



Public Inquiry Into Foreign Interference in Federal
Electoral Processes and Democratic Institutions

Enquête publique sur l'ingérence étrangère dans les
processus électoraux et les institutions démocratiques
fédéraux

Public Hearing

Audience publique

**Commissioner / Commissaire
The Honourable / L'honorable
Marie-Josée Hogue**

**VOLUME 3
ENGLISH INTERPRETATION**

Held at :

Library and Archives Canada
Bambrick Room
395 Wellington Street
Ottawa, Ontario
K1A 0N4

Wednesday, January 31, 2024

Tenue à :

Bibliothèque et Archives Canada
Salle Bambrick
395, rue Wellington
Ottawa, Ontario
K1A 0N4

Le mercredi 31 janvier 2024

INTERNATIONAL REPORTING INC.

<https://www.transcription.tc/>

(800)899-0006

II Appearances / Comparutions

Commission Lead Counsel / Procureure en chef de la commission	Shantona Chaudhury
Commission Counsel / Avocat(e)s de la commission	Gordon Cameron Erin Dann Matthew Ferguson Hubert Forget Howard Krongold Hannah Lazare Jean-Philippe Mackay Kate McGrann Lynda Morgan Siobhan Morris Annie-Claude Poirier Gabriel Poliquin Natalia Rodriguez Guillaume Rondeau Nicolas Saint-Amour Daniel Sheppard Maia Tsurumi
Commission Research Council / Conseil de la recherche de la commission	Geneviève Cartier Nomi Claire Lazar Lori Turnbull Leah West
Commission Senior Policy Advisors / Conseillers principaux en politiques de la commission	Paul Cavalluzzo Danielle Côté
Commission Staff / Personnel de la commission	Annie Desgagné Casper Donovan Michael Tansey

III

Appearances / Comparutions

Ukrainian Canadian Congress	Donald Bayne Jon Doody
Government of Canada	Gregory Tzemenakis Barney Brucker
Office of the Commissioner of Canada Elections	Christina Maheux Luc Boucher
Human Rights Coalition	Hannah Taylor Sarah Teich
Russian Canadian Democratic Alliance	Mark Power Guillaume Sirois
Michael Chan	John Chapman Andy Chan
Han Dong	Mark Polley Emily Young Jeffrey Wang
Michael Chong	Gib van Ert Fraser Harland
Jenny Kwan	Sujit Choudhry Mani Kakkar
Media Coalition	Christian Leblanc Patricia Hénault
Centre for Free Expression	John Mather Michael Robson

IV Appearances / Comparutions

Churchill Society	Malliha Wilson
The Pillar Society	Daniel Stanton
Democracy Watch	Wade Poziomka Nick Papageorge
Canada's NDP	No one appearing
Conservative Party of Canada	Michael Wilson Nando de Luca
Chinese Canadian Concern Group on The Chinese Communist Party's Human Rights Violations	Neil Chantler
Erin O'Toole	Thomas W. Jarmyn Preston Lim
Senator Yuen Pau Woo	Yuen Pau Woo

V

Table of Contents / Table des matières

	PAGE
Introduction of the Expert Panel by/Introduction du panel de spécialistes par Mr. Gordon Cameron	1
Presentation by /Présentation par Mr. Alan Jones	3
Presentation by /Présentation par Mr. John Forster	12
Presentation by/Présentation par Mr. Richard Fadden	17
Questions to the panel by/Questions aux panélistes par Mr. Gordon Cameron	26

Ottawa, Ontario

--- The hearing begins January 31, 2024 at 10:00 a.m.

THE REGISTRAR: Order, please.

This sitting of the Foreign Interference Commission is now in session. Commissioner Hogue is presiding.

The time is 10 o'clock.

COMMISSIONER HOGUE: So good morning, everyone.

MR. GORDON CAMERON: Good morning.

COMMISSIONER HOGUE: First, participants were informed yesterday evening, but this is just for the purposes of informing the public, there were some constraints with the panelists, so exceptionally today the panel discussions will end around 12:30 p.m. as well as today's session.

So for those who have other things to do this afternoon, they can go ahead and do so.

Mr. Cameron, if you want to come to the podium. I understand it's you that will lead the panel this morning, so.

--- INTRODUCTION OF THE EXPERT PANEL BY/INTRODUCTION DU PANEL DE SPÉCIALISTES PAR MR. GORDON CAMERON:

MR. GORDON CAMERON: Thank you, Madam Commissioner.

My name is Gordon Cameron. I'm one of the Commission counsel. Today we have a panel of three former national security intelligence public officials. The parties might have had a chance to read their biographies, but I'll

1 do a brief introduction of them.

2 Seated closest to the counsel tables is Mr.
3 Richard Fadden. Mr. Fadden served as Director of the
4 Canadian Security Intelligence Service from 2009 to 2013 and
5 was then the National Security Advisor to the Prime Minister
6 in 2015 and 2016. Prior to that, he held various Deputy
7 Minister positions, including the Deputy Minister of Defence
8 in the government, and currently, among other roles, he is a
9 senior Fellow at the University of Ottawa's graduate school
10 of Public and International Affairs.

11 Seated beside Mr. Fadden is Mr. Alan Jones.
12 Alan Jones began his working career with the RCMP and then
13 moved to CSIS, where he held various operational and
14 management positions, rising to Assistant Director of
15 Operations at CSIS, thus responsible for all operational
16 programs, and then as Assistant Director for Technology,
17 which included both corporate and operational technology. He
18 is currently an executive advisor in the University of
19 Ottawa's Professional Development Institute for courses on
20 national security and cyber security.

21 Mr. John Forster joins us by video link and
22 he -- Mr. Foster was the Chief of the Communications Security
23 Establishment, which is, as you might have learned from some
24 of the filed materials, the federal government's agency for
25 signals intelligence and cyber security. He was in that
26 position from 2012 to 2015. Prior to that, he, too, held
27 various Deputy Minister and Associate Deputy Minister
28 positions, including as Deputy Minister of Defence. And

1 since his retirement from the government, he has continued as
2 a consultant with CSIS with National Defence and with
3 Infrastructure and Communities.

4 Madam Commissioner, what we plan to do first
5 is to have the panelists make an opening presentation
6 expressing some of their views on the topics before us today,
7 and though there's no necessary order to this, we've decided
8 that we would begin by asking Alan Jones to begin with his
9 comments.

10 So Mr. Jones, could you get us started?

11 **--- PRESENTATION BY/PRÉSENTATION PAR MR. ALAN JONES:**

12 **MR. ALAN JONES:** Thank you very much for the
13 opportunity to speak today.

14 I thought I might start my comments with
15 making some commentary on the panels yesterday, which I found
16 very informative. I was here yesterday, and there were some
17 -- there was a discussion and some information offered that I
18 thought I would offer some comments on for context.

19 One, I thought the overview by Professor Leah
20 West on the process around section 38 was extremely useful
21 and the comparison to what happened in the Arar Commission
22 was informative and useful and a very appropriate way to
23 introduce those topics to this Commission because things will
24 probably unfold in a similar manner, although obviously
25 there's been some evolution of that process and law since
26 that.

27 I was very grateful to -- for Professor
28 West's submission on that.

1 One point that did not come out clearly I
2 thought I would make was the classified information is not
3 owned per se by the agencies. It is owned by the Crown.
4 Information is governed by federal law, by precedents, by
5 federal policy and the decisions for disclosure are made on
6 behalf of the Governor of Canada, not solely on the volition
7 of agencies for what they would or would not want to
8 disclose.

9 **MR. GORDON CAMERON:** Excuse me, Mr. Jones.
10 Could you move the microphone closer to your mouth just to
11 make sure the interpreters and people can hear you better?

12 **MR. ALAN JONES:** Is that better?

13 Okay. There was also considerable reference
14 to the Arar Commission, which I had considerable involvement
15 in. And I think the process around disclosure in Arar is
16 very relevant to this Commission, but I was a bit not
17 concerned, but I don't necessarily view -- actually, I don't
18 view at all that the focus of the Arar Commission, which was
19 on wrongdoings, is the focus of this Commission.

20 I think that there is quite a divergence in
21 the Terms of Reference for this Commission to the Arar
22 Commission and I was a little concerned that the impression
23 would be left that this focus was on wrongdoings by whoever,
24 which changes the complexion of a number of things.

25 One, it changes the complexion of requests
26 for disclosure, particularly if it's to third parties, where
27 a third party, if it's another country, is -- because other
28 countries are watching this process. This is public. That

1 another country if it is asked to disclose into a Commission
2 on wrongdoings then may take something of a defensive
3 position about what it is willing to disclose compared to a
4 request for disclosure for fact finding.

5 The other being if there is a perception of
6 wrongdoing, criminal wrongdoing, as there was in Arar, that
7 that has an effect on the type of disclosure. The
8 credibility of information, the source of information, where
9 that information comes from is looked at in a very different
10 context than it is for a fact finding.

11 So I just wanted to put -- make that as a
12 clear point that I think this Commission is not Arar 2, so to
13 speak in terms of its focus and its intent, but the analogue
14 for the process around disclosure in Arar is very relevant.

15 The other point I would make about Arar, that
16 was a -- the subject matter was totally different. It was
17 counter-terrorism as opposed to foreign interference, which
18 involves different agencies, a different methodology for how
19 that information is collected, how intelligence produced, and
20 obviously, the context of Arar was post-911, which was a
21 different time than we are in now.

22 In reference to third party intelligence, we
23 are, as the comment was made, a net importer-receiver of
24 intelligence produced by allies and partners, primarily the
25 Five Eyes, but also NATO, but also others. Government of
26 Canada has relationships with many different organizations
27 worldwide. The world is bigger than the Five Eyes in NATO,
28 and those relationships are all important.

1 But I think what is important to bear in mind
2 is those other countries run their intelligence programs not
3 for the benefit of Canada. They run their programs for the
4 benefit of protecting their own countries.

5 Intelligence that they provide to Canada is a
6 byproduct, or sometimes an intentional product if their own
7 interests are involved, of their programs which are designed
8 to protect themselves. They will disclose intelligence to
9 Canada, share intelligence with Canada for collective
10 security. They'll disclose if they believe that there is a
11 threat to their own country that is emanating from Canada or
12 from someone or an organization linked to Canada and they're
13 looking for cooperation. They will disclose as general
14 information for a broad-based threat.

15 They will disclose sometimes just to be in
16 good standing with Canada because they have other relations,
17 even economic and tourism relations, that they want to make
18 sure that Canada understands that they are safe and they are
19 working hard to keep their borders safe. But their primary
20 intent of producing intelligence is for their own purposes.

21 So when Canada makes a request for disclosure
22 and there are at risk their sources, whether they're human
23 sources, technical sources or if they're covert operators
24 working for their agencies or their methodologies, they must,
25 in their deliberations about disclosure, measure the impact
26 on their own national security when providing that
27 information to Canada or reviewing any type of disclosure
28 request for public disclosure.

1 So it is not simply that they're looking at
2 how it affects Canada. It affects them.

3 There's also an element that was discussed
4 yesterday of the time that it takes to process disclosure
5 requests and go through the section 38 process of the *Canada*
6 *Evidence Act*, that it is slow. It is not simply a Canadian
7 process.

8 When Canada makes that request to a third
9 party, to another country, that request ends up going to
10 specialized sections within those agencies which are policy
11 and legal sections who tend to be swamped with requests from
12 their own internal processes, whether they're preparing
13 documents for Congressional hearings, for Parliamentary or
14 state inquiries or responding to lawsuits or responding to
15 other countries. So it -- I think it's important to
16 understand that, although it is tempting at times to think
17 that another country is dragging its feet and doesn't want to
18 cooperate, you're entering into yet another bureaucratic
19 process with deliberations take a long time and the response
20 time is not necessarily compelled by the response time of a
21 Canadian interest. They have to look at their own priorities
22 as well.

23 And while pressure can be put to say, "Look,
24 this is very important, we need you to respond within this
25 timeframe", there's often goodwill. They often do
26 understand. Many countries want to understand, do understand
27 that this is important. They have their own pressures to
28 deal with.

1 There was a comment made about sometimes that
2 there is tension around even asking another country for
3 disclosure on certain topics. Most of the countries that
4 Canada deals with, the Five Eyes in NATO, there is -- that's
5 really not an issue.

6 They have their own processes. They
7 understand why we were asking -- we would be asking those
8 questions. They may not be happy about it because sometimes
9 they would wish that Canada would resolve its own issues
10 without asking them to have to become part of it. But that
11 there's no -- there's no real risk of damage to the
12 relationship, we'll work that through.

13 Other countries who do not have similar
14 systems to Canada, who do not have rule of law, who don't
15 have democratic governments, not liberal democracies, their
16 response to these types of questions sometimes is quite
17 different. They don't understand why they're being asked.
18 They will have -- they'll try and overlay their own lens as
19 to why we'd be asking those questions. That sometimes
20 requires a lot of finesse, a lot more work and sometimes they
21 just simply either don't respond or they say no.

22 The types of responses that you can get can
23 be a "Yes, we will disclose", "We will disclose part of what
24 you want, but not all of it", but sometimes you get a nuanced
25 response which is, "We have disclosed this to the Government
26 of Canada for you to use as you see -- as you require, but
27 we'll also hold you accountable for the consequences of your
28 disclosure".

1 This is that middle ground grey area where
2 you have to make decisions about what you disclose and you
3 don't, so it's not -- again, there's no formula for this and
4 no written rules.

5 There's very ample discussion, as I say,
6 about the need to protect human sources. Obviously, we have
7 an obligation, legal and moral, to protect people who are
8 putting their lives at risk to provide intelligence to Canada
9 to protect Canada.

10 Often they are providing intelligence to
11 Canada, particularly in the context of foreign interference,
12 because they want to protect themselves, their families,
13 their communities and others, but they are concerned that the
14 exposure of their cooperation with the government would have
15 negative consequences on them reputationally in business or
16 for more dire consequences to their family and their
17 interests back in whatever country that is the source of the
18 coercion or the intimidation or the interference.

19 These are real issues. These real street-
20 level issues that you have to deal with when you're dealing
21 with a disclosure request because these are human beings.

22 The disclosure of technical sources -- and
23 there was a comment yesterday that was made that I thought
24 was very -- was worth repeating, is in intelligence reports,
25 the source is not disclosed in reports itself. In fact, the
26 type of source is not referenced. There is no reference to
27 whether it is a human source or a technical source because
28 the mere reference as to whether it is a human or a technical

1 source can point to exactly what that source is, so the
2 source itself is anonymized in every reporting.

3 The identity of that source is always kept
4 separate in a separate process, and that is done for the
5 need-to-know principle and to protect those assets.

6 Technical assets are often a technical
7 source, has often been deployed or put in place with the
8 support of a human source, so you can't necessarily partition
9 those disclosure requests. Technical sources are often very,
10 very expensive, but they also come with their own risks, and
11 the risks are that a human source may have been in support or
12 that individuals may have been operating in covert positions
13 where there was physical risk to put that source in place.

14 Just as a bit of an anecdote, hyperbole, I
15 think most people are aware that in the CIA lobby there's a
16 memorial wall with stars on the wall. For every CIA agent
17 that has been killed, there's a star on the wall.

18 The NSA, which is CSE's equivalent, has a
19 similar memorial wall. There are more stars on the NSA wall
20 than there is on the CIA wall. So the physical risk around
21 technical sources is not trivial. It's not inconsequential.
22 It does exist for various reasons.

23 But there are risks to these. It's not
24 simply a technical source.

25 In both of those cases, whether it's a human
26 source or technical source, they've been developed, often
27 over years of time. They've been developed because there's a
28 need for them. And so if there's a loss of them, you also

1 lose the ability to produce that intelligence reporting on
2 future threats.

3 So that goes into the disclosure
4 considerations as well, is if you lose those sources for a
5 disclosure, although it may be a very important reason, how
6 do you replace them and are you leaving yourself vulnerable
7 because there is a gap?

8 Just to sum up, I've outlined a lot of things
9 of concerns based on the conversations yesterday, but I have
10 long believed that there is scope for more disclosure of the
11 good work that is done by the intelligence services in Canada
12 on behalf of the people of Canada and the Government of
13 Canada, that there are ways that we could look at being more
14 transparent, but managing to protect those sources, those
15 risks in future. I'm not sure that the current rules and
16 laws as they're interpreted now have been as innovative as
17 possibly as they could be in a modern context and that there
18 may be ways to interpret. I'm not going to go too far down
19 that road because there's legal issues in there, but I think
20 that there is a very -- at times the narrowest interpretation
21 of risk based on the various ways that disclosures can happen
22 that there may be latitude on innovation and scope for
23 broader disclosure. One of them might be -- is what I would
24 call a temporal issue, because over time, the risk to -- of
25 disclosure may be mitigated, not necessarily. But there are
26 times when a human source, for as long as they live, has to
27 be protected, or protecting the source is long. But there
28 are circumstances when a risk that may have exist to

1 disclosure of information that is a year, or two, or five
2 years old is not the same as information that is longer than
3 10 years old or even in a different timespan. And I'm not
4 sure we've ever really looked at that temporal aspect or the
5 depth that possibly we could as to what that means. That is
6 one example. But I think more work needs to be done. I
7 think it is very important for the credibility of agencies,
8 for the people of Canada and Parliamentarians to understand
9 why agencies are doing what they're doing, to understand the
10 good work that is being done on behalf of the people of
11 Canada, and the only way to do that is to be more
12 transparent. And I think -- I urge that more work be done on
13 this in future.

14 So I've laid out a bunch of risks, but at the
15 same time, I want to put that marker down as we need to do
16 better on disclosure than we have in the past.

17 **MR. GORDON CAMERON:** Okay. Thank you, Mr.
18 Jones.

19 And now, Mr. Forster, if we can hear some
20 comments from you? Let's see if the video comes up.

21 **MR. JOHN FORSTER:** Okay. Thank you, Gordon.
22 Can you hear me all right?

23 **MR. GORDON CAMERON:** Yes, that's working
24 well.

25 **--- PRESENTATION BY/PRÉSENTATION PAR MR. JOHN FORSTER:**

26 **MR. JOHN FORSTER:** Okay, great. Good morning
27 and thank you for the opportunity to be here this morning.
28 As Gordon mentioned, I worked in several departments in my

1 career, three of which involved national security and
2 defence. At Transport Canada we were consumers of
3 intelligence to try and identify threats to the
4 transportation system, particularly aviation, such as putting
5 in place a liquid ban overnight due to a flight from the UK.
6 As Chief of the Communications Security Establishment, we
7 were collectors of foreign intelligence that we provided to
8 other departments. And finally, as Deputy Minister of
9 National Defence, which has a very significant intelligence
10 function, we were both a collector and a consumer of
11 intelligence to assist the Armed Forces.

12 I'll start off by saying I'm not a lawyer and
13 I'm not a specialist in intelligence classification, but I
14 thought I'd share a few perspectives from my experience as
15 both a collector and consumer of intelligence products. And
16 I support the inquiry's view that, you know, it wishes to be
17 as transparent as possible and to make as much information
18 public as possible. In fact, there was many times,
19 especially when I was at CSE, and during many appearances in
20 front of parliamentary committees where it would have made my
21 job as the head of one of the agencies a lot easier to
22 disclose classified information, to explain threats to
23 Canada, or explain the operations of my department.

24 But even if it wasn't against the law, there
25 were real reasons that prevented me from being able to do
26 that, so I'll touch on a few of these, and Al had mentioned
27 some of them already, but I'll touch on a few of the key
28 constraints that we faced.

1 First, intelligence agencies like CSE and
2 CSIS must at all costs protect their sources, their
3 techniques, their technology. So when you publish a report
4 about a conversation, even if you take out names and you
5 redact locations and some of the specifics, you can easily
6 divulge who or how the information was obtained, and that
7 puts your sources at risk, or your target will take steps to
8 evade your technology and techniques and you go dark. And so
9 that's always going to be a very critical consideration.

10 Second, important to remember, intelligence
11 is not fact. The disinformation campaigns are escalating.
12 Attribution, particularly that's identifying the real source
13 of the information, particularly in the cyber domain where
14 CSE works, can be extremely difficult. And so as a result,
15 if you publish a report, even with varying degrees of
16 confidence, there may be a risk of inadvertently disclosing
17 information before further analysis confirms or corrects it.

18 Third, intelligence requires good analysis
19 and context. So when I began at CSE, I was cautioned about
20 consuming raw intelligence, a report of a conversation, a
21 report of a meeting, because they can be misleading. So
22 analysts combine an in-depth knowledge of their subject, the
23 trends, the context, reporting from different sources to
24 eventually build an assessment. So when you publish a single
25 individual report, it may mislead the reader who doesn't have
26 access to other critical reporting and context. This is a
27 caution I shared with previous Ministers of National Defence.

28 Now fourth, as Alan mentioned, a lot of the

1 information is not ours to share. We are a huge net importer
2 of intelligence. We rely on our allies, particularly the
3 Five Eyes, particularly in the SIGINT world, for much of it.
4 And we consume more than we produce. And so the originator
5 of the intelligence imposes their conditions or caveats on
6 how we can use it and we need their approval. And if you
7 disclose it without that approval, no matter -- and it may
8 take long time, they'll simply stop sharing with you. And
9 Canada would be severely weakened.

10 Finally, another key point I think to mention
11 is the need to know, as Alan referenced it earlier. Some of
12 the intelligence is so sensitive, the source so crucial, and
13 the information so valuable, there are only a handful of
14 people in the federal government that have access to it.
15 It's compartmentalized, it's highly restricted, and you must
16 be indoctrinated to review it in a secure location. It's not
17 routinely available even to people with a top-secret
18 clearance, and that goes for deputy ministers as well.

19 So does this mean that all intelligence needs
20 to be kept secret and can't be made public? Not at all, and
21 I think, in fact, CSIS wants to be able to share more of its
22 intelligence with governments and companies and universities,
23 but it has to require a change to its Act. And it's really
24 important that the inquiry has the access to what it needs
25 and can challenge the government on what can be released.

26 So there's three points I'll make in that
27 respect. One, I think it's important for participants and
28 the public to remember that, as I understand it, the inquiry

1 will have full access to all of the unredacted information.
2 So even if they can't release it or refer to it explicitly,
3 the inquiry certainly will be able to consider it in doing
4 its work and formulating its findings.

5 The second, the inquiry can and should
6 challenge the government to justify what can't be released
7 and why. Departments do, on occasion, over-classify
8 material. There can be a natural inclination to default to
9 less is more. So it's important that a challenge process
10 include a senior-level review of an initial decision by an
11 expert where a broader perspective may be required, but it
12 can't be in every instance. And even though the inquiry can
13 challenge it to the Justice Department or the court, it's
14 such -- so time consuming and resource intensive, both for
15 the inquiry and the government that it's -- I think a spirit
16 of cooperation will be critical and it will need to be
17 communicated by the government to -- at the senior level.

18 The third point I would make is I think it
19 will be important for the government and agencies to produce
20 unclassified versions of reports, public summaries, or an
21 unclassified assessment. You know, it's not necessary that
22 specific details, names, locations, dates, specifics of a
23 conversation necessarily be disclosed to get the gist of the
24 report and what its impacts are on the Inquiry's mandate.

25 You know, there is no simple kind of general
26 rule or one-size-fits-all solution that we'll find. Each
27 report will require careful consideration. There are real
28 risks at stake. And public interest and transparency will be

1 -- is very important, but it must be balanced also against
2 very real and serious national security interests, which are
3 also in the public interest.

4 So I think the public date the Inquiry is
5 hosting this week is really an important and very valuable
6 one, and I'll conclude there and turn it back to Gordon.

7 **COMMISSIONER HOGUE:** Thank you.

8 **MR. GORDON CAMERON:** Thank you, Mr. Forster.

9 And now Mr. Fadden, could you give us your
10 remarks?

11 **--- PRESENTATION BY/PRÉSENTATION PAR MR. RICHARD FADDEN:**

12 **MR. RICHARD FADDEN:** Good morning. Thank
13 you, and thank you for the opportunity to speak to you.

14 I should say in starting, I have a moderately
15 bad head cold, so if I sound like Donald Duck, I apologize.

16 I'm going to apologize again to the plethora
17 of lawyers, I guess including to myself as a lapsed lawyer,
18 that I'm not going to talk very much today about the law
19 governing confidentiality and openness. I acknowledge their
20 importance and the fact that if my remarks take me outside
21 that ambit, any number of people will correct me.

22 But what I'm going to try and do today is to
23 present to you a practitioner's practical perspective on this
24 topic. And I should say that over the years, I've had some
25 jobs where the emphasis was on protection and other jobs
26 where the emphasis has been on openness, so if I come across
27 as schizophrenic, it's, in fact, intentional.

28 So I think from a practitioner's perspective,

1 you start with the recognition that the law needs to be
2 respected and then you move on. In a democracy absent clear
3 constitutional or legal direction to the contrary, openness
4 and transparency is the default.

5 And I can remember that I -- we often used as
6 an example the old Soviet Union where everything was
7 classified unless there was a clear, clear indication that it
8 could be made public and that the reverse was true in Canada,
9 that everything was open unless there was clear direction
10 that it had to be kept classified.

11 I can't say that that particular perspective
12 was shared by everybody, but it sort of captured, I think,
13 the distinction between ourselves and our adversaries.

14 I think we have to acknowledge that the law
15 pushes both sides. For example, the *Security of Information*
16 Act pushes towards protection and the *Access to Information*
17 Act pushes towards openness.

18 But my first key point is that all laws and
19 policies are very susceptible to both bureaucratic and
20 institutional and personal interpretation. The Commissioner
21 wouldn't have her full-time job if that's not true. I mean,
22 we interpret at all levels within the bureaucracy, within the
23 judiciary, and this has an impact on what people do with the
24 laws and the policies.

25 And I think this is important because these
26 interpretations over time result in the creation of a culture
27 which can and does become as determinative of what's released
28 as the actual law and policies.

1 So CSIS or GAC or CSE each develop a broad
2 approach to classifying, declassifying and releasing
3 information that is unique to that institution, approaches
4 which also, as John and Al have pointed out, are also guided
5 by third party counterparts. And if you have a number of
6 institutions that have contributed to a particular piece of
7 intelligence, almost always the default is to classify to the
8 highest level sought by any given institution. It's very
9 rarely that you end up with the lowest common denominator or
10 the lowest common classification.

11 So with the possible exception of PCO, the
12 agencies we are mostly concerned about have closed personnel
13 systems, which I think reinforces this culture. And by
14 "closed personnel system", I mean you join CSIS as a boy or
15 girl spy and you want to become the Director. You join CSE
16 as a cryptologist and you want to become the Chief. And that
17 really results in a culture that's very, very, very strong.

18 Just say a couple of words about PCO, which
19 stands at some distance from other departments and agencies
20 both in terms of working for the Prime Minister, but also, in
21 the national security area, they have distance, which is
22 something that departments and agencies don't have. And it's
23 like anybody who works in a specialized area. You
24 concentrated long enough, hard enough, and you develop this
25 sort of closed world view of what you're doing, including
26 decisions to classify or declassify.

27 PCO can be very helpful. Having all the
28 clearances and whatnot, when something is important enough

1 they, ideally, are able to take a broader perspective.

2 Certainly when I was NSA, that's -- that was
3 required of us on a few occasions. You then negotiate with
4 the departments and you point out that there's often or
5 sometimes a broader perspective than that could be seen by
6 individual departments and agency.

7 So I'm not suggesting, you know, a conscious
8 desire on the part of agencies to disregard my default
9 position, but rather, a conscious effort to legitimately
10 protect information. And the balance there is, I think,
11 clearly in favour of protection.

12 I think over time the protective culture
13 becomes dominant, and this actually sits well with Ministers
14 and central agencies and senior officials, especially when
15 the protective effect, the practical effect, is reducing the
16 likelihood of controversy. I'm not suggesting that
17 controversy or partisanship very often plays a role, but if
18 by happenstance you're invoking protection under particular
19 legal provision means that you're not releasing something
20 that would call all sorts of controversy, there's nobody in
21 the system that points in the opposite direction.

22 And I'll come to this in a minute, but
23 there's no openness advocate in the entire system because the
24 Access to Information Commissioner doesn't play on these
25 highly-classified matters, so everybody sort of goes in with
26 the expectation that they're maintaining an appropriate
27 balance and, if I'm correct, the balance is sometimes tilted
28 in favour of protection because of the culture that I talked

1 about. And it often means that very, very quick decisions
2 are taken because you have the volume of material and you
3 have a culture that indicates that you're going in a
4 particular direction with respect to classification.

5 This is also true when you're getting
6 information or intelligence from the same source, the same
7 methodology or you're producing the same kinds of reports.
8 And it might be interesting for you to ask to what extent my
9 successors use algorithms as opposed to the human brain to
10 determine classifications.

11 I think that given the volume today, very,
12 very frequently -- everything's produced electronically, so
13 why not introduce an algorithm that classifies which can be
14 reviewed if appropriate or necessary by human beings, but I
15 suspect that in a lot of cases the algorithm wins.

16 And I think in the system it's important to
17 note, too, that appeals outside the system, they're
18 difficult, they're lengthy and they're expensive, so if you
19 can't get somebody within the system to respond to a request
20 for declassification, it's very difficult to get otherwise.

21 So my central point is that while much of the
22 information that you will be interested in deserves
23 protection, and John and Al have pointed out a good number of
24 reasons why, the culture, the workload and the tradition in
25 agencies, I think, is to tend towards overprotection. Not
26 always the case, but it's frequently the case.

27 Again, I want to stress the absence of an
28 openness advocate in all of this, with the possible exception

1 of the Department of Justice, which unfortunately, tends to
2 focus on the law. That's a joke, and bad one, it seems. And
3 PCO where the files, if they're important enough, they merit
4 consideration there.

5 So what I'm trying to say in my roundabout
6 way is there is room to push because of this overprotection,
7 this culture. And I don't know in the context of this
8 Commission to what extent PCO and DOJ are going to be
9 involved in individual decisions, but I would commend to you
10 the view that if you have a lot of trouble getting openness,
11 you, Commissioner, should consider talking to the Clerk of
12 the Privy Council, who is the guardian of all of these things
13 for the public service, and the statutory guardian of Cabinet
14 secrets.

15 So before suggesting a couple of ideas to
16 consider as it works its way through specific reports of the
17 Commission, let me revert to the practical and try and put
18 myself in the shoes of people who are working in the system
19 and who have to deal with all sorts of secrets.

20 And I think in the practical sense, there are
21 three kinds of secrets. There are national security secrets
22 that we've talked about this morning, there are national
23 interest secrets that have been discussed yesterday and Al
24 alluded to briefly, and then there are Cabinet secrets. And
25 everybody has to be aware of these as they work their way
26 through the classification process and the release process.

27 Each have their own rules, each have their
28 own culture, but I think for your purposes, probably the most

1 important is the national security secrets. Cabinet secrets,
2 as you know, are entirely the prerogative of PCO and nobody
3 else plays on them, or if they do it's at the risk of their
4 lives.

5 But national interest information is often
6 in the background and is often passed on to analysts in
7 access to information shops, which don't necessarily have a
8 picture of what the national security implications are. So
9 what I'm trying to say again, in my round about way, is that
10 these three categories sometimes overlap and interlock with
11 one another, and disaggregating them is an important part of
12 the process.

13 In the absence -- again, I'm repeating
14 myself, but in the absence of an openness advocate, things
15 tend to be classified more than they need to be. So a couple
16 of concrete thoughts. If you believe that what I'm saying
17 has some value, this culture bit, trying to get the
18 government to admit that this plays a role would I think help
19 you discuss on a practical level, individual
20 declassifications.

21 Agencies do get too close to their material
22 and there has to be a way to provide some distance. I don't
23 know if you have this within the Commission, but hiring
24 somebody who's recently retired and worked in this area would
25 I think, be helpful explaining the mindset of people. I know
26 people like Mr. Cameron have worked in this area for a long
27 time, but it's not exactly the same as finding a practitioner
28 who's recently retired to give you a bit of an insight.

1 Involve PCO to play the openness advocate. This should be
2 consistent with the Prime Minister's view that he wants all
3 of this information to be as open as possible.

4 I think another area that's worth thinking
5 about is our allies, our close allies, our close allies are
6 much, much more open than we are. They really protect their
7 core secrets, but the Brits, the Yanks, the Australians tend
8 to be much more open than Canada is. And you know, you can
9 often point to something that they've released that's very
10 close to what you want to release, and ask the officials, why
11 can't we do this? Al has alluded to the question of passage
12 of time. I think that's very important.

13 One of the issues that came up when I was
14 still working was -- well, let me stop for a second. I
15 suspect that you're not going to be looking that every piece
16 of raw intelligence that's produced in the period for which
17 you have a mandate, and a lot of it will be consolidated
18 analyses of one point or -- one sort or the other. And one
19 of the reasons sometimes that things are classified is
20 because the individuals, the officials, don't want to release
21 a set of information that relates to one of the things that
22 John or Al pointed out about, while at the same time, all of
23 this information is in the public domain.

24 And one of the reasons that I used to push
25 back a little bit on my colleagues is, is because within the
26 national security community, people will always prefer
27 national security collected information over the fact that
28 the economist has reported this, or it appears on CBC on the

1 evening news. I'm exaggerating slightly to make my point.
2 But if you can argue with officials that all of this
3 information is broadly speaking, public, why don't you just
4 take it from the perspective and forget about the collection
5 angle, and somewhat change your summaries or your actual
6 final analysis being presented?

7 And I think the other point I would just
8 make, and then I'll stop talking, is -- and it's a device
9 that I used in talking to parliamentary committees, is that
10 you can take a lot of intelligence and aggregate it up a
11 level. It doesn't change the substantive message, but you
12 just lose a little bit of the detail, but in the end, nothing
13 is lost.

14 And I think it's important to remember that
15 Ministers and senior officials very rarely get raw
16 intelligence. They get analytical reports. So everybody
17 getting all upset because they can't read the particular CSE
18 intercept, that you know, took place on date X from person Y,
19 that may or may not be important for the historians, but
20 Ministers, the Prime Minister and senior officials rarely ever
21 get that. They will get consolidated reports, they will get
22 analytical reports, and it's in these kinds of reports, I
23 think, where you have a little bit more flexibility to argue
24 that, you know, if you take out two words or if you aggregate
25 up a level, or if you compare them to the allies, you might
26 get them to release.

27 So I don't mean to suggest as I conclude that
28 I'm in favour of releasing everything, I think there are some

1 secrets that are -- it's absolutely critical to protect, but
2 that doesn't mean that there should not be discussions on the
3 interpretation given by officials on what particular point of
4 information can be released or not.

5 So thank you for your attention.

6 **COMMISSIONER HOUGE:** Thank you.

7 **--- QUESTIONS TO THE PANEL BY/QUESTION AUX PANÉLISTES PAR MR.**

8 **GORDON CAMERON:**

9 **MR. GORDON CAMERON:** Thank you, Mr. Fadden.

10 Gentlemen, as we all know, we will tomorrow
11 have, roughly speaking, your counterparts, plus someone from
12 PCO who are currently incumbent in positions that you held in
13 the course of your careers. And so we will have an
14 opportunity to get perhaps a more detailed account of how the
15 institution of CSIS works, how CSE works.

16 But just so that we can put the comments
17 you've made today and some of the points we might be able to
18 explore in the time left to us into context, I'd like to ask
19 each of the agencies, so to speak, to describe roughly
20 speaking, the type of work you do with a view to contrasting
21 the two of them. And in particular, people hear CSIS, they
22 hear CSE, for a lot of people I think the mere emergence into
23 the public of CSE is a relatively new phenomenon.

24 So if I could ask either or both of you, Mr.
25 Fadden and Mr. Jones, to talk about the type of work CSIS
26 does and then Mr. Forster, I'll ask you to describe the type
27 of work that CSE does, and hopefully the participants will
28 have a better perspective on what different types of

1 intelligence is originating from the two agencies.

2 **MR. RICHARD FADDEN:** Well, if I may, I'll
3 start with just a couple of general comments.

4 Al was far more involved in operations than I
5 was, but the first comment I'd like to make is the law makes
6 it very clear that CSIS must distinguish between domestic
7 intelligence and foreign intelligence. It's the sort of
8 thing that permeates the agency. In both cases you can
9 incidentally collect the other kind of intelligence.

10 But fundamentally, CSIS was created to be a
11 domestic intelligence agency. It was to worry about
12 sabotage, terrorism, sedition, and things like that. And
13 while today there's a clear shift towards being able to
14 collect foreign intelligence both here and abroad, the
15 agency, the service clearly distinguishes the two. And the
16 law requires that, and it's one of the -- I may be so bold,
17 one of the fixations, in my view, the exaggerated fixations
18 of the Federal Court, but that's for another debate over a
19 glass of wine.

20 But that sort of view permeates everything
21 that they do, and we have to be very careful not to do that.

22 The other general statement I would make is
23 that the law allows one agency to ask another agency to do
24 something within it's mandate that it cannot technically do.
25 So CSIS regularly asks CSE to do some collection for it, as
26 long as it's clearly within CSIS' mandate. So I say this to
27 make the point that while both agencies have very clear
28 mandates, John will explain CSE's, which is more focussed on

1 foreign affairs, but CSIS can make use of CSE's technical
2 capabilities as long as it's well within it's own legal
3 mandate, and it does so on a regular basis. And in fact, it
4 can do the same of any other institution in the Government of
5 Canada.

6 So just those two macro points, along with
7 the indication that CSIS collects all of this stuff to be
8 helpful to the government. So there's always a judgement to
9 be made about what is used internally to develop broader
10 reports, and what is kicked into the system that heads up to
11 the Minister, Ministers, and to agencies around town. But a
12 lot of stuff that CSIS collects doesn't leave the agency
13 because it's too specific, it's too narrow, it doesn't really
14 apply to particular interests today. There are other things
15 -- pardon me -- there are other things that CSIS does, like
16 do security clearances and whatnot.

17 But I think I'll stop there. Al is probably
18 better equipped than I am to talk a little bit about some of
19 the more specific operational issues of what CSIS does.

20 **MR. AL JONES:** Sure. I'll start with the
21 mandate in the *CSIS Act*, which is as someone once said to me,
22 who'd come into the service from outside the public service,
23 they had never met a group of people who walked around
24 carrying their *Act* all the time like people did at CSIS. It
25 really does guide what we do on a daily basis. Because
26 everything flows from that *Act*, including all the internal
27 authorities for operational activities must reference back to
28 the *Act* itself, the section 12, which is the primary mandate

1 to collect by investigation or otherwise, the threats to the
2 security of Canada.

3 And then the specific threats under 2(a),
4 (b), (c), and (d) of the *CSIS Act*, (a) being espionage, (b)
5 being foreign interference, (c) being terrorism, and (d)
6 being subversion, which is a muted authority at the moment,
7 hasn't used in many years.

8 So the service, as Dick said, is a domestic -
9 - primarily is a domestic service, or in intelligence
10 parlance, a security service. I know the RCMP call it
11 security, but internationally, countries have what's called a
12 security service, deals with internal security. In the UK,
13 it would be MI5; United States, the intelligence part of the
14 FBI; Australia, it's ASIO, et cetera, et cetera. It has a
15 hybrid foreign intelligence mandate under section 16, where
16 the service can collect on behalf of department -- Global
17 Affairs Canada or National Defence, intelligence as foreign
18 intelligence, but only within Canada.

19 On the security intelligence side,
20 section 12, there is no geographic restriction on where CSIS
21 can operate. We protect -- service protects -- I still use
22 the royal "we" after decades of being there. The service
23 protects Canada and Canadians anywhere on the planet. So you
24 are looking at the security of Canada and Canadians at home,
25 and you're looking at the security of Canada and Canadians
26 abroad, and many of the threats against Canada emanate from
27 abroad, so you have to go where the threats are active in
28 order to get the intelligence you need to protect Canada.

1 CSIS also has, under section 21, the
2 authority to intercept private communications. This is
3 called lawful access. Tapping telephones, putting
4 microphones in walls, all these things CSIS does, publicly
5 known.

6 CSE has a tremendous technical capability for
7 signals intelligence, which is, generally speaking, outwardly
8 facing from Canada, not aimed at Canadians inside Canada.
9 But the types of intelligence that Jonathan talked to in more
10 detail than I can that CSE collect, CSIS doesn't have the
11 technical capability to do, so to support -- there is mutual
12 support, and both consume each other's intelligence. We
13 provide intelligence to CSE, which they need to help focus
14 their mandate, and likewise.

15 So that is the broader mandate of CSIS. It
16 also provides security assessments for government screening.
17 People get security clearances. CSIS does an investigation
18 based on its mandate. It also provides investigations on
19 clearances on immigration. So if people are coming to
20 Canada, they go through a CSIS check as well.

21 That's the primary overview of what CSIS
22 does. And I'll just add. There's no powers of arrest in
23 Canada or elsewhere.

24 **MR. GORDON CAMERON:** That's very helpful,
25 Jones.

26 Now, Mr. Forster, can you bring CSE into the
27 picture?

28 **MR. JOHN FORSTER:** Sure. Thanks, Gordon.

1 So the Communication Security Establishment
2 started as part of the Department of National Defence, and
3 then it received -- it became its own separate agency and its
4 own legislation. It does still report to the Minister of
5 National Defence, but is separate now from DND.

6 And it has two main focusses. One is, as has
7 been mentioned, signals intelligence, which is really
8 electronic communications in all its forms. Another
9 important distinction is its mandate is foreign, not
10 domestic. So it is not allowed to collect information
11 intentionally on Canadians, not just in Canada, but anywhere
12 in the world. And if it inadvertently comes across that, it
13 has to take steps to desensitise it and remove it.

14 It's a provider of raw intelligence, largely,
15 and it provides it to the rest of government, so CSIS, RCMP,
16 GAC, National Defence, CBSA. So it provides intelligence
17 reports for others to do their analysis and take appropriate
18 action.

19 It does have an assistance mandate. So it
20 may assist CSIS, National Defence, RCMP, to do domestic
21 operations, but they're really -- they're undertaking that
22 work on behalf of the agency and under their mandate. So
23 they're kind of a technical arm for other departments.

24 The second key part of its mandate is on
25 cybersecurity. So it protects the federal government,
26 Government of Canada's IT infrastructure from cyber attacks
27 and hackers. It recently got a mandate, not just to block
28 and prevent those attacks, but it can take steps online in

1 the global communications infrastructure to deter those
2 attacks as well.

3 And then it has the cybersecurity centre,
4 which is more the public facing arm of the -- of its mandate
5 on cyber to work with the private sector, other levels of
6 government to help them with their cybersecurity and
7 assistance and advice to Canadians.

8 And I think that kind of captures most of
9 what the CSE does.

10 **MR. GORDON CAMERON:** Thank you, Mr. Forster.

11 One point that we wanted you to just
12 describe, but it's probably something you can explain very
13 simply. But we have seen reference, and you have described
14 it yourself, that CSE collects signals intelligence.

15 First of all, can you just describe for us
16 what broadly speaking signals intelligence is?

17 **MR. JOHN FORSTER:** Yeah, sure. It's largely
18 electronic communications. So CSE, unlike CSIS, would not
19 have human sources. So it's really focussed on the global
20 communications infrastructure. It could be cell phone
21 conversations, texts, you know, computer, any kind of
22 computer communications. So it's -- it really operates in
23 that realm of the global communications infrastructure.

24 **MR. GORDON CAMERON:** And if you can explain,
25 why is it that signals intelligence tends to have special
26 designations and special treatment?

27 **MR. JOHN FORSTER:** It has certain
28 classifications because of the nature of the technology or

1 the sources of the information. So as I mentioned in my
2 remarks, some of these -- the -- you don't want to be
3 disclosing your techniques, your technology, your
4 capabilities, your sources because the targets of your
5 collection will simply take steps to avoid or block it.

6 So its techniques and its technology and its
7 access are extremely sensitive information. So reports,
8 intelligence reports you produce from those can divulge those
9 sources, as I mentioned in my opening remarks. So they take
10 steps to make sure it's very carefully -- access to that
11 information is very carefully controlled. And some of it is,
12 as I mentioned, not available to -- only a -- it's only
13 available to a handful of people in the government.

14 **MR. GORDON CAMERON:** Right.

15 Now, I'm going to move on to a different
16 topic, but Mr. Fadden or Mr. Jones, is there anything you've
17 wanted to add to the respective allocation of
18 responsibilities between the two agencies before we move on
19 to another topic? No? Okay.

20 **MR. ALAN JONES:** I'll ask you. Would you
21 want us to discuss the disclosure regime in -- for CSIS as to
22 what it does with its intelligence within the community?

23 **MR. GORDON CAMPBELL:** That's on my list, so
24 let's go there now. Yes.

25 **MR. ALAN JONES:** Yeah.

26 **MR. GORDON CAMERON:** The types of
27 intelligence reports you produce and the distribution and
28 disclosure you make within the intelligence community.

1 **MR. ALAN JONES:** Okay. So it is -- Dick and
2 I have often commented, there's not much point in spending a
3 lot of time and money collecting intelligence and then just
4 sitting there and admiring how clever you were at gathering
5 it. It actually has to become useful at some point.

6 So obviously, the service is very detailed in
7 its reporting. One of the tenets of doing good intelligence
8 work is attention to detail. So the reports are very
9 detailed. We document everything. Things -- others might
10 say, "Why would you document such -- in such details?"
11 Because you don't know in the future when that detail may
12 become relevant, and that detail may actually prove that what
13 you thought about something in the first place was wrong or
14 right. Data is somewhat self-correcting. The more of it
15 that you get the clearer the picture becomes.

16 John mentioned earlier the risk in reading a
17 singular report on a file. What you know at the outset of an
18 investigation is often quite different than what you
19 ultimately know after you explore more, do more
20 investigation, more fact finding, challenge what you know;
21 you may end up in a very different place.

22 We live in a global world where there is --
23 television is on, CNN is on all the time. My general rule in
24 running operations was the first thing you hear on the
25 television is wrong. You know? It will take time to
26 actually figure out what happened.

27 So we document everything in great detail.
28 Those reports sit in a automated database because you need to

1 be able to recover it and compare it and analyse it to other
2 data and do it quickly. And those documents, that
3 information is kept for many years because it may be years
4 before you get more clarifying information because what you
5 know suddenly comes into context.

6 I have seen many investigations where a piece
7 of intelligence collected, seven, eight, ten years ago,
8 suddenly becomes key in understanding a threat that is --
9 that has developed. That's what intelligence services do.

10 The threshold for what you collect is
11 different than a criminal investigation. For a police
12 officer, that was educated many times in the Superior Court
13 of British Columbia by judges who informed me that what I
14 believed was irrelevant, it's what I knew that was important,
15 when you were doing intelligence investigations, you gather a
16 lot of information that is at not the level of what criminal
17 evidence would be. Rumours, fractured pieces of information,
18 bits and pieces, contradictory investigation, we'll often get
19 things that are -- simply can't be two things at the same
20 time, but yet you get information saying that it is, all of
21 that sits in your database, all of it sits in reports.

22 So learning how to read intelligence is very
23 important. Learning how to understand what it is that's
24 being presented to you, as John said, is very important.

25 As Dick said, providing raw data to senior
26 decisionmakers is often not useful because you don't want to
27 turn the prime minister or a deputy minister into an analyst.
28 And I have seen circumstances in the past, which are better

1 now, where you were dealing with a crisis and the information
2 that was coming in was almost raw. And so you had deputy
3 ministers and senior officials sitting there trying to track
4 in their mind all these reports that they've seen over the
5 last two or three weeks, which, as I said, is not necessarily
6 the same every time you see it, and make sense of it. This
7 is not a helpful way to run a crisis.

8 So someone needs to do that work for our
9 seniors, and that is done. So that's why they're getting
10 assessed information, analysed information, and not just raw
11 pieces of information thrown at them.

12 We share information with other intelligence
13 services between threats are global. We need to have
14 cooperation to protect Canada. We sometimes come into a
15 section of intelligence on a threat that is developing
16 against an ally or a partner, even a country who you may not
17 have the best of diplomatic relationships with, but if you
18 find out that there is going to be, for example, a terrorist
19 attack where there is life at risk, you have an obligation to
20 try and tell other countries "this is what we know; be
21 careful." We don't want to sit on that information and allow
22 something to happen on the other side of the world, just as
23 we would hope that another country would not sit on
24 information that would identify a threat to Canadians.

25 When there is intelligence that is pointing
26 to criminal activity, and criminal activity that either rates
27 -- relates to one of those threats that I described,
28 espionage is a crime in the *Criminal Code*, terrorism is a

1 crime. We'll learn more about how much foreign interference
2 actually becomes a crime or not. That when we get
3 intelligence at that level, we have a mechanism or mechanisms
4 to advise the police of jurisdiction. In a national security
5 case, it's the RCMP. And there are mechanisms to do that.

6 We have what's called a disclosure letter.
7 There may be some changes to this. I am a little dated. I
8 am retired. We'll find out more tomorrow, I'm sure. But a
9 disclosure letter, and these terms are a bit odd for anyone
10 who is not familiar with it. There is a disclosure letter
11 and an advisory letter.

12 Disclosure letter would simply say to the
13 RCMP or police of jurisdiction, "We found out information
14 about this we think is criminal activity. You may want to
15 respond to this, but this information is ours. We're not
16 disclosing it to you for court purposes or for anything else,
17 we're just letting you know."

18 An advisory letter is a more complex process.
19 We are actually providing advice to the RCMP and saying,
20 "Here's what we know, and here's what you can use." And when
21 you say, "here's what we -- what you can use", this obligates
22 the service to do certain things, whether it's retained
23 intercepted communications, whether you document something,
24 whatever, you start to become part of that process. The
25 whole intelligence to evidence is a complicated piece. Won't
26 get into that today.

27 The service may also incidentally come across
28 information that is not related to its mandate, but may be

1 valuable to it through another part of its mandate, or -- or
2 another criminal investigation. You might discover drug
3 dealing or a bank robbery in the process of doing something
4 else, so you would want to disclose it to the police of
5 jurisdiction. "We have discovered information which relates
6 to Health Canada, which relates to the Department of
7 Environment, Department of Finance, we have a mechanism to
8 say this was incidentally collected. It's not part of our
9 mandate, we weren't looking for it. We came across this
10 information. It might be useful to you. Rather than it
11 sitting in our databases and going nowhere, we can disclose
12 this amount to you and this is what we'll agree for you to do
13 with it."

14 So that disclosure regime and those
15 interrelationships are ongoing 24 hours a day, 7 days a week.
16 They're very active. These are not occasional things that
17 you do, this is your life all day, every day in operations in
18 CSIS.

19 **MR. RICHARD FADDEN:** May I add a thought?

20 **MR. GORDON CAMERON:** Yes, please; please do.

21 **MR. RICHARD FADDEN:** I agree with everything
22 that Alan said, but just to make a further distinction. The
23 service produces report, CSE produces report, the military
24 produce reports, GAC produces diplomatic reports, and every
25 now and then, so does CBSA and a bunch of other departments.
26 There's a secretariat in the Privy Council Office called the
27 Intelligence Assessment Secretariat, which is focussed mostly
28 on things foreign, but when there's an overlap with things

1 domestic they have a mandate. So their particular mandate is
2 to consciously seek out reports and intelligence from
3 anywhere in the Canadian Government and anywhere from our
4 allies.

5 So they would take, for example, if they were
6 producing a report on foreign interference by China, they'd
7 take CSIS reports, CSE reports, they'd ask Foreign Affairs
8 whether there is anything, they'd check into what the allies
9 are saying. I think they now do open sources much better
10 than they used to. And they will put this in a consolidated
11 level report, which would most likely be the kind of report
12 that would go to the prime minister, ministers, and senior
13 officials. As Alan said, very rarely do you give very senior
14 people a specific narrow piece of intelligence.

15 More broadly, the system distinguishes, I
16 think quite consciously, strategic analytical intelligence
17 and tactical intelligence. Not that there's a rule or
18 anything, but I just want to emphasise what Alan said. You
19 don't give ministers tactical information about a terrorist
20 attack. You may tell them that one is going to happen, but
21 you don't give them the details. But you do in a strategic
22 report pull together everything you might know about the
23 origins of that potential attack, or foreign interference, or
24 whatnot, so that they can make sense of it.

25 But it might be interesting, given your
26 interest in -- I suspect your interest in what ministers and
27 prime ministers knew in the context of foreign interference,
28 to see what the IAS has produced in this context, which is

1 the prime minister's intelligence secretariat, but the
2 material is also made available to ministers and senior
3 officials. Thank you.

4 **MR. GORDON CAMERON:** And we will be hearing
5 from a representative of PCO tomorrow.

6 But that's a good segue to the next question
7 I was going to ask all of you. You've talked about the
8 process by which intelligence and information is collected
9 and made into the types of reports and intelligence products
10 that your agencies produce, and in that case, for an audience
11 that is receiving and cared to receive classified
12 information.

13 The next question for each of the agencies
14 would be about situations in which you've been called on to
15 make what will be explicitly public comments. That is,
16 you're going to be appearing in front of a parliamentary
17 committee, or perhaps you've been asked to create a briefing
18 that is going to go to cabinet or to some audience that isn't
19 an appropriate audience for the classified information, or
20 there's a report, even an annual report of your agency,
21 something like that.

22 What process do you go through, you know,
23 I'll put it to you, Mr. Fadden. You've been summoned to
24 speak to a parliamentary committee on a topic that you know
25 about almost exclusively as a result of your exposure to
26 classified information that you're about to be questioned.
27 You'd like to be able to say something more than "I'm sorry,
28 I can't answer that question." What process do you go

1 through to prepare yourself for an appearance like that?

2 **MR. RICHARD FADDEN:** I'm smiling because I
3 have been bitten by that process once or twice. I mean,
4 there are two phases to it. One is you produce written
5 comments that you make as close to what you want to say as
6 possible, and if there's anything at all controversial with
7 them, you share it with another department that might be
8 interested. But in particular, if you're a senior official,
9 if you're a deputy minister, you make sure that PCO is
10 comfortable. So that's the written document that, you know,
11 will go on the record. As is often the case, as you're going
12 to demonstrate today with your questions, often, very often
13 before a parliamentary committee, the tendency to ask for
14 more detailed information comes through questions. From
15 there, it's a matter of judgment. I've tried very hard, and
16 mostly I think I've succeeded, in doing what I suggested that
17 you do, which is I try and aggregate up classified
18 information, or sensitive information, so that you can make a
19 general statement on the topic that is -- you're being
20 queried about, and I think that's what they pay you for. If
21 you're a deputy minister, or the director of CSIS, or the
22 chief of CSE, you have to demonstrate judgment about how much
23 you can say because the general rule under all of the
24 governments for which I've worked is try to be as
25 collaborative as you can in front of parliamentary committees
26 without causing, you know, all sorts of grief with allies or
27 with the law.

28 So there's no -- you can't plan for what

1 parliamentary committees are going to ask you. So a lot of
2 it is your understanding of the broad political environment,
3 your understanding of the national security environment, and
4 the application of judgment. And I've found, I don't know if
5 John or Al's experience has been the same, that if you make
6 even the slightest effort to aggregate up and to answer
7 questions on the basis of your judgment, it works. But the
8 written material you process through the system.

9 **MR. GORDON CAMERON:** Right. And if I can
10 just ask, we've used the expression summarize or generalize.
11 Is that roughly analogous to what you're calling aggregate
12 up?

13 **MR. RICHARD FADDEN:** I guess you could. I've
14 used it mostly in the context -- in the practical context of,
15 you know, you have a report, and you just remove some of the
16 detail. I don't know if that's what you mean.

17 **MR. GORDON CAMERON:** Yes.

18 **MR. RICHARD FADDEN:** But very often,
19 classifications are determined by, you know, a word or a
20 sentence or a paragraph. And without necessarily removing
21 them, you can rewrite them to remove the detail a little bit,
22 and that goes on a lot. I mean, I -- to be honest, I spent a
23 bit of my time when I was NSA, trying to convince the
24 agencies to do that, because the higher the classification,
25 the more difficult it is to get in front of people. And as
26 both Al and I have said, the objective is to get it in front
27 of people. So by aggregation, I just mean slightly deluding
28 the detail, sometimes by shifting the wording, while still

1 being very careful that you don't lose the core message.

2 **MR. GORDON CAMERON:** Thank you. An
3 expression we've seen is "right to release"; in other words,
4 a document that is created specifically with the objective of
5 it being released to an unclassified context. Is that the
6 same thing we're talking about?

7 **MR. RICHARD FADDEN:** Not -- well, I guess in
8 the end it is, yes.

9 **MR. GORDON CAMERON:** Yes. Okay. Mr.
10 Forster, can you describe how your agency approached that
11 during your day; that is, situations where the agency had to
12 produce either a briefing to an unclassified audience, or an
13 annual report, or an appearance by you, or one of your
14 colleagues before -- in the public or before a parliamentary
15 committee?

16 **MR. JOHN FORSTER:** Sure. Well, when I
17 started at CSE, it was very -- its general practice was not
18 to disclose much of everything. In fact, it was only in the
19 '80s that the government even acknowledged it existed, so and
20 that the practice and the culture was not to say too much at
21 all. We faced some -- you know, a very healthy challenge and
22 spotlight based on unauthorized disclosures of U.S.
23 intelligence where we actually now had to go to committee and
24 talk about -- more openly about what we did, and why we did
25 it, and how we did it. And we started producing material on
26 the website that better explained. And we found that it's,
27 as Dick mentioned, a lot of the classification comes from
28 some of the details, and that don't -- aren't really

1 necessary to communicate the gist of what you're doing, or
2 what the issue is, or the event that you're trying to
3 communicate. So it's really finding a way to communicate it
4 strategically, here's the issue, here's the current state,
5 while removing a lot of the details that may disclose your
6 methodology, your technology, your sources, or embarrass the
7 country, or whatever, you know -- or not embarrass, but
8 damage your international relations.

9 So I think it -- you know, it's similar to
10 what Dick said. It's finding that right balance and there
11 were times where certainly with our staff we'd have a pretty
12 healthy exchange about what we could and couldn't say about
13 issues, and I think we advanced it, and since I was there,
14 they're even more open now, so it's been kind of an evolution
15 so.

16 **MR. GORDON CAMERON:** Okay. Now, gentlemen,
17 subject -- what I'd like to do is ask you if you have any
18 final comments because then we're going to break for about a
19 half an hour. The participants are going to see if they have
20 any questions that they'd like you to answer, and we'll
21 resume. But before we break for that Q and A process, are
22 there any comments you'd like to make to just recap or cover
23 some of the points that you've heard others talk about?

24 **MR. RICHARD FADDEN:** Just one small point,
25 and it's drawing on what I -- I'm trying to be helpful to the
26 Commission, about strategic intelligence. And I know a lot
27 of people in this country advocate for the almost total
28 release of classified information, which I don't think is

1 possible. So as I was trying to indicate earlier, the Prime
2 Minister, an official, rarely gets detailed tactical source-
3 based intelligence. He gets strategic intelligence. So for
4 those people who are asking for, you know, raw intelligence,
5 or details, I guess my thought would be why should they get
6 it when the Prime Minister doesn't, because he really doesn't
7 get it except in the most exceptional circumstances where,
8 you know, life and limb would be at risk. And I think that's
9 true of most ministers and deputy ministers most of the time.
10 Pardon me. There's this belief, I think, among some parties
11 that, you know, people go to, you know, go to the office in
12 the morning and they, you know, they read all these details
13 of, you know, what colours was the pyjamas of the Consul
14 General in Vancouver wearing and things like that. Well, it
15 doesn't happen that way. You usually get fairly highly
16 aggregated strategic intelligence.

17 So my simple point is, if it's good enough
18 for the Prime Minister, it should be good enough for
19 everybody else, except there are always exceptions. But I
20 just wanted to try and make that point. And not everybody in
21 government gets all of this detail that a lot of people
22 consider to be critical when very often it's not. Thanks.

23 **MR. GORDON CAMERON:** Thank you.
24 Commissioner, that is the completion of this session, so it
25 would be timely to take a break.

26 **COMMISSIONER HOGUE:** Yes, and we'll take a
27 longer break just to make sure that the participants have the
28 time to draft their question that they want to send to the

1 Commission counsel. Thank you.

2 So it's -- we'll be back in about 30 minutes.

3 **MR. GORDON CAMERON:** Okay.

4 **THE REGISTRAR:** Order, please.

5 The hearing is in recess for 30 minutes.

6 --- Upon recessing at 11:15 a.m.

7 --- L'audience est suspendue à 11h15

8 --- Upon resuming at 11:53 a.m.

9 --- L'audience est reprise à 11h53

10 **THE REGISTRAR:** Order, please.

11 This sitting of the Foreign Interference
12 Commission is back in session.

13 **COMMISSIONER HOGUE:** You can go ahead.

14 **--- QUESTIONS TO THE PANEL BY/QUESTIONS AUX PANÉLISTES PAR**

15 **MR. GORDON CAMERON (cont'd/suite):**

16 **MR. GORDON CAMERON:** Gentlemen, we have a
17 number of questions, a good number of questions, probably
18 more than we have time to address them all individually, but
19 helpfully, in a way, many of the same questions were asked by
20 different parties so we're doing our best to amalgamate them
21 together or aggregate them, as you would say, Mr. Fadden,
22 into single questions.

23 Let me begin with one which we've received,
24 as I say, in various forms from several parties, but I'll use
25 one of the formulations to put the question to you.

26 It's probably a question that's more likely
27 to have arisen in the context of CSIS and CSE, but Mr.
28 Forster, we'd welcome your views on this as well, which is

1 how do your agencies approach considerations around
2 intelligence you've received that might suggest that an
3 individual is under threat or potentially is a target of
4 foreign interference, and specifically, if that individual is
5 a parliamentarian?

6 What would you do when you got that
7 intelligence and how would you approach possible disclosure
8 issues in relation to that?

9 **MR. RICHARD FADDEN:** Well, let me take a stab
10 at it, if I may.

11 One, I would make the point that what would
12 happen today is not what would have happened in my day. I
13 think the current government has broadened considerably the
14 instructions they've given to CSIS in particular about
15 forewarning people who may be threatened.

16 But in my day, when I was in CSIS, if I had
17 found out that somebody was under threat, parliamentarian or
18 not, I would have found a way to do something about it. And
19 I don't say that lightly.

20 If it were a parliamentarian, I would have
21 made sure my Minister knows about it and that the Privy
22 Council knew about it. If it was another person, you know,
23 my colleagues and I would have consulted and decided if it
24 was a physical threat, you have to bring in the police
25 because, at the time, the service didn't have the ability to
26 affect physical activities, but rightly or wrongly, I've
27 always thought that CSIS had a mandate to deal with threats.

28 Most of them were systemic or national-level

1 threats, but if individuals were threatened, we would have
2 found a way to do something about it. The more political it
3 was, the more we would have made sure that Ministers know
4 about it.

5 Is that a fair thing to say, Al?

6 **MR. ALAN JONES:** Absolutely.

7 If it involved a physical criminal threat, or
8 threat, threatening is a criminal activity, that would be
9 involved police jurisdiction, usually the RCMP and any
10 contact would go through the RCMP. But the disclosure to a
11 parliamentarian is governed at the headquarters level, it's
12 not something just regional. It would be done locally, a
13 local decision in consultation and probably up through PCO to
14 start with, which also deals with the security of
15 parliamentarians and cabinet ministers.

16 **MR. GORDON CAMERON:** Now, Mr. Forster, if
17 your agency received intelligence to that effect, how would
18 it be handled?

19 **MR. JOHN FORSTER:** Right. So again, remember
20 ours was the ---

21 **MR. GORDON CAMERON:** Oh, got an audio
22 problem.

23 **MR. JOHN FORSTER:** Hello, can you hear me?

24 **MR. GORDON CAMERON:** There you go. We got
25 you now.

26 **MR. JOHN FORSTER:** Sorry. Remember ours is a
27 foreign mandate. So we'd pick that up through foreign
28 collection. The CSE has a series of what they call crows.

1 They're sort of people who just take very sensitive
2 intelligence around to different departments to make sure
3 they've got access and have read it. So we definitely would
4 flag that with a couple of the crows to make sure that that
5 intelligence was read and understood by some of the key
6 agencies.

7 And depending on the target -- since it's a
8 threat and a target, I would want to make sure my colleague,
9 the Director at CSIS, and the National Security Advisor were
10 personally aware of it. Because again, CSE isn't -- doesn't
11 take action on the intelligence, they're a collector of it.
12 But I would certainly want to make sure that the proper
13 agencies who would respond to it were personally aware of it
14 at the very senior level.

15 **MR. GORDON CAMERON:** Okay. Thank you.

16 Gentlemen, during your discussion, and this
17 was particularly a point that Mr. Jones and Mr. Fadden made,
18 you talked about intelligence over time becoming -- the
19 disclosure of the intelligence becoming less injurious over
20 time as it gets older. And the question is, could you expand
21 on that? Is that invariably the case, or is there some
22 intelligence that the confidentiality of which survives the
23 passage of time?

24 **MR. ALAN JONES:** It would be the latter. The
25 -- it's not invariably, it's case by case. As I said, there
26 are some circumstances which protection of the source,
27 particularly human source, would endure for the lifetime of
28 that source. There are other times when the circumstances

1 have changed around that human source, or other circumstances
2 which would mitigate those threats.

3 With a technical source, it's very similar,
4 but not necessarily the same. I'll talk to a section 21
5 warrant that the service would have intercepting the phone or
6 whatever. That would be top secret, the fact that that
7 intercept would exist. It is highly protected, don't reveal
8 that it's happened.

9 After a period of time, if you no longer have
10 that intercept and there's no technological barrier, the risk
11 to revealing that information would be mitigated, unless of
12 course, you had a human source involved in the deployment of
13 that -- of that technology. But it's more likely to happen,
14 but not as an absolute rule, more likely to happen with a
15 technical source than a human source.

16 And I would add to that where the CSIS sits
17 in a different world than police, police notify people after
18 they've intercepted their phone, after a period of time,
19 unless there's reason to continue protecting it under part 6
20 of the *Criminal Code*. That's very a different regime.
21 Right?

22 **MR. GORDON CAMERON:** Very different in the
23 sense that the person is never told when there's been a CSIS
24 interception?

25 **MR. ALAN JONES:** Another question about some
26 of the answers you gave in our session earlier this morning,
27 and Mr. Fadden, in particular, you noted that the PM doesn't
28 get raw intelligence but rather strategic assessments without

1 all of the technical details. And the question is, is the
2 suggestion here that the Prime Minister is missing important
3 parts of the picture when he or she makes their decision?

4 **MR. RICHARD FADDEN:** No, I don't think so.
5 And if I didn't, I should have said there are always
6 exceptions to that rule. I can think of one instance that I
7 can remember where I gave a Prime Minister something from
8 John's old shop, because it was particularly relevant to
9 something that was quite sensitive. But very, very rarely.

10 And as I think all of us were trying to say,
11 a lot of intelligence, including intelligence that has a
12 physical outcome, is built up over time. It's rarely one
13 single piece. It's rarely one source, you know, that tells
14 the whole story. So the objective in dealing with Ministers
15 and the Prime Minister is to pull all of these together so
16 that they can understand what happened. There may be a list
17 behind, you know, an annex which sort of says, you know, this
18 has been going on since time X to time Y, and give some sense
19 of where we got the information.

20 But no, I absolutely don't think that's the
21 case. And to support that view, in all the times that I've
22 worked with Ministers and Prime Ministers I can only think of
23 one instance where I was asked to provide the raw
24 intelligence. So I think if it had been a real issue with
25 Ministers, we would have been asked much, much more
26 frequently.

27 **MR. GORDON CAMERON:** All right.

28 **MR. ALAN JONES:** Could add just one thing to

1 that? Is when you are disclosing the -- or briefing up on
2 any of these issues, at the front of your mind is, why are
3 you telling this person what you're telling them? Because
4 most -- whether it's a Prime Minister or any senior leader in
5 your organization, usually the first thing they'll say is,
6 why are you telling me this and what is it you expect me to
7 do about it? So these are policy decisions, you're briefing
8 up because it's impacting policy, you're not looking for
9 operational direction or operational input.

10 So that would put into context the type of
11 aggregated information or analyzed information, is why are
12 you briefing the Prime Minister on this?

13 **MR. GORDON CAMERON:** Again, on this point. I
14 think it arose out of some of the comments you made this
15 morning, Mr. Fadden, about a higher-level aggregated
16 information being more -- more appropriate for disclosure.
17 And the question was, are you proposing that the Commission
18 ask the government to prepare such reports for the purposes
19 of its use in this inquiry? Or is it that they should be
20 looking for the higher-level aggregated reports?

21 **MR. RICHARD FADDEN:** No, I certainly wasn't
22 suggesting that new reports be prepared. A, it would, you
23 know, with the passage of time it might give a different
24 impression. But I think you'd probably gridlock the system
25 if you started asking for these on a systematic basis.

26 What I was suggesting is that if you have a
27 particular report that you wanted made public and the
28 government is not readily accepting your request, making a

1 suggestion or asking them to make a suggestion on an existing
2 report about how to aggregate up a level or two might be a
3 way to go. But certainly not to create a new report.

4 **MR. GORDON CAMERON:** And again, a number of
5 questions about -- presumably arising in part out of some of
6 the information that we've received -- that the Commission
7 has received over the last few days about the role of the
8 public interest in disclosure, and weighing the importance of
9 confidentiality for national security purposes, and the
10 public interest in disclosure.

11 Where would that fit into the analysis in
12 your agency's consideration of potential disclosures? Where
13 if ever within your agency, would you be assessing the
14 importance to the public of knowing this information when
15 you're deciding what to disclose to the public?

16 **MR. RICHARD FADDEN:** Well, in theory it takes
17 place at every level. But in practical terms, I'm not sure
18 it can be, you know, utilized equally every time a piece of
19 information is classified.

20 My sense is that, you know, this issue
21 becomes important when for some reason or other it -- the
22 file is raised. It may be for legal reasons, it may be for
23 tactical reasons, it may be for policy reasons, it may be
24 because there's a media interest.

25 But as a general routine, you know, the
26 individuals who classify reports are quite junior and they
27 have a series of criteria, and they apply them, or the
28 computer applies them for them. And answering the question

1 that you pose can either take place because an individual
2 file is pulled, and you know, a more senior person is asked
3 to focus on it. Or because there's a declassification
4 process that's ongoing, and that takes place in headquarters
5 at a fairly senior level.

6 In other words, the authority to classify
7 information is fairly widely delegated. The authority to
8 lower the classification, or to declassify it is much, much
9 less widely delegated and it would be restricted to
10 headquarters. And if a matter were at all sensitive, it
11 would go to quite senior levels.

12 **MR. ALAN JONES:** If I could add, from an
13 operational perspective, when there is a judicial, quasi-
14 judicial process and a request for disclosure, there are
15 specialized areas, policy and legal, that deal with those,
16 that process. It is not dealt with by the operational area.
17 So even as a senior operational leader, I would never have
18 been asked how much do you want redacted and how much do you
19 want left in the clear. That would not be an appropriate
20 question for me to become involved in as an operational
21 manager. That would be managed by those who were managing
22 the relationship with the judicial proceeding or whatever.
23 You might be asked what to do a damage -- a potential damage
24 assessment around specific pieces of information if they were
25 to be disclosed, what is the risk associated to that, but you
26 would not be asked in the operational sense should or
27 shouldn't we be disclosing to the maximum or the minimum.
28 That is handled otherwise, and those decisions are made

1 there. I'm not sure if that's useful, but that's ---

2 **MR. GORDON CAMERON:** Yes, thank you. Mr.
3 Forster, did you -- this seems -- the area of balancing the
4 public interest seems to arise more at the -- more downstream
5 from the agency you were in, but do you have anything to add
6 to that?

7 **MR. JOHN FORSTER:** Yeah, I would agree with
8 both Dick and Alan's comments. The other two layers in this
9 I think that are important, depending on the sensitivity and
10 the views of the inquiry and the originator, the Department
11 of Justice would also play a role in this if they felt that
12 the agency was maybe not disclosing everything it could. The
13 justice lawyers would also intervene and make sure -- provide
14 a bit of a challenge to it, have you considered this. And as
15 Dick said, I think as it -- it would get elevated to a
16 reasonably senior level to make sure that there's a broader
17 perspective taken to it than just the subject matter expert
18 who would have more of a narrow kind of focussed view on, you
19 know, does this disclose my source, or my information, or my
20 technique. So the Justice and PCO would also, you know, play
21 a bit of a challenge function there, or should play a bit of
22 a challenge function there to the agencies to make sure that
23 the broader public interest and views are also considered.

24 **MR. GORDON CAMERON:** Thank you. And we had
25 several questions arising out of your comments, Mr. Jones,
26 with respect to what went on in the Arar Inquiry, and in
27 particular, whether we have lessons to learn from that
28 process, and as I'll phrase one of the questions, do you

1 think the matter was adequately described by Professor West
2 yesterday or do you have anything to add to that?

3 **MR. ALAN JONES:** I don't have anything to
4 add. I think Professor West did an excellent job of
5 outlining the relevant part of Arar for -- regarding
6 disclosure and the process.

7 **MR. GORDON CAMERON:** Now some questions about
8 -- for either Mr. Jones or Mr. Fadden about the division
9 within your agency between -- this came out of your
10 discussion of the terrorism investigations, but we are here
11 in a foreign interference context, so could you describe how
12 your agency divides its functions as between investigations
13 of those two fields of interest, between terrorism and
14 counterintelligence or foreign interference?

15 **MR. ALAN JONES:** I mentioned earlier that the
16 *CSIS Act* defines a lot of how CSIS operates and how it's
17 organized. Section 2, finding threats, A, B, C, and D. You
18 essentially have operational branches and operational branch
19 that deals with A, which is espionage, C, which is terrorism,
20 which is the big, you know, a big file. The foreign
21 interference file tends to fall more under the A section,
22 although it's at section B of the Act as a specific threat.
23 It has never been a particularly large program within the
24 service. Counterterrorism, obviously, dominated for decades
25 the investigative capabilities and resources of the service.
26 CSIS always maintained operational capability under 2-A and
27 2-B, primarily in its counterintelligence branch. Even
28 during the years post-9/11 when counterterrorism became

1 everything for many agencies, the service maintained a
2 capability, albeit reduced, on its espionage and its foreign
3 intelligence -- foreign interference investigations while
4 some of our allies reduced theirs to almost nothing, to a
5 nub. And, in fact, over a period of years, as other larger
6 agencies in other countries began to get back into the
7 espionage and foreign interference areas, they did approach
8 the service because they were aware that we had maintained
9 some capability, reduced from what it had been, but we did
10 not turn the lights out, so to speak, on that program. And
11 that meant we could keep expertise, language capabilities,
12 knowledge and some continuity on those files even while the
13 service was under tremendous pressure with counterterrorism
14 program. But they are kept separate.

15 There are, of course, some areas where
16 foreign interference overlaps with the terrorism program.
17 There are some countries which are involved in state-
18 sponsored terrorism who play in the peripheries of other
19 terrorist activities. So you have a terrorist investigation,
20 but yet they do engage in political meddling in Canada at the
21 same time. So that's a time that was a shared responsibility
22 between some of the counterintelligence branch and the
23 counterterrorism branch, and sometimes you just make
24 arbitrary decisions as to which branch will hold that file,
25 but there is sometimes an overlap.

26 **MR. RICHARD FADDEN:** Can I add a thought?
27 Just about foreign interference. Essentially, rather
28 difficult to deal with because it means a desire to influence

1 under the radar. So if you look at the spectrum of human
2 contact between just a social gathering and foreign
3 interference with a threat of violence, you have a whole
4 bunch of things in the middle including diplomacy. So in the
5 case of terrorism, you know, if anybody's putzing around with
6 a bomb or something like that, it's pretty clear you need to
7 pursue it. But if the Consul General of country X is talking
8 to somebody over lunch, it could be foreign interference of
9 the worst sort, or it could be a social meeting where they're
10 sort of saying, well, you know, our two countries should get
11 together and agree on this particular policy. So if there's
12 no threat of violence involving the diaspora at issue, simply
13 catching people, you know, who are engaged in active foreign
14 interference of one sort or the other is in some ways more
15 difficult than terrorism where you have sort of something
16 kinetic to deal with because in many ways you're just dealing
17 with conversations. There could be implied threats. There
18 could be implied benefits and whatnot. But in many cases, I
19 think service or the RCMP have discovered FI efforts simply
20 because they related, as Al had said, to other inquiries.

21 So I just want to stress that, you know,
22 people who say, well, you know, it's obvious, you know, that,
23 you know, the Consul General of country X was talking to
24 somebody, it's foreign interference, well, it isn't obvious.
25 It's part of the job of diplomats. I was a diplomat briefly
26 early in my career and it was my job to go out and try and
27 influence that country. So finding where it's situated on
28 the spectrum is actually quite difficult to do. And not

1 unreasonably, Canada doesn't want to offend foreign
2 governments unnecessarily. So you have to find something to
3 hook on before the service or the RCMP can become actively
4 involved.

5 So all I'm trying to do is to suggest that
6 there's a spectrum here, and before you can become actively
7 involved, you have to make sure that there's a serious
8 possibility of foreign interference. And as Alan suggested,
9 sometimes it's easier if you're -- it's connected with
10 another investigation.

11 **MR. ALAN JONES:** And if I add to that, it
12 gets even more complicated when countries use proxies and
13 non-diplomatic actors to carry out foreign interference
14 campaigns.

15 **MR. GORDON CAMERON:** Can you elaborate on
16 that, Mr. Jones?

17 **MR. ALAN JONES:** Well, foreign journalists
18 sometimes, certain media representatives could be part of a
19 state campaign. I mean, to be very specific, I have a
20 certain amount of exposure to the activities of the Republic
21 of China in foreign interference in Canada. They had a
22 multi-prong -- they have a multi-prong approach. It might be
23 diplomats at the Consulate, but it might be trade
24 representatives, journalists, tourism groups who are just
25 individuals coming to Canada. It may happen in -- the
26 interference may actually happen in China itself, where they
27 have coercive abilities because they can reach families or
28 reach -- meet dual citizens who are travelling to China and

1 back to see family or to do business. So it's not just
2 simply, as Dick said, what defines an aggressive political
3 campaign, or aggressively standing up for your country, or
4 aggressively trying to get economic -- do economic lobbying.
5 At which point does it become foreign interference and
6 meddling? Clearly, if it's interfering with an election,
7 well, that's -- you know, that's -- you're into that category
8 where, like, terrorism, it's pretty clear if someone puts a
9 bomb somewhere. But the gradience between that something
10 that stark and benign or acceptable activity, it's --
11 activities, there's a lot of activities in the middle.

12 **MR. JOHN FORSTER:** Can I just add a point as
13 well on this?

14 **MR. GORDON CAMERON:** Please do.

15 **MR. JOHN FORSTER:** Yeah. Just the other
16 element of foreign interference is, not so much the human
17 context inside Canada, or whatever, but the online campaigns
18 that are waged. So disinformation campaigns that could be
19 state sponsored. The very attribute -- so CSE would be
20 trying to track and report on that activity. It's very
21 difficult. You can, you know, send that stuff through
22 umpteen number of servers around the world to cover its
23 source, or they'll -- countries may use third parties to do
24 it on their behalf. But there's a disinformation component
25 to the foreign interference, foreign influence that shouldn't
26 be forgotten, and that will only get more difficult as AI
27 technology advances further.

28 **MR. GORDON CAMERON:** Thank you. Now -- thank

1 you, Mr. Forster, for bringing us, I think -- I want to bring
2 the discussion we've just had back to the question of what
3 can be disclosed. How do we deal with the information that
4 the Commission's going to be looking at, and get as much of
5 it out to the public? And the question that we were touching
6 on earlier is balancing the public interest, et cetera.

7 And a question that's come in from several
8 different parties in different ways is, whether it would be,
9 and if so, how it would be important for the Commission to be
10 in touch with diaspora communities to get their perspectives
11 on foreign interference and how it affects them, and thus,
12 how it might affect the public interest in disclosure of the
13 intelligence about foreign interference?

14 **MR. RICHARD FADDEN:** Well, to be blunt, I
15 think if you don't develop an interest in diaspora points of
16 view, I think you will be missing an important component of
17 your mandate. I mean, the threats to, you know, diaspora
18 communities for the purpose of advancing, you know, foreign
19 state objectives I think is becoming increasingly clear.

20 And one of the difficulties that we have is
21 that most members of these diasporas come from a background
22 where dealing with the police or the security services is the
23 last thing they want to do. So even though they are
24 threatened, they feel badly, they want to do something, you
25 know, calling up CSIS or the RCMP, or anybody else, given
26 their experience with security services back home, is not
27 something they want to do.

28 So we don't have as many of those contacts as

1 I think we should have. So I would very much urge the point
2 of view that the Commission should have an active outreach
3 program, and possibly one that provides them with
4 confidentiality because people are scared. I'm generalising.
5 Not everybody is, but you know, members of some diasporas are
6 just plain scared.

7 I would argue also that one of the things
8 that government should do, and I hope the Commissioner will
9 consider this in her recommendations, is to develop a means
10 for diaspora community members to communicate with the
11 government confidentially because walking into an RCMP
12 substation or to a CSIS regional office, they don't want to
13 do by and large. And so the only time we find out about this
14 is when something goes very wrong so it's too late to do
15 anything about it.

16 So long answer to your short question, but I
17 very much hope that you don't miss the opportunity of
18 speaking with diaspora representatives.

19 **MR. GORDON CAMERON:** Mr. Jones, do you
20 have....

21 **MR. ALAN JONES:** I agree with that. I have
22 nothing to add.

23 **MR. GORDON CAMPBELL:** Yes.

24 And Mr. Forster?

25 **MR. JOHN FORSTER:** Yeah, I would certainly
26 echo Dick's comments.

27 **MR. GORDON CAMPBELL:** Okay.

28 Commissioner, I am in the happy situation of

1 having completed all of the questions that the parties
2 submitted, though in many cases they were aggregated
3 together. Some of them will be punted to tomorrow's panel,
4 where we have the incumbent equivalent of these gentlemen,
5 and the questions will be more appropriate for them.

6 But with that said, that is as much as I have
7 for this panel.

8 **COMMISSIONER HOGUE:** So thank you. I imagine
9 everyone will be happy to be free for lunch and for the
10 afternoon.

11 So see you all tomorrow morning at ten.

12 **THE REGISTRAR:** Order, please.

13 This sitting of the Foreign Interference
14 Commission has adjourned until ten tomorrow.

15 --- Upon adjourning at 12:20 p.m.

16 --- L'audience est ajournée à 12h20

17

18

19

20

21

22

23

24

25

26

27

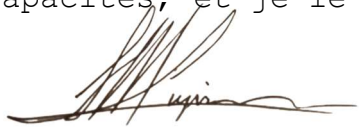
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

C E R T I F I C A T I O N

I, Sandrine Marineau-Lupien, a certified court reporter,
hereby certify the foregoing pages to be an accurate
transcription of my notes/records to the best of my skill and
ability, and I so swear.

Je, Sandrine Marineau-Lupien, une sténographe officiel,
certifie que les pages ci-hautes sont une transcription
conforme de mes notes/enregistrements au meilleur de mes
capacités, et je le jure.



Sandrine Marineau-Lupien