MEETING OF THE
DEPUTY MINISTERS' NATIONAL SECURITY COMMITTEE

December 15, 2014
Time: 3:00 p.m. to 5:00 p.m.
Location:

TABLE OF CONTENTS

TAB 1 Agenda
TAB 2 Record of Decision
TAB 3
TAB 4
TAB 5
MEETING OF THE
DEPUTY MINISTERS' NATIONAL SECURITY COMMITTEE

October 15, 2014
Time: 3:00 p.m. to 5:00 p.m.
Location:

AGENDA

1.
2.
3. Other Business

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.

REVÊTE 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.
MEETING OF THE
DEPUTY MINISTERS’ NATIONAL SECURITY COMMITTEE

May 5, 2014
From: 3:30 p.m. to 5:30 p.m.
Room:

Record of Decision

List of Participants

| Stephen Rigby, Chair          | Greta Bossermaier, as acting DM CIDA          |
| Anita Biguzs, CIC              | Jeff Yaworski, for Michel Coulombe, CSIS      |
| Richard Fadden, DND            | John Ossowsk, for François Guimont, PS        |
| Liseanne Forand                | Martin Bolduc, for Luc Portelance, CBSA       |
| John Forster, CSEC             | Christine Hogan, PCO                          |
| Don Head, SCS                  | Brigitte Diogo for David Vigneault, PCO       |
| Daniel Jean, DFATD             | Dave Cochrane, PCO (Item 1 only)              |
| John Knubley                   |                                               |
| Louis Lévesque, TC             |                                               |

Notetaker: Alan Hamson
Presentation to the
Deputy Ministers' Committee on National Security

October 15, 2014
Overview

1. Context
2.
3.
4. Managing these issues
5. Discussion
Placeholder: Slide 10
Discussion

- Are our posture and organization sufficient to manage these issues?
- What should be our next steps?
MEMORANDUM TO THE DIRECTOR

MEETING OF THE DEPUTY MINISTERS’ COMMITTEE ON CYBER SECURITY

10:00 — 11:30
Wednesday, 24 September 2014
269 Laurier Avenue West, 19th Floor Boardroom

The following items may be discussed, as per the agenda (TAB 1):

1. International Internet Foreign Policy and Internet Governance; and,
2. Recent Cyber Developments

BACKGROUND

The last meeting of the Deputy Ministers’ Committee on Cyber Security took place on 5 June. The meeting included an update on the Government-wide Secret Network by Shared Services Canada, a Treasury Board Secretariat overview of the Government IT Incident Management Strategy and a discussion of recent cyber security developments led by Public Safety Canada.

AGENDA ITEM 1 – INTERNATIONAL INTERNET FOREIGN POLICY AND INTERNET GOVERNANCE

The Deputy Ministers of Foreign Affairs and Industry will present a deck on cyber foreign policy, internet governance and related economic opportunities for Canada through engagement in international fora.

To address these concerns, DFATD is developing a policy response to guide coordinated efforts in
upcoming international meetings.

The Deputy Minister of Industry will speak to the economic benefits to Canada of its support for an open, robust and global internet.

While the file continues to be an important policy avenue for the Government of Canada, StratPol will continue to maintain visibility on the file through engagement with DFATD.

AGENDA ITEM 2 – RECENT CYBER SECURITY DEVELOPMENTS

Public Safety will provide a deck (TAB 3) to facilitate a structured roundtable discussion of recent developments in cyber, including upcoming events.

Operational Updates
As part of the presentation, Public Safety will provide an update on recent operational cyber developments. To facilitate your participation, the Cyber Centre has provided the following snapshot on cyber activity in Canada in recent months:

National Research Council (NRC) Cyber Incident
- **TAB 1**: Agenda, Deputy Ministers' Committee on Cyber Security, 24 September June (Public Safety)
- **TAB 2**: Deck, "Promoting a free, open, and secure Internet" (DFATD)
- **TAB 3**: Deck, "Recent Cyber Developments" (Public Safety)
Deputy Ministers Committee on Cyber Security

September 24, 2014 – 10:00 to 11:30 a.m.
19th floor, Executive Boardroom, 269 Laurier Avenue West

AGENDA

<table>
<thead>
<tr>
<th>Time</th>
<th>Item</th>
<th>Associated Documentation</th>
</tr>
</thead>
</table>
| 1. 9:00-9:05 (5 mins) | Opening Remarks  
François Guimont, Deputy Minister  
Public Safety Canada |
| 2. 9:05-10:10 (65 mins) | International Internet Foreign Policy and Internet Governance  
Daniel Jean, Deputy Minister, Department of Foreign Affairs, Trade and Development  
John Knubley, Deputy Minister, Industry Canada |
|            | For discussion: A presentation on cyber foreign policy and response to international cyber developments, complemented by a presentation on Internet governance and economic implications.  
A discussion will follow. |
| 3. 10:10-10:25 (15 mins) | Recent Cyber Developments  
Lynda Clarmont, Senior Assistant Deputy Minister  
Public Safety Canada |
|            | For information: Review of cyber-related developments and events from across Government |
| 4. 10:25-10:30 (5 mins) | Roundtable | N/A |

Documents will be distributed prior to or at the meeting.

The deck will be distributed prior to or at the meeting.
MEMORANDUM TO THE DIRECTOR

TECHNICAL BRIEFING FOR PARLIAMENTARIANS ON BILL C-44

15:30-17:00
Thursday, 30 October 2014
Justice Building, Parliamentary Precinct, Vittoria Street
Office of Parliamentary Secretary, Room 302

You have been invited to appear before the House of Commons on 2014 10 30 to provide a technical briefing on Bill C-44 (The Protection of Canada from Terrorists Act) to Parliamentarians.

You will be accompanied by Ritu Banerjee, Director, Intelligence Policy (PS) and Nathalie Benoit (DLS).

BACKGROUND:

The proposed amendments will:
- Confirm CSIS's authority to conduct investigations outside of Canada;
- Confirm that the Federal Court can issue warrants for CSIS to investigate threats to national security outside of Canada;
- Give the Federal Court authority to operate within the scope of relevant Canadian law when issuing warrants to authorize CSIS to undertake certain activities to investigate a threat to the security of Canada outside of Canada;
- Protect the identity of CSIS human sources from disclosure in court proceedings; and
- Protect the identity of CSIS employees who may engage in covert activities in the future.

The proposed amendments will not:
- Directly impact information-sharing with partners;
- Change the mandate of CSIS.
INFORMATION SHARING:

Media reports have linked the amendments to increased information sharing between CSIS and partners. The proposed amendments do not directly impact information sharing and the Bill contains no amendments to s.17 of the CSIS Act. However, the amendments clarify CSIS’ authority to operate outside of Canada and the Federal Court’s authority to issue warrants without regard to the laws of any foreign state. In so doing, they clarify CSIS’ authority in relation to matters where CSIS may operate independently or cooperate with allies abroad, or seek assistance from CSEC in warranted collection on targets abroad. Thus, while the proposed amendments do not impact CSIS’ authority to cooperate with foreign states they can only have a positive effect on our ability to cooperate with partners.

RELATIONSHIP WITH CITIZENSHIP ACT AMENDMENTS:

The CSIS Act amendments and the Strengthening Canadian Citizenship Act (SCCA) amendments are two distinct and separate elements of the bill. The Citizenship Act amendments will facilitate expedited entry into force of the citizenship revocation elements of Bill C-24, which received Royal Assent in the spring.

KEY MESSAGES (UNCLASSIFIED):

- The objective of the Bill is to respond to gaps created by recent judicial decisions by amending the CSIS Act to confirm CSIS’ ability to effectively investigate threats outside of Canada, and the Federal Court’s jurisdiction to issue warrants for collection abroad. The amendments will also provide protection for the identities of CSIS human sources and employees who are likely to engage in covert activities.
- The amendments do not change the Service’s mandate in any way, nor do they make the Service a foreign intelligence agency. Foreign intelligence collection remains limited to collection within Canada, and on the written request of the Minister of Foreign Affairs or the Minister of National Defence, per s.16 of the Act.
- Recent Court decisions created significant uncertainty with regard to CSIS’ investigative activities outside Canada, to the detriment of priority national security investigations. As the most recent court decision has not yet been made public, I cannot speak to the details of that decision.
- The CSIS Act amendments are not in any way intended to facilitate revocation of citizenship.

INFORMATION SHARING

- Cooperation with partners is an essential part of CSIS’ intelligence collection and, without the benefits of such cooperation,
-3-

- Clarification of the Service’s authority to act outside Canada in fulfilling its duties and functions under s.12 and s.15 of the Act can only strengthen its ability to cooperate with partners.

- The Service’s authority to cooperate with foreign partners flows from s.17 of the Act, which is not amended by Bill C-44.

As always, please do not hesitate to contact me should you require further information.

Enclosures:

TAB A: Bill C-44
TAB B: Senate Committee Note on Amendments to the CSIS Act (prior to introduction)
TAB C: Clause-by-Clause Analysis of Bill C-44
TAB D: Banff Press Event Q&A
COMMITTEE NOTE – AMENDMENTS TO THE CSIS ACT

- All of CSIS' activities are conducted in accordance with Canadian law, including the Privacy Act and Charter of Rights and Freedoms, and are subject to full and complete review by SIRC. This Bill will not change that in any way.

- Rather, this bill clarifies elements of CSIS' mandate and sets the conditions to fill serious gaps in our operational framework.

- I understand the key provisions of the bill would:
  - Confirm CSIS' legal authority to conduct investigations within or outside Canada;
  - Confirm the Federal Court's ability to issue warrants for CSIS' international activities;
  - Clarify that the Federal Court can issue warrants for CSIS activities abroad without regard to any other law, including that of a foreign state;
  - With few exceptions, prohibit the disclosure of the identity of a CSIS human source in court and administrative proceedings; and,
  - Protect the identity of CSIS employees who may engage in covert activities in the future.

- These amendments are important to ensuring CSIS remains able to investigate threats to our national security, in particular the threat posed by terrorist travelers abroad and here at home.
BILL C-44

An Act to amend the Canadian Security Intelligence Service Act and to make a consequential amendment to another Act

Clause by Clause Analysis
An Act to amend the Canadian Security Intelligence Service Act and to make a consequential amendment to another Act

Loi modifiant la Loi sur le Service canadien du renseignement de sécurité et modifiant une autre loi en conséquence

Clause by Clause Analysis / Analyse article par article

INTERPRETATION / INTERPRÉTATION

CLAUSE 1

Analysis

The short title of the Act is the Protection of Canadians from Terrorists Act.
AN ACT TO AMEND THE CANADIAN SECURITY INTELLIGENCE SERVICE ACT AND TO MAKE A CONSEQUENTIAL AMENDMENT TO ANOTHER ACT

Loi modifiant la Loi sur le Service canadien du renseignement de sécurité et modifiant une autre loi en conséquence

Clause by Clause Analysis / Analyse article par article

INTERPRETATION / INTERPRÉTATION

CLAUSE 2

Analysis

This clause defines "human source", a term which is used in the new section 18.1 (clause 7 of this Bill). In particular, the definition limits the scope of the protection created in section 18.1 to those who have received a promise of confidentiality.
INTERPRETATION / INTERPRÉTATION

CLAUSE 3
Analysis

This clause adds a new section 12(2) to the Act that would specify that duties and functions performed by CSIS pursuant to section 12 of the Act may be performed within or outside Canada. Section 12(1) will maintain the original language of section 12 which authorizes CSIS to collect, analyse and retain information and intelligence respecting activities that may constitute threats to the security of Canada, and to report or advise the Government of Canada.

Note that there is currently no geographic limit on section 12, and CSIS can therefore already perform these duties and functions within or outside of Canada. This addition merely makes this fact explicit in the Act for greater certainty.

ARTICLE 3
Analyse

Cet article ajoute un nouveau paragraphe 12(2) à la Loi précisant que les fonctions du SCRS en vertu de l’article 12 de la Loi peuvent être exercées à l’extérieur du Canada. Le paragraphe 12(1) n’altère pas la version originale de l’article 12, qui autorise le SCRS à recueillir, à analyser et à conserver les informations et renseignements sur les activités qui pourraient constituer des menaces envers la sécurité du Canada, et à en faire rapport au gouvernement du Canada ou à le conseiller à cet égard.

L’article 12 n’a jamais contenu de limites géographiques et le SCRS exerce déjà ces fonctions même l’extérieur du Canada. Cet ajout ne fait que rendre ce fait explicite dans la Loi par souci de précision.
An Act to amend the Canadian Security Intelligence Service Act and to make a consequent
amendment to another Act
Loi modifiant la Loi sur le Service canadien du renseignement de sécurité et modifiant une autre loi en
conséquence
Clause by Clause Analysis / Analyse article par article

INTERPRETATION/INTERPRÉTATION

CLAUSE 4

Analysis

This clause adds a new section 15(2) to the Act
that would specify that duties and functions
performed by CSIS pursuant to section 15 of the
Act may be performed within or outside Canada.
Section 15(1) will maintain the original language
of section 15 which authorizes the CSIS to
conduct investigations for the purposes of
providing security assessments or advice
pursuant to the Citizenship Act or the
Immigration and Refugee Protection Act.

Note that there is currently no geographic limit
on section 15, and CSIS can therefore already
carry out investigations within or outside of
Canada. This addition merely makes this fact
explicit in the Act for greater certainty.

ARTICLE 4

Analyse

Cet article ajoute un nouveau paragraphe 15(2) à
la Loi précisant que les fonctions du SCRS en
vertu de l'article 15 de la Loi peuvent être
exercées à l'extérieur du Canada. Le
paragraphe 15(1) n'altère pas la la version
originale de l'article 15, qui autorise le SCRS à
mener des enquêtes dans le but de fournir des
évaluations de sécurité ou des conseils en vertu
de la Loi sur la citoyenneté ou de la Loi sur
l'immigration et la protection des réfugiés.

L'article 15 n'a jamais contenu de limites
géographiques et le SCRS mène des enquêtes
même à l'extérieur du Canada. Cet ajout ne fait
que rendre ce fait explicite dans la Loi par souci
de précision.
INTERPRETATION/INTERPRÉTATION

CLAUSE 5

Analysis

This clause corrects two typographical errors in the French version of the Act.

Sub-Clause 5(1): Currently, section 16(2) makes reference to subsections 16 (1)b)(i), (ii), and (iii). These subsections exist in the English version of the Act, but do not exist in the French version of the Act, which uses a different format for section 16 (1)b). The proposed amendment would reformat subsection 16 (1)b) in the French version of the Act to make it consistent with the English version of the Act, thereby correcting the error in the French version of 16(2).

Sub-Clause 5(2): Currently, section 16(3)b) in the English version of the Act requires that the personal consent in writing of the Minister be obtained before the Service performs its duties and functions under subsection 16(1). However, the French version of the Act does not stipulate that this consent be in writing (note that CSIS has always followed the more restrictive English requirement and obtained such consent in writing). The proposed amendment would add the word “écrit” to the French version of the Act, so that both versions would be consistent.

Sous-article 5(1) : Actuellement, le paragraphe 16(2) renvoie aux sous-alinéas 16(1)b)(i), (ii) et (iii). Ces sous-alinéas existent dans la version anglaise de la Loi, mais pas dans la version française, puisque cette dernière utilise un format différent pour l’alinéa 16(1)b). La modification proposée vise à changer le format de l’alinéa 16(1)b) dans la version française de la Loi afin qu’il soit conforme à la version anglaise, corrigeant ainsi l’erreur qui s’est glissée au paragraphe 16(2) de la version française.

Sous-article 5(2) : Actuellement, l’alinéa 16(3)b) dans la version anglaise de la Loi stipule que le consentement personnel écrit du ministre est requis avant que le Service exercer ses fonctions en vertu du paragraphe 16(1). Toutefois, la version française de la Loi ne précise pas que le consentement doit être obtenu par écrit (veuillez prendre note que le SCRS a toujours respecté l’exigence la plus rigoureuse qui figure dans la version anglaise et qu’il a toujours obtenu un tel consentement par écrit). La modification proposée vise à ajouter le terme « écrit » dans la version française de la Loi afin que les deux versions soient uniformes.
CLAUSE 6

Analysis

Section 18(1) of the CSIS Act currently makes it an offence to disclose the identity of an employee who is or was engaged in covert operational activities of the Service. This clause amends section 18(1) to also make it an offence to disclose the identity of a CSIS employee likely to become engaged in covert operational activities of the Service.

The clause also adds the word “knowingly” to section 18(1), so that it is only an offence to knowingly disclose the information described in that section.

Finally, this clause would also remove the offence related to the disclosure of the identity of a confidential source that is currently described in section 18(1)(a). This will now be covered by the new section 18.1 (see clause 7).
A judge could also issue, if it is relevant to the proceeding, an order declaring:

- that the individual is not a human source or the information is not information from which the identity could be inferred. In this case, the prohibition would not apply, or
- in the prosecution of an offence, that the disclosure of the identity of information from which the identity could be inferred is essential to establishing the accused's innocence. In this case, the judge could declare that the identity and/or information is to be disclosed, subject to any conditions that the judge specifies.

The prohibition on disclosure would apply to any proceeding before a court, person or body with jurisdiction to compel the production of information.

This prohibition would replace the prohibition currently described in section 18(1)(a) of the Act.

The information could be disclosed in a proceeding when the human source and the Director of CSIS consent to the disclosure.

A judge could also issue, if it is relevant to the proceeding, an order declaring:

- that the individual is not a human source or the information is not information from which the identity could be inferred. In this case, the prohibition would not apply, or
- in the prosecution of an offence, that the disclosure of the identity of information from which the identity could be inferred is essential to establishing the accused's innocence. In this case, the judge could declare that the identity and/or information is to be disclosed, subject to any conditions that the judge specifies.
An order authorizing disclosure can only take effect once the time provided to appeal the decision has expired. If the order is appealed and confirmed, until either the time provided to appeal the judgment confirming the order has expired or all rights of appeal have been exhausted.

The hearing of the application for such an order is to be held in private and in the absence of the applicant and their counsel, unless the judge decides otherwise. In any case, the judge must ensure the confidentiality of the identity and information from which the identity of the human source could be inferred, and information and other evidence provided if its disclosure would be injurious to national security or endanger the safety of any person. The same principles of confidentiality must be respected in the event that an appeal of the judge’s order is sought.

An order authorizing disclosure can only take effect once the time provided to appeal the decision has expired. If the order is appealed and confirmed, until either the time provided to appeal the judgment confirming the order has expired or all rights of appeal have been exhausted.
CLAUSE 8

Analysis

Sub-Clause 8(1): This clause would amend section 21(1) of the Act to clarify that warrants may be applied for to enable CSIS to investigate a threat to the security of Canada within or outside Canada.

Note that this would not apply to warrants required for the performance of CSIS' duties and functions under section 16 of the Act, which would remain limited to “within Canada”.

Sub-Clause 8(2): This clause would also create a new section 21(3.1), which would clarify that a judge may issue a warrants that would authorize activities outside of Canada, without regard to any other law, including that of a foreign state.

Sous-article 8(1) : Cet article modifie le paragraphe 21(1) de la Loi afin de confirmer que le SCRS peut demander à un juge de décerner un mandat, même à l'extérieur du Canada afin de lui permettre d'enquêter sur une menace envers la sécurité du Canada.

Veuillez prendre note que cette modification ne vise pas les demandes de mandats permettant l'exercice des fonctions du SCRS en vertu de l'article 16 de la Loi, qui demeurerait limité aux activités menées « dans les limites du Canada ».

Sous-article 8(2) : Cet article crée également un nouveau paragraphe 21(3.1) clarifiant qu'un juge peut décerner un mandat qui autorise des activités à l'extérieur du Canada, sans égard à toute autre règle de droit, notamment le droit de tout État étranger.
CLAUSE 9

Analysis

This clause modifies subsection 39(2) such that the new protection created by clause 6 does not apply to the Security Intelligence Review Committee. As such, the Committee would be entitled to have access to the information protected under that clause.

ARTICLE 9

Analysis

Cet article modifie le sous-alinea 39(2) de telle sorte que la nouvelle protection cree par l'article 6 ne s'applique pas au Comite de surveillance des activites de renseignement de securite. Il s'ensuit que le Comite aurait le droit d'avoir acces aux informations protegees par cet article.
CONFIDENCE OF THE QUEEN'S PRIVY COUNCIL

An Act to amend the Canadian Security Intelligence Service Act and to make a consequential amendment to another Act

Loi modifiant la Loi sur le Service canadien du renseignement de sécurité et modifiant une autre loi en conséquence

Clause by Clause Analysis / Analyse article par article

INTERPRETATION / INTERPRÉTATION

CLAUSE 10

Analysis

This clause amends Schedule II of the Access to Information Act by replacing the reference to “section 18” of the Canadian Security Intelligence Service Act to “sections 18 and 18.1”.

This consequential amendment is necessary because the protection of information related to human sources, currently addressed under section 18 of the Canadian Security Intelligence Services Act, will be addressed under section 18.1 as a result of the amendments made by clauses 6 and 7 of this Bill.

ARTICLE 10

Analyse

Cet article modifie l'Annexe II de la Loi sur l'accès à l'information par le remplacement de la référence à « article 18 » de la Loi sur le Service canadien du renseignement de sécurité par « articles 18 et 18.1 »

Cette modification correlative est nécessaire parce que la protection d'information relative aux sources humaines, traitée actuellement par l'article 18 de la Loi sur le Service canadien du renseignement de sécurité sera traitée par l'article 18.1 à la suite des modifications apportées par les articles 6 et 7 de ce projet de loi.
Questions on the Amendments:

Q: Why does the CSIS Act need to be amended?

- The CSIS Act came into force in 1984 when the primary threats to Canada's national security were of the Cold War era.
- Today's threats, chief among which is terrorism, are global in scope and far more diffuse.
- Technology has dramatically changed the way in which threats evolve and materialize, where social media and the internet enable widespread and often anonymous distribution of information.
- The CSIS Act must keep pace with change if the Service is to fulfill its duties and functions in effectively investigating threats to Canada's national security.

Q: Doesn't CSIS already operate abroad, for instance, weren't you present in Afghanistan?

- The Service has always had the authority to operate outside of Canada to investigate threats to national security.
- This authority is not, however, explicit in the current wording of the CSIS Act.
- Confirming this authority is consistent with the findings of the MacDonald Commission and the original intentions expressed by Parliament when the CSIS Act was passed.

Q: Why does CSIS need to be active abroad?

- The Canadian public expects and demands that CSIS take all necessary legal steps to ensure their safety and security. To do so, we must be positioned to identify and address threats to the security of Canada and Canadians, at home and abroad.
- It is critical that CSIS is able to track the movement of these targets and investigate threats to national security even beyond our borders.
- Threats to our security may come from within or outside Canada. Threat actors may depart Canada to participate in threat activities and return to Canada afterward.
• Terrorist threats, in particular, are global in scope and reach - terrorist travellers are mobile and highly connected, while plots against Canada can be directed from anywhere in the world.

Q: Do these amendments give CSIS a foreign intelligence mandate?

• In section 16 of the CSIS Act, CSIS is mandated to collect information on the capabilities, intentions or activities of foreign states WITHIN CANADA and at the direction of the Minister of National Defence or the Minister of Foreign Affairs.

• The proposed amendments will not affect the current parameters of this mandate.

Q: How can the public be certain that CSIS will operate lawfully abroad?

• All of CSIS' investigative activities, whether in Canada or abroad, are undertaken in accordance with its mandated authorities under the CSIS Act, the Charter of Rights and Freedoms, Ministerial Direction, and internal policy.

• When a threat is such that the Service must engage in more intrusive investigative measures, judicial authorization, with the consent of the Minister, is required.

• CSIS is subject to full review by the Security Intelligence Review Committee, which has access to all information held by the Service, with the exception of Cabinet confidences.

• CSIS' activities are always in compliance with Canadian law and values; its primary responsibility is to the safety and security of Canadians.

• The proposed amendments will not, in any way, reduce existing measures to oversee and review CSIS activities.

Q: What are human sources and why do they need protection?

• Human sources are individuals who provide invaluable information to CSIS on threat activities, often at significant personal risk.

• It is essential that the identities of human sources remain confidential to ensure their safety and security.

• Without these protections, human sources may cease cooperating with the Service.

Q: Aren't CSIS employees' identities already protected?

• The CSIS Act currently offers limited protections for the disclosure of employee identities.

• The safety and security of CSIS employees engaged in covert activities requires strong protections from disclosure of their identities.
Q: What will these amendments do to help CSIS investigate terrorist travellers?

- The conflicts in Iraq and Syria have become a magnet for global Sunni Islamist extremists, attracting not just Canadians, but individuals from all over the world.

- The number of radicalized Canadians traveling abroad has not fluctuated greatly over this past year and remains consistent with the numbers that have been widely reported (viz. 130-145 abroad, of which 50 in the region).

- I also 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.

- Investigating the activities of Canadians travelling for terrorist purposes is made difficult by a number of factors:
  - Individuals regularly depart Canada on false pretenses and travel to third countries to disguise their final destination.
  - Once abroad, individuals often adopt noms de guerre or online aliases to hide their identity.
  - Monitoring individuals in conflict zones and where there is frequent, undocumented movement across international borders is extremely difficult.

- In this context, cooperation and intelligence sharing with our partners – including those in the region – is of critical importance.

- When individuals travel from Canada to engage in threat-related activity, CSIS' investigative activities to respond to those threats cannot be limited to Canada's borders.

- Further, human sources provide valuable information on aspiring travellers or individuals already abroad, and their identities must be protected.

General Questions on Terrorist Travel

Q: What threat is posed to Canada by returnees?

- Extremists returning to Canada have the potential to pose a significant threat to our national security.

- Many returnees have the perceived credibility to encourage and recruit other individuals to go abroad or the knowledge and experience to plot terrorist related activities in Canada.

- Individuals' experiences vary widely, however: some never achieve their intent and simply return to Canada, while others return because of injury, lack of resources, or for personal reasons.

If pressed...

- CSIS is aware of a number of individuals currently in Canada who have previously travelled abroad – to a number of destinations – for a range of extremist purposes (viz. ~80 returnees).
• CSIS actively investigates individuals suspected of being engaged in threat-related activity. However, for reasons of national security, I am not at liberty to discuss specific investigations or the locations of individuals.

Q: What is CSIS doing to prevent terrorist travellers?

• As you know, CSIS is not an enforcement organization, but we work closely with Canadian partners who may be in a position to take action against such travelers.

• CSIS cannot detain or arrest people, nor do we issue or have the authority to seize travel documents.

• CSIS is supportive of the RCMP’s efforts to develop an early intervention program to address radicalization, including measures to raise awareness among affected communities.

If pressed on particular cases...

• Due to reasons of national security and privacy considerations, I cannot discuss the activities of specific individuals.

• I certainly sympathize with the families of radicalized individuals, especially those with children who are presumed to have been killed overseas.

• I would encourage all families and individuals who are concerned about radicalization to reach out to their local social service providers or law enforcement authorities.

• Every individual’s pathway of radicalization to violence is unique and the Service is conducting research to better understand this phenomenon in Canada.

Q: Is CSIS aware of particular mosques where radicalization is happening?

• CSIS does not investigate institutions and I cannot comment on specific mosques.

• According to section 2 of the CSIS Act, CSIS investigates individuals or groups who support the threat or use of violence for the purpose of achieving a religious, ideological or political objective.
## Comité des sous-ministres sur la cybersécurité

Le 24 septembre 2014 – de 10 h à 11 h 30
19e étage, Salle de conférence de la haute direction, 269, avenue Laurier Ouest

### ORDRE DU JOUR

<table>
<thead>
<tr>
<th>Heure</th>
<th>Point</th>
<th>Documents connexes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 9 h – 9 h 05</td>
<td>Mot de bienvenue</td>
<td>François Guimont, sous-ministre Sécurité publique Canada</td>
</tr>
<tr>
<td>(5 min)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. 9 h 05 – 9 h 40</td>
<td>Stratégie internationale sur la cybersécurité</td>
<td>Daniel Jean, sous-ministre, Affaires étrangères, Commerce et Développement Canada</td>
</tr>
<tr>
<td>(35 min)</td>
<td>Pour discussion : Une présentation sur le point sur la politique étrangère en matière de cybersécurité et réactions aux progrès accomplis en matières de cybersécurité internationale et une présentation sur la gouvernance d'Internet et ses incidences économiques. Une discussion suivra.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>John Knubley, sous-ministre, Industrie Canada</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Les documents seront distribués avant ou lors de la rencontre.</td>
</tr>
<tr>
<td>3. 9 h 40 – 10 h 10</td>
<td>Gouvernance d'Internet</td>
<td>Les documents seront distribués avant ou lors de la rencontre.</td>
</tr>
<tr>
<td>(30 min)</td>
<td>Pour discussion : Discussion sur la gouvernance d'Internet et ses incidences économiques</td>
<td></td>
</tr>
<tr>
<td>4. 10 h 10 – 10 h 25</td>
<td>Développements récents en matière de cybersécurité</td>
<td>Lynda Clairmont, sous-ministre adjointe principale Sécurité publique Canada</td>
</tr>
<tr>
<td>(15 min)</td>
<td>L'exposé sera distribué avant ou lors de la rencontre</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pour information : Examen des derniers développements et événements en matière de cybersécurité</td>
<td></td>
</tr>
<tr>
<td>5. 10 h 25 – 10 h 30</td>
<td>Tour de table</td>
<td>S.O.</td>
</tr>
<tr>
<td>(5 min)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Promoting a free, open, and secure Internet

September 2014
Why the Internet works

Open & Permissionless

Global & Interoperable

Multistakeholder governance
Connection to foreign policy priorities

- Prosperity: Increase economic opportunity & advance development goals
- Values: Promote human rights and democracy
- Security: Ensure stability and protection of networks
Major trends

- Growing threats to privacy and security
- Rise of the global South and East
- Disruptions to established business models
- Empowerment of civil society actors
Responses and risks

There are competing visions for how the Internet should evolve in light of emerging trends, and many responses now being pursued risk undermining the openness and interoperability of the Internet:

Intergovernmental control

Some states want intergovernmental organizations to assume more control over the Internet, including its governance, contents, and security arrangements. This would take power away from non-government stakeholders.

Fragmentation

Internet fragmentation takes several forms: censorship; fees levied on content providers (in violation of Net Neutrality); data localization rules, etc. The trend is driven by privacy concerns, a desire for state control of content, and other factors.

Censorship and surveillance

Content restrictions and intrusive surveillance are becoming more prevalent as non-democratic states look to punish dissent and reassert control over public discourse.
A pivotal time for the Internet

- Debates on the future of the Internet are playing out in a number of international settings on a range of issues.

- How these debates unfold will indelibly shape the future of the Internet, with profound impacts for Canadian interests.

- The international calendar is highly charged:
  - ITU Plenipotentiary
  - WSIS+10 Review
  - UN General Assembly and Human Rights Council
  - Internet Governance Forum
  - IANA transition deadline
  - Dutch Cyberspace Conference

- Canada is working with likeminded partners in these settings to preserve the multistakeholder governance model and a free and open Internet.
Internet foreign policy activities

Prosperity

• Mainstream the role of ICTs in post-2015 Millennium Development Goals
• Resist state control of the Internet at the ITU and defend multistakeholder model
• Promote Canadian economic and security interests in trade agreements
• Support prosperity through expanded opportunities for Canadian ICT sector

Values

• Defend human rights and freedom of expression online
• Co-sponsor resolutions at the United Nations on the applicability of human rights online
• Resist proposals at the UN to limit free expression online
• Member of the Freedom Online Coalition

Security

• Establish existing international law as the basis for state behaviour
• Work with Allies to strengthen cyber defence coordination
• Promote the Budapest Convention on Cybercrime and resist a UN treaty
• Provide cyber security capacity building assistance

All in coordination with our closest allied and leveraging our network of missions around the world
<table>
<thead>
<tr>
<th>Activity</th>
<th>Canada</th>
<th>US</th>
<th>UK</th>
<th>Australia</th>
<th>South Korea</th>
<th>Japan</th>
<th>China</th>
<th>Brazil</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appointed a cyber coordinator &amp; dedicated staff</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Articulated a cyber foreign policy</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Setting technical standards</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Funded cyber capacity building</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Funded Internet freedom initiatives</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>n/a</td>
</tr>
<tr>
<td>Recognized leadership on an Internet issue</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Hosted a major Internet event</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Convened bilateral cyber dialogues</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Issues requiring further policy work

- How should we reconcile trade, human rights, and security interests?
- What should be our response to the growing threat of cyber espionage and cyber crime?
- How can Canada ensure policy coherence and protect privacy in our approach to data protection and localization rules?
- How should Canada promote and protect cultural content in a globally interconnected Internet?
Questions

Has the time come for Canada to play a more active international role on Internet issues? What is required for us to accomplish this?

Have we identified the right issues for further policy work?

What are the next steps?
Update on Recent Cyber Security Developments

Deputy Ministers Committee on Cyber Security

September 24, 2014
Cyber Activity in Canada

- Government of Canada (GC) systems continue to be targeted:
  - Compromise of National Research Council of Canada (NRC)
  - Isolated NRC networks

- Strengthening CANARIE network

- Coordinated response/mitigation across government:
  - SSC, CSE, TBS, DND, PS/CCIRC, RCMP
• Operation Tovar disrupts GameOver Zeus botnet
  FBI-led international operation across 11 countries
  Canadian participation: CCIRC and RCMP

• Lessons Learned Report for Heartbleed is complete
  - The findings can be summarized into the following four strategic areas:
Policy Developments

- Cyber policy proposals

- CEO Advisory Committee on Cyber Security

- Defence Research and Development Canada open call for proposals
International Developments

- Deeper engagement with Israel

- Arrest of Chinese National and Canadian permanent resident Su Bin

- Partnership with the National Cyber Forensics Training Alliance (NCFTA)
International Developments

- Upcoming notable international cyber events
  - INTERPOL Cybercrime Conference, Singapore
  - International Telecommunications Union Plenipotentiary Conference, Busan, Korea
  - NCFTA Summit, Pittsburgh
  - Defence Cyber Contact Group Principals meeting, Washington
  - Ottawa 5 meeting,
  - Global Commission on Internet Governance, Ottawa
Media Environment

- Priority areas for Get Cyber Safe campaign:
  - Mobile security
  - SMB cyber security
  - Digital literacy for kids

- Themes for Cyber Security Awareness Month (October):
  - Promoting Online Safety
  - Secure Development of IT Products
  - Critical Infrastructure and the Internet of Things
  - Cyber Security for Small and Medium Businesses
  - Cyber Crime and Law Enforcement