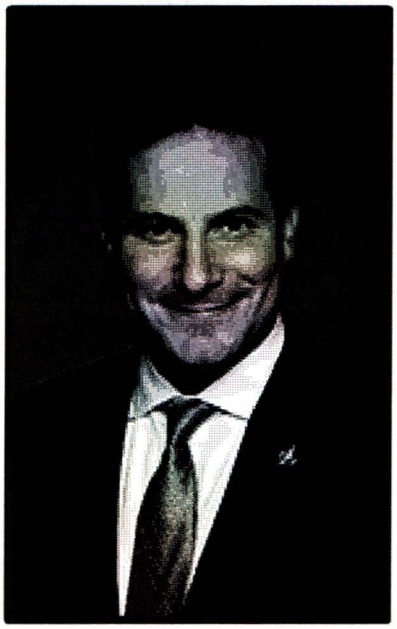
Larry has presented many petitions on behalf on his constituents and has also taken a lead role on two very important pieces of legislation. In the 39th session of Parliament, he sponsored Bill S-215: An Act to Protect Heritage Lighthouses, which received Royal Assent on May 29th, 2008. Larry has also successfully passed a Private Members Bill, Bill C-383: The Transboundary Waters Protection Act, which received Royal Assent on June 19th, 2013. This bill will ensure that all waters under Federal jurisdiction will be protected from bulk export while complementing Provincial regulations that are already in place.

Prior to entering Federal politics, Larry ran a beef farming operation and spent 13 years in Municipal politics. He represented the people of Georgian Bluffs and Grey County as a Municipal Councilor, Reeve, and Mayor as well as Warden of Grey County in 2002. He also chaired the Highways Committee and the Finance and Personnel Committee.

Updated February 2016

House of Commons Standing Committee on Public Safety and National Security (SECU)

Liberal Party of Canada



Name: **Marco Mendicino**
Riding: **Eglinton – Lawrence, Ontario**

Parliamentary Experience:

- New MP

Activities/Experience of Interest to the Portfolio:

- Member of SECU (February 2016 -)
- Federal prosecutor against organized crime and terrorism

A lawyer and family man with deep roots in Eglinton – Lawrence, Marco Mendicino has dedicated his career to keeping our communities safe. As a federal prosecutor for nearly a decade, he fought against organized crime and terrorism. Marco was also the president of a national association representing nearly 3,000 federal prosecutors and Government of Canada lawyers. While in this position, he testified before the House of Commons and Senate to advocate for better laws and access to justice.

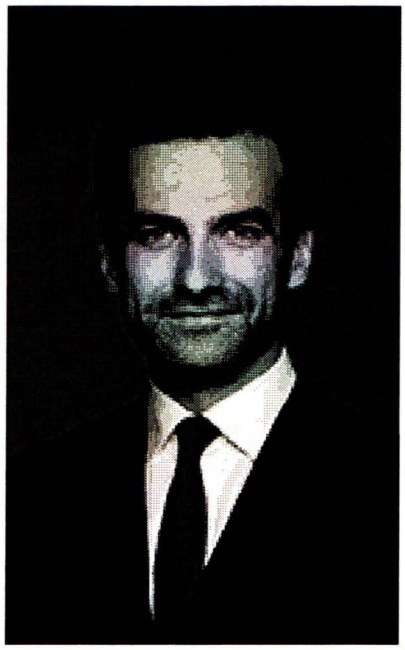
An avid community organizer, Marco is committed to improving education and has worked on local school initiatives, like rolling out lunch programs for full-day kindergarten and improving outdoor facilities. He dedicates his time to the John Wanless Childcare Centre, North Toronto Soccer Club and COSTI Immigration Services – an organization that helps immigrants acquire the educational, social and economic skills they need on arriving in Canada.

Marco runs his own law practice, focusing on regulatory, and labour and employment matters. He is adjunct professor at Osgoode Hall Law School, a small business owner and soccer coach to his daughters' teams. Marco and his wife Diana are long-time residents of Eglinton-Lawrence, raising their two daughters in the riding.

Updated February 2016

House of Commons Standing Committee on
Public Safety and National Security (SECU)

New Democratic Party of Canada



SECOND VICE-CHAIR

Name: **Matthew Dubé**
Riding: **Beloeil – Chambly, Quebec**

Parliamentary Experience:

- MP Since 2011

Activities/Experience of Interest to the Portfolio:

- Deputy NDP House Leader

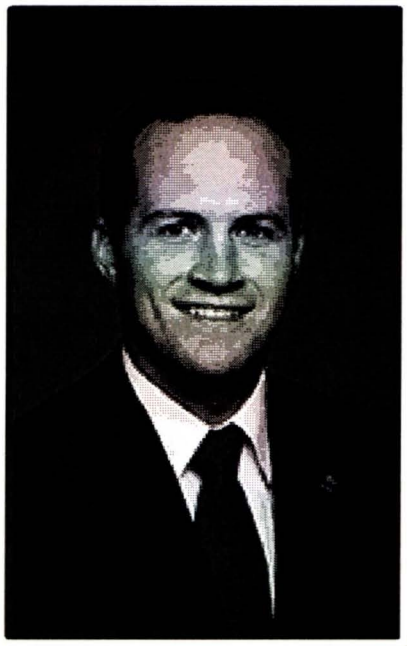
As Member of Parliament since May 2011, Matthew Dubé has served as the NDP critic for Sports and Youth

Matthew obtained his Bachelor of Arts degree in Political Science and History from McGill University. Since 2011, he has defended the interests of his constituents and advanced a number of important local issues, including rail safety, development of the Richelieu River and recognition of the value of Fort Chambly.

Updated February 2016

House of Commons Standing Committee on
Public Safety and National Security (SECU)

Liberal Party of Canada



Name: **Nathaniel Erskine-Smith**
Riding: **Beaches – East York, Ontario**

Parliamentary Experience:

- New MP

Activities/Experience of Interest to the Portfolio:

- Member of SECU (February 2016 -)

A litigation lawyer, born and raised in Beaches – East York, Nathaniel Erskine-Smith understands that his community deserves honest and respectful representation and he is dedicated to being a strong voice in Ottawa for all of its residents.

Nathaniel previously practised commercial litigation in downtown Toronto. He obtained both his B.A. and J.D. from Queen's University and his Master of Laws (B.C.L.), with distinction, at the University of Oxford, where he studied political philosophy and constitutional law.

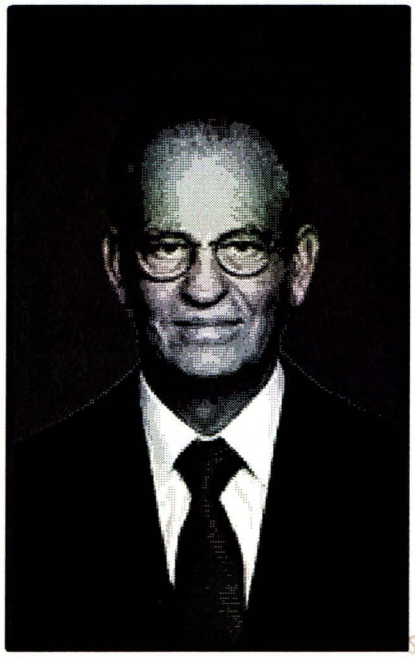
Committed to public service, Nathaniel is active in his community, and he regularly provided pro bono legal services to a range of clients and causes. He previously volunteered with the Canadian Civil Liberties Association, and he has fought public interest matters before the Divisional Court and the Ontario Human Rights Tribunal.

An avid baseball fan, Nathaniel pitched for the baseball teams at Queen's University, the University of Oxford, and the City of Oxford. He lives in Beaches – East York with his wife Amy Symington, a nutrition professor and chef at George Brown College.

Updated February 2016

House of Commons Standing Committee on
Public Safety and National Security (SECU)

Liberal Party of Canada



Name: **Nicola Di Iorio**
Riding: **Saint-Léonard — Saint-Michel, Quebec**

Parliamentary Experience:

- New MP

Activities/Experience of Interest to the Portfolio:

- Member of SECU (February 2016 -)

A lawyer specializing in labour and employment law, Nicola Di Iorio is a partner at the national firm Langlois Kronström Desjardins. He has gained both recognition and respect through his 32 years of practice, repeatedly ranking among lawyers most frequently recommended by their peers in the annual survey by Lexpert Magazine. Nicola was also recognized as one of Canada's leading labour and employment law experts in the 2014 edition of The Best Lawyers in Canada. A well-known guest speaker, Nicola teaches at McGill University and the professional training school of the Barreau du Québec.

Always with the best interests of others at heart, Nicola co-founded Cool Taxi – a prepaid taxi coupon initiative that provides people with a safe way home. The initiative earned him a nomination for the 2015 Person of the Year award of the Chamber of Commerce and Industry of Saint-Laurent–Mount Royal. Nicola is the Secretary of the Board of Centro Leonardo da Vinci – an organization that he co-founded – and Secretary of the Board of the Italian-Canadian Community Foundation of Quebec.

Nicola holds an LLB from Université de Sherbrooke and an LLM from Columbia University and has co-authored two works entitled Les normes du travail.

Updated February 2016

House of Commons Standing Committee on
Public Safety and National Security (SECU)

Liberal Party of Canada



Name: **Pam Damoff**
Riding: **Oakville North – Burlington, ON**

Parliamentary Experience:

- New MP

Activities/Experience of Interest to the Portfolio:

- Member of SECU (February 2016 -)

Pam Damoff is a business professional and community activist who has served as a town councillor in Oakville since 2010. Her extensive public service, combined with over 27 years of corporate experience on Bay Street, provides a solid background to represent Oakville North-Burlington in Ottawa.

Working hard to ensure her community's sustainability for future generations, Pam is an ardent advocate for preserving greenspace and a healthy, active lifestyle. She co- founded Cycle Oakville to promote cycling and improved cycling infrastructure and received the 2013 Bicycling Leadership Award for her tireless promotion of cycling in Ontario.

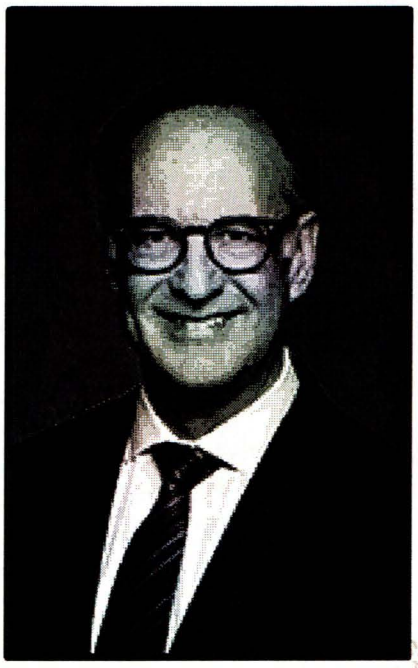
Pam is an active volunteer in her community; she is Chair of the Oakville Santa Claus Parade and Terry Fox Run, and a member of the organizing committee of the Courage Polar Bear Dip. She also volunteers countless hours with many local charities and community groups.

Pam was the proud recipient of the Queen Elizabeth II Diamond Jubilee medal and Paul Harris Fellow Award for her community service and the Top 40 Fabulous Women Over 40 Excellence Award for Community Leadership. She earned a Bachelor of Arts degree from the University of Western Ontario. Pam lives in Oakville and has one grown son.

Updated February 2016

House of Commons Standing Committee on Public Safety and National Security (SECU)

Liberal Party of Canada



CHAIR

Name: **Robert Oliphant**
Riding: **Don Valley West, Ontario**

Parliamentary Experience:

- MP From 2008 – 2011
- Returning MP in 2015

Activities/Experience of Interest to the Portfolio:

- Former Member of SECU (Jan – Dec 2009)

Rob Oliphant is the former President and CEO of the Asthma Society of Canada, a national health charity and patient organization. He is a community leader with a long history of advocating for poverty reduction, affordable housing, at-risk youth, and seniors' economic security. Much of this advocacy has been through his work as an Ordained Minister of the United Church of Canada, an organization he has served and represented in several provinces and territories across Canada, including almost ten years as a Senior Minister at Eglinton St. George's United Church in Toronto.

Rob is a founding member of Affirm Canada, an organization that has advocated on behalf of members of the LGBTTQ community since 1982. He was also the founding chairperson of Neighbourhood Interfaith Group, which seeks to promote Christian-Jewish-Muslim dialogue. Currently, Rob is the President of the Global Allergy and Asthma Patient Platform and serves on the Governing Council of the Health Charities Coalition of Canada. In 2013, he was awarded the Queen's Diamond Jubilee Medal in recognition of his contributions to Canada.

From 2008 to 2011, Rob was the Member of Parliament for Don Valley West, and served as the Opposition Critic for Veterans Affairs and Multiculturalism. He holds a Bachelor of Commerce from the University of Toronto, a Master of Divinity from the Vancouver School of Theology at the University of British Columbia, and a Doctor of Ministry from the Chicago Theological Seminary at the University of Chicago.

Updated February 2016