



**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 38

ENGLISH INTERPRETATION

Held at :

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

Wednesday, October 23, 2024

Tenue à:

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

Le mercredi 23 octobre 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
Leila Ghahhary
Benjamin Herrera
Howard Krongold
Hannah Lazare
Jean-Philippe MacKay
Kate McGrann
Emily McBain-Ashfield
Hamza Mohamadhossen
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

III

Appearances / Comparutions

Commission Staff / Personnel de la commission	Annie Desgagné Casper Donovan Hélène Laurendeau Michael Tansey
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 Sébastien Lafrance Nancy Miles Sujit Nirman
Human Rights Coalition	David Matas 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

IV

Appearances / Comparutions

Jenny Kwan

Sujit Choudhry

Mani Kakkar

Churchill Society

Malliha Wilson

The Pillar Society

Daniel Stanton

Democracy Watch

Wade Poziomka

Nick Papageorge

Canada's NDP

Lucy Watson

Conservative Party of Canada

Nando De Luca

Chinese Canadian Concern Group on
The Chinese Communist Party's
Human Rights Violations

Neil Chantler

David Wheaton

Erin O'Toole

Thomas W. Jarmyn

Preston Lim

Senator Yuen Pau Woo

Yuen Pau Woo

Sikh Coalition

Balpreet Singh

Prabjot Singh

Bloc Québécois

Mathieu Desquilbet

Iranian Canadian Congress

Dimitri Lascaris

V Table of Content / Table des matières

	PAGE
ROUNDTABLE : CANADA’S NATIONAL SECURITY APPARATUS / TABLE RONDE: L’APPAREIL DE SÉCURITÉ NATIONALE DU CANADA	1
Panel moderated by/Panel animé par Dr. Leah West	1
Presentation by/Présentation par Mr. Richard Fadden	3
Presentation by/Présentation par M. Daniel Jean	11
Presentation by/Présentation par Ms. Lex Gill	20
Presentation by/Présentation par Mr. Alan Jones	31
Presentation by/Présentation par Dr. Stephanie Carvin	45
Presentation by/Présentation par Dr. Maria Robson-Morrow	57
Open discussion/Discussion ouverte	67
 ROUNDTABLE : ENFORCING, DETERRING AND PROSECUTING FOREIGN INTERFERENCE ACTIVITIES / TABLE RONDE: MISE EN OEUVRE, DISSUASSION ET POURUITE DES ACTIVITÉS D’INGÉRENCE ÉTRANGÈRE	 110
Panel moderated by/Panel animé par Dr. Leah West	110
Presentation by/Présentation par Dr. Alex Wilner	111
Presentation by/Présentation par Mr. Bob Paulson	119
Presentation by/Présentation par Mr. Croft Michaelson	124
Presentation by/Présentation par Dr. Michael Nesbitt	130
Presentation by/Présentation par Mr. Rob Currie	138
Open discussion/Discussion ouverte	146

Ottawa, Ontario

--- The hearing begins Wednesday, October 23, 2024 at 9:02 a.m.

COMMISSIONER HOGUE: [No interpretation].

Good morning. Welcome, and thank you.

I will have the opportunity to thank you at the end, but.

Today the roundtable is entitled a very simple title, actually, today, "Canada's National Security Apparatus". And we are lucky enough for having six guests this morning that are well -- widely recognized, actually, as experts in this field for various reasons. Some are coming from the academic world, and others are coming from the field. And the table will be moderated by Leah West, and she will introduce more deeply the various participants -- panellists, I should say.

--- ROUNDTABLE: CANADA'S NATIONAL SECURITY APPARATUS:

--- PANEL MODERATED BY DR. LEAH WEST:

DR. LEAH WEST: Sure.

The Commission is mandated to examine and to assess the capacity of the federal government, including its intelligence agencies, to detect, deter, and counter foreign interference in Canada's democratic processes.

The Commissioner's initial report noted difficulties in identifying, confirming, and attributing foreign interference, especially online activities, and the process of making intelligence-informed decisions in response to that threat.

1 The report also discussed the challenge of
2 effective communication of foreign interference intelligence
3 and information to stakeholders, the public, and to those
4 most likely being vulnerable to foreign interference.

5 This aspect of the Commission's mandate
6 raises several questions, including:

7 "Do Canada's intelligence agencies
8 have the legal authorities, technical
9 capabilities and resources necessary
10 to detect, deter and counter foreign
11 interference? What measures can be
12 taken to make the relationship
13 between Canada's intelligence
14 agencies and government decision-
15 makers stronger? What measures can
16 be taken to improve communications of
17 intelligence and the understanding of
18 the implication of foreign
19 interference threats with external
20 stakeholders, including diaspora
21 communities? What is the current
22 public perception of Canada's
23 national security agencies and, if
24 there is a lack of trust, how has
25 that affected their ability to deter,
26 detect and counter foreign
27 interference, and how should that
28 trust be rebuilt? And should

1 Canada's national security agencies
2 better communicate with the public
3 about the threat of foreign
4 interference and how to protect
5 themselves against it?"

6 So I'm very pleased to introduce our six
7 panellists today. I'm going to introduce them in the order
8 that they will be giving their opening remarks.

9 So we'll be starting with Mr. Richard Fadden,
10 former National Security Advisor and Deputy Clerk, and former
11 Director of the Canadian Security Intelligence Service.

12 Mr. Daniel Jean, former National Security and
13 Intelligence Advisor to the Prime Minister, and former Deputy
14 Minister of Global Affairs Canada.

15 Ms. Lex Gill, a senior Fellow at the Citizen
16 Lab at the University of Toronto.

17 Mr. Alan Jones, former Assistant Director of
18 the -- of Canadian Security Intelligence Service.

19 Professor Stephanie Carvin, Associate
20 Professor at Carlton University.

21 And Dr. Maria Robson-Morrow, who's the
22 program manager at the Harvard Intelligence Project.

23 Each panellist will address these questions
24 in an opening statement and, should time permit before the
25 break, I'll invite a round of responses.

26 So having said that, we'll turn the floor
27 over to Mr. Fadden.

28 **--- PRESENTATION BY MR. RICHARD FADDEN:**

1 **MR. RICHARD FADDEN:** I would like to start
2 with a couple of what I consider to be meta statements, so
3 they don't directly address the structure issues that Leah
4 has mentioned.

5 I would argue that, generally speaking,
6 outside of the Ottawa bubble, a few academics and a few
7 journalists, the clear and present danger presented by
8 foreign intelligence to our democratic processes is not
9 acknowledged, and I think to the extent that it is not
10 acknowledged and that politicians pay attention to what
11 people think outside of the bubble, I would suggest that it
12 will help the implementation of your recommendations if, on
13 the basis of what you've read and heard, you can say in your
14 report there is a clear, present and serious danger. This
15 has been repeated any number of times, but if you look at
16 polling, generally speaking, it's not accepted that it is a
17 clear and present danger.

18 I think for the countering activities to
19 succeed, the country at large has to be more aware than they
20 are now, I would submit.

21 Second point, I think it will be important as
22 you formulate your recommendations to recognize -- I refer to
23 your FI efforts as within your mandate -- that your FI
24 recommendations will be situated by government within the
25 broader era of foreign intelligence, with foreign
26 interference, which is really quite broad. So expecting the
27 government to go off and set up a whole set of separate
28 institutions, separate legislation and ignoring the rest of

1 FI I think will present governments with challenges and
2 possibly with reasons for not proceeding. So integrating the
3 two, I think, to the extent practical, will be very
4 important.

5 I think that our adversaries who try and
6 engage in foreign interference are sophisticated, they're
7 persistent and they're very well resourced. The only way
8 that we are going to successfully counter them is if we have
9 a whole-of-government and, indeed, a whole-of-society
10 perspective. And I would argue, I may be a bit at odds with
11 some of my colleagues here, that there is too much of an
12 emphasis on the intelligence or national security community.

13 There is clearly a role for national security
14 and intelligence, but I would say that dealing with foreign
15 interference has to take place on a range of activities: at
16 one end, the RCMP and the courts prosecuting people and
17 sending them to jail if need be, at the other end, some
18 institution or other trying to deal with public education and
19 trying to relieve people's concerns about what is happening,
20 and a whole range of other things in the middle.

21 My point being that I know this is about
22 national security, but I worry a little bit that there's too
23 much emphasis on national security. We have to involve other
24 components of both government and civil society.

25 I think recognizing -- if you accept what
26 I've just said, foreign interference is an ongoing and
27 permanent thing. It is not limited to electoral periods,
28 it's not limited to writ periods, it's ongoing, all the time.

1 And I think if we don't take that point, we're going to miss
2 something very seriously.

3 So slowly coming to the issue of
4 institutions, the role of political parties is obviously
5 very, very important, and we have to find a way of involving
6 them and countering activities without negatively affecting
7 their role in our democratic process, but I think key to this
8 will be keeping Ministers and the Public Service out of this
9 effort to the extent possible.

10 I think it is unreasonable to expect partisan
11 Ministers and partisan players to all of a sudden push a
12 button when they're dealing with foreign interference in
13 these matters and expect them to be entirely non-partisan.
14 And I'll come back to this when I talk about a panel, but I
15 think it's unreasonable to ask public servants who spend
16 their entire lives trying to stay out of partisan politics
17 to, all of a sudden, be the ones who determine what may or
18 may not be done.

19 So political parties, I think, have to be
20 brought between the ambit of regulation or law, but we should
21 set them up as self-regulating and have the panel that I will
22 talk about in a minute be the overseer of this activity.

23 I also would argue that the definition of a
24 political party may be one that requires a little bit of
25 review. The Liberal Party of Canada, for example, has almost
26 become a movement. You don't have to register, you don't
27 have to pay a fee. I'm not judging whether this is good or
28 bad, but I'm not sure it's going to be easy to have

1 countering activities against movements as opposed to
2 relatively structured political parties.

3 So this gives rise to the question, I think,
4 of what organization can take an interest in overseeing
5 countering activities on a permanent basis.

6 As I said, I think Ministers and Public
7 Service should be kept out of this, so I think the panel as
8 it's presently constituted should be abolished. I would
9 argue that, as I've just said, it's unfair to ask public
10 servants to do that.

11 The Brits have an expression, "the great and
12 the good", and this means, basically, people who have been in
13 public life who've retired and aren't as partisan. I suspect
14 that, with a bit of effort, the government could find a few
15 of these even in Canada, and I would put them on this panel.
16 You know, a former Minister who's, you know, become a
17 statesman, a public servant who's been around for a long
18 time, an academic who has an interest in these matters.

19 I would constitute a panel made up of these
20 people, give them a small secretariat, and make them
21 permanent. I think anything less than permanent oversight of
22 the subject matter is not going to work.

23 I think its operational arm should be a
24 reconstituted Chief Electoral Officer, who should have his
25 writ or her writ extended to political parties, but there
26 should be a relationship between the panel and the Chief
27 Electoral Officer in order to get things done.

28 But I think the particularly important part

1 on this is that the panel should access and have the right to
2 know anything that the intelligence community or the police
3 or anybody else collects on this subject, and they should be
4 able to dialogue and deal with the Chief Electoral Officer on
5 this basis. It has the advantage, I think, of providing
6 permanency and keeping Ministers and public servants out of
7 this issue.

8 One of the issues that we've been asked to
9 look at is whether or not currently the law is sufficient to
10 provide the intelligence communities and others to deal with
11 these issues. I'm not sure I can answer that question
12 absolutely, but I'm a firm believer in making use of the
13 authorities you have before creating new authorities, and I
14 don't think we're doing this across the board.

15 C-70 has barely been registered by the
16 institutions. They're still thinking about how to do it.

17 CSIS has a lot of powers that its risk
18 aversion doesn't allow it to use all the time. I think
19 that's also true of the Mounties. So I would argue that it
20 would be helpful if your recommendations included strong
21 injunction to institutions that currently have authority, use
22 it. Don't be so risk averse, but use it in conjunction with
23 the panel of these great and goods that I'm recommending that
24 you consider.

25 The one element where I do think there is the
26 beginnings of a consensus, I don't think all of these
27 institutions have enough resources. Virtually every other
28 year, there's a new mandate being given to the intelligence

1 communities, and this is a significant one. They still have
2 to worry about traditional espionage, other forms of FI,
3 terrorism and a bunch of other things, and I think it would
4 be unreasonable to expect them to treat this seriously.

5 I think, as I was alluding earlier -- I would
6 argue there's no such thing as national security because
7 there's always a subnational and an international component,
8 and in this respect, I think if we're going to counter your
9 FI efforts, we have to involve the provinces, we have to
10 involve civil society or it's not going to work.

11 The federal government is the most distant
12 level of government from the people in this country, and they
13 find it very difficult to deal on an ongoing basis. Some
14 institutions do better than others, but it was, I think, very
15 similar to how we tried to deal with terrorism.

16 The federal government did a bunch of things
17 at one level, but civil society was best placed to try and
18 deal with people who were thinking about it who are on the
19 verge of doing something negative. So finding a way to have
20 the panel and the Chief Electoral Officer and any other
21 department engage, liaise and actively collaborate with the
22 provinces and civil society I think it's a *sine qua non* to
23 success in this area.

24 The federal government alone, I would submit
25 strongly, cannot counter FI successfully. They just cannot
26 do it. I think this has been proven to be the case in a
27 number of other countries that have also tried to do these
28 things.

1 Just coming back to my panel for a moment, I
2 forgot, I think it should be enshrined in law, but it would
3 be also good if we could do this within our lifetime. So
4 asking the Government of Canada to use existing executive
5 authorities to put it into place, the *Public Inquiries Act* is
6 one way of doing it. If they actually galvanize themselves,
7 it seems to me it would be possible to have such a panel in
8 place before the next federal election, assuming it doesn't
9 happen until May or June.

10 I'm not optimistic, but if we're serious
11 about this, you know, we should get on with it and do
12 something as soon as we possibly can.

13 Lastly, and this is another meta point,
14 having been the recipient on behalf of governments throughout
15 my career of Royal Commission and inquiries' recommendations,
16 I would strongly urge you to prioritize your recommendations.
17 The one thing that governments will do, any Party, is pick
18 and choose the ones that are the easiest or the one that
19 present the most advantage to themselves, so if you
20 prioritize and give them short-, medium-, and long-term
21 timeframes in which to be implemented, I think it will be --
22 you will make it easier for government to implement and to
23 avoid going out.

24 I think I'll stop there, and I look forward
25 to any questions that you might have.

26 **COMMISSIONER HOGUE:** Thank you.

27 **MR. RICHARD FADDEN:** Thank you.

28 **DR. LEAH WEST:** Mr. Jean.

--- PRESENTATION BY MR. DANIEL JEAN:

MR. DANIEL JEAN: Thank you very much, Madam Commissioner. Thank you for the invitation.

COMMISSAIRE HOGUE: [No interpretation].

MR. DANIEL JEAN: The Phase 1 of the Commission did a very good work, and I think with respect to it, I think now you're in the most critical phase right now where you'll be able to guide us with respect to prevention and deterrence for foreign interference. The security apparatus has to work, and we're going to be discussing that.

Before doing that, I have two key messages, and a lot of the points that were brought forward will be similar to what Mr. Fadden had said. But two important points; first, I will be talking about improvements that needs to be done with the intelligence (indiscernible). I do admire the work but I think [no interpretation]

MS. LEILA GHAAHARY: Excuse me. Mr. Jean, please, could you slow down for the interpreters?

Thank you.

MR. DANIEL JEAN: Okay. I thought I was slow enough, but fine.

(LAUGHTER)

MR. DANIEL JEAN: So first of all I think I do appreciate their dedication, but I think it takes two to tango, as Mr. Fadden said. So there have -- people have to be ready to go ahead and work. And that doesn't mean that I don't respect the fact that politicians are very -- are working very hard for Canadians, but I do think that takes a

1 lot of courage.

2 So I don't want to repeat everything that I
3 said Monday. And Mr. Fadden has said many things, but the
4 most important point, the fact right up until now we have
5 seen through the Inquiry that foreign interference happens
6 well before the elections, and I think there's, of course,
7 the nominations process that is particularly affected, and
8 what Dick said also with respect to the problems with
9 democracy, it's very -- it goes above and beyond just the
10 problem with elections, and it's important.

11 Right now we have three criminal processes in
12 court with respect to intimidation, harassment of the
13 diaspora. India, China, and we know that there are other
14 countries that are also involved. I have decided to respond
15 to the issues that we have seen before the Commission. I
16 would like to identify what I really feel is important with
17 respect to national security. So I've identified six.

18 The first I've talked about it, the lack of
19 national security culture, which means that we're not putting
20 a lot of attention on the most strategic evaluations, and we
21 already do our updates of our legal tools belatedly. And I
22 think that we need a quality intelligence, and it has to be
23 -- Madam Commissioner, we spoke about it has to be
24 trustworthy.

25 And, thirdly, the dissemination for key
26 players and also for those responsible within government so
27 they can guide the actions.

28 Fourth, I think that we needed a more

1 systemic approach to ensure that the greatest threats are
2 really brought forward to -- whether it's to the government
3 or the political parties, and there also has to be a system
4 set up so that we can document the awareness of such things.

5 Fifth, we live in a world where the Jewels of
6 the Crown are more and more outside of the government. So it
7 is necessary for the safety officer to change their culture
8 to better alert and support Canadians against the foreign
9 interference.

10 And sixth, the importance of having a good
11 horizontal governance at Cabinet and amongst the Public
12 Service.

13 So the first. I'm going to go quickly; I
14 spoke about it Monday. I agree with Dick, we don't have a
15 national security culture. If the Canadians are not
16 interested, then the politicians won't be interested. And,
17 unfortunately, means that Canadians, you know, will become
18 interested when there's a crisis, same for the politicians.
19 So we have a tendency to always draft the laws in a time of
20 crisis, like what happened after the RCMP scandal in 1989.
21 And now we have Bill C-70 that came up very fast because we
22 have a crisis.

23 There is an effort that it made with the
24 creation of a national security council to try and change
25 this culture. It is still very early so we can't really
26 assess it.

27 A second challenge, developing quality
28 intelligence products with clearly stated degrees of quality.

1 The work of your Inquiry, especially when we look at the
2 different interpretations made by the public, especially with
3 regard to the material supporting the report of the
4 Parliamentarians Committee on National Security and
5 Intelligence show that people can read the same documents and
6 come to different interpretations.

7 As far as I'm concerned, maybe the people who
8 draft those reports draft for themselves rather than for non-
9 experts. That is not a problem only in national security. I
10 could talk about this for 35 years, so we have to change
11 this.

12 And there's also the issue that you raised
13 that was already in my remarks, so it's a very good point; it
14 cannot happen in a void. Intelligence is independent, the
15 collection, analysis, but cannot be done in a void. There
16 has to be an exchange with the audiences. Intelligence is
17 neutral in terms of policies and operations. They have to
18 respect independence, but they will be an added value.
19 Products will be better and we will be better served.

20
21 If -- you know, a lot of progress was made in
22 the capacity of the National Security Committee to work
23 horizontally. In terms of intelligence this is where we
24 should look for a lot of improvement.

25 Third, dissemination of those products with
26 key civil servants and relevant political authorities to
27 guide actions if necessary and possible. If necessary and
28 possible, well, 95 percent and more of the intelligence

1 reports that we read, they do not call for any action, or if
2 they call for an action, often agencies don't want to do it
3 because they must protect the methods, the sources, and
4 ongoing investigations. This is why I say, if necessary and
5 if possible.

6 When I say that we must bring those documents
7 to the attention of the audiences, I'm talking beyond the
8 traditional audiences. Of course CSIS must constantly work
9 with the departments in their community but also with the
10 departments of economy.

11 You have a nice case study, the Commission
12 could be inspired by this, on how Canada's response to
13 economic security since 2016. Departments that would not
14 talk to each other, Innovation, Science and Technology, work
15 with National Security. Look at the statistics on *Canada*
16 *Investment Act* and you will realize that you have a very
17 beautiful case study where the system worked. And why did it
18 work? Because the civil servants worked together, they
19 managed to engage the Cabinet, and Cabinet worked.

20 A letter of mandate from the Minister saying
21 that we must increase foreign investments at a time when it
22 came from China, and it was quite a concern. The system
23 worked perfectly. You should include a paragraph in the
24 report.

25 And now another important point, there's a
26 lot of reports that political class is busy, the Ministers,
27 the Prime Minister are busy; they cannot read everything,
28 know everything. So we have to choose what we show them, but

1 also same thing for political parties, the important players,
2 parliamentarians. Now we must find a way to make the system
3 more accountable for everyone. We must know how to describe
4 what has been briefed. The contents should be known, not
5 necessarily publicly but known, and it must be documented.

6 My fifth point, we live in a world where the
7 Jewels of the Crown are outside of the government more and
8 more; I know that Maria will talk about it. So for safety
9 agency they need a fundamental cultural change. What do I
10 mean when I say the jewels are more and more outside of the
11 government? Sensitive technologies and the private sectors
12 and research and academic sectors, the manipulation of the
13 systemic information that can divide and weaken the trust in
14 our democratic institutions; the harassment and bullying of
15 the diasporas to muffle those people, trying to influence
16 them. The fact that some of those Jewels of the Crown and
17 vulnerabilities and found in various government levels,
18 provinces, territories, municipalities and so on.

19 Under Michael Warnick a lot of effort has
20 started with the other Clerks as well where there are
21 exchanges with provinces and territories, but it has to
22 become more systemic and also at lower levels of government.

23 Now, they should be able to use the existing
24 authorities, and the new authorities, Bill C-70, for
25 instance, will provide this to CSIS to share the nature of
26 the threat and its manifestation while protecting the
27 sources, the methods, and the investigations.

28 This requires a deep cultural change. The

1 way we do this is in the way we recruit, we train, and we
2 encourage with the proper incentives, what we want from that.

3 And I agree with Dick as well when he says
4 that we need to have a national security lens that is not
5 just up to national security. People in other departments
6 must also do it, and this is what we managed to do for
7 economic security.

8 So what could that mean for a few of the
9 players? Let's think about CSC. It was interesting, CSC was
10 the most secret government agency, but cyber security threat
11 forced them with the creation of the Cyber Security Centre to
12 really have a dialogue with the population on the cyber
13 threat. So they've changed the way they work, but this -- in
14 the knowledge continuum alert people. But we must go further
15 in terms of resilience. If we had a JBS Foods where 30
16 percent of beef and pork was paralyzed, if you have, you
17 know, an oil and gas pipeline paralyzed by a cyber attack,
18 we'd be ready to act.

19 For CSIS the change is important because so
20 far they were handcuffed. They should have been able to do
21 things, but the law did not allow them to do it. They went
22 as far as they could, but also because they're internal
23 culture is to play inside baseball. And they really need an
24 important cultural change.

25 Now, concerning RCMP, and I don't want to
26 provide any recommendations on the structure of the RCMP but
27 we have to solve the conflict with regards to the capacity of
28 the RCMP to play its role fully as the federal police when

1 most of its attention and most of its resources, 70 percent,
2 is police, contractual police. So we must have the courage
3 to find a solution.

4 And my last point, maybe the most important
5 one given the panel, horizontal governance.

6 First, regarding civil servants. Huge
7 progress were made since the creation of the role of National
8 Security Chief in 2003. Specifically a consistent and
9 coordinated response to crisis, very well.

10 I said that we must improve intelligence; it
11 shouldn't be done in a void. With regards to policy
12 developments, it is not perfect, but still there are efforts
13 being made to make things more horizontal in terms of policy
14 development, which is the government's mandate. And also
15 having an eye on what is coming. This is what enable Canada
16 and the US to be the two countries who reacted faster on
17 economic security issues.

18 Now, as I said earlier, there's never been a
19 space, a time in former governments, regardless of the
20 parties; they tried at one point to create Cabinet committees
21 for strategic discussions, it did not occur. Now we have a
22 Strategic Security Council. I hope that that will mean that
23 we will win this space, but it's still too early to see.

24 Now, the role of National Security, which is
25 key in this horizontal governance matter for civil servants
26 and the link with the Prime Minister and his Cabinet. As I
27 said Monday, I have no objection in the suggestion of
28 including this in the law, but our expectations may be a bit

1 exaggerated because unless we challenge the Westminster model
2 where responsibilities are under the Ministers and their
3 institutions, that will simply confirm the role of the
4 function. And the role of the function is the mirror of the
5 Privy Council three roles.

6 First, independent advice to the Prime
7 Minister. Second, support and council advice to the Cabinet,
8 a bit like the Clerk working very closely. For instance, to
9 bring *National Security Act* in 2019 that I did with Minister
10 Goodale at the time under Minister Malcolm Brown. Those are
11 fundamental factors if we want to move forward quickly with
12 our legislation, a legislation that was very well accepted by
13 the public.

14 There are a lot of similarities between the
15 attributes required to be a good National Security Chief and
16 a good portfolio Deputy Minister. Dick will understand,
17 because those Deputy Ministers, if you're at Transport
18 Canada, Innovation Canada, Heritage, there is a plethora of
19 independent actors. They don't report to you but you have to
20 give independent advice to the Minister on how we can do
21 better, and also consistency and coordination amongst them.

22 A big revelation -- it won't be a revelation
23 for Dick -- some of our best Deputy Ministers are extremely
24 uncomfortable in this position of portfolio Deputy Minister,
25 just like when you're National Security Chief, it's not for
26 every Deputy Minister, even if they're extremely competent.

27 The attributes of a National Security Chief
28 must be -- the person must be experimented and respected by

1 his peers to bring consistency and coordination, and to
2 challenge assumptions like the PCO role.

3 The second role, the capacity to offer what
4 we call fearless advice. Fearless advice, like in the
5 Westminster model to key audiences, the Prime Minister and
6 his Cabinet. It's not by chance that a lot of advisors did
7 this just before their retirement because there's a certain
8 freedom to provide fearless advice.

9 And my third point, which might demonstrate
10 its added value to the community and other audiences like the
11 Prime Minister and his Cabinet, we always explain to Deputy
12 Ministers that being a Deputy Minister is being a sandwich
13 between an institution and a Minister, because the
14 institution always think that you don't do enough to make the
15 Minister understand that they know what to do, and the
16 Minister is always saying that you do not push enough on the
17 institution for what they want to do. A good National
18 Security Advisor or intelligence advisor is somebody who will
19 be a good link between the two, and not the amplification of
20 one or the other.

21 I'm going to stop there. Thank you very
22 much.

23 **COMMISSAIRE HOGUE:** Thank you very much.

24 **DR. LEAH WEST:** Mrs. Gill?

25 **--- PRESENTATION BY MS. LEX GILL:**

26 **MS. LEX GILL:** [No interpretation]. Good
27 morning, Commissioner, colleagues. Thank you for having me.
28 While the views that I'm sharing this morning are my own,

1 they're informed primarily by the longstanding work of the
2 Citizen Lab, which is an interdisciplinary organization that
3 conducts both technical and investigative research regarding
4 digital threats to civil society, as well as legal and policy
5 analysis at both the domestic and international level
6 regarding issues at the intersection of information and
7 communications technologies, human rights and global
8 security.

9 I'm also a litigator with a practice broadly
10 focused on constitutional law, human rights and state
11 liability, and a background representing civil liberties
12 groups, and so I'm bringing all of those perspectives to my
13 comments today, which means that, at this table, I'm a little
14 bit of an outsider, and I want to use that perspective to
15 perhaps offer a bit of friction or critical insight for my
16 comments today.

17 And in that spirit, there are essentially
18 three issues I'd like to raise this morning. First, I want
19 to talk about the role of the *Charter* and how we think about
20 new national security powers. Then I want to talk about how
21 -- or I want to talk about some of the constitutional issues
22 that come up when we talk about foreign contact. And
23 finally, I want to share some thoughts on the particular
24 issue of digital transnational repression all through the
25 lens of Citizen Lab's work.

26 So some of the discussion questions for the
27 Commission go to the adequacy of the existing powers and
28 capabilities of Canada's intelligence agencies, and I want to

1 speak to those questions.

2 In response to complex problems like foreign
3 interference, the reflex is often to demand more, more power,
4 more funding, more resources, more information sharing. Our
5 Constitution nonetheless imposes very strict limits on both
6 legislation and government action for good reason including
7 the sphere of national security and intelligence. And in
8 that sphere, we need to exercise particular care and
9 attention with regard to the impacts of these potential new
10 powers on freedom of expression, on privacy, on the rights to
11 liberty and security of the person, on equality rights, the
12 right to non-discrimination. There is simply nowhere else in
13 Canadian law where the state is entitled to act with so much
14 latitude, exercise so much power, access so much information
15 and impact the lives of so many people.

16 And we know that errors and abuses can have
17 very grave consequences on individuals, on their futures, on
18 their families, on their status in Canada, and this is all
19 the more true because in the national security context, the
20 powers engaged are particularly difficult, in some cases
21 almost impossible to meaningfully review. And the ability to
22 engage in a full adversarial process is often necessarily
23 limited by the evidentiary and intelligence constraints at
24 play. And we have to admit too that Canadian intelligence
25 bodies have a less than perfect record before our courts and
26 before the Federal Court, in particular, on these issues.

27 This is not meant to suggest that there are
28 no protections or safeguards in place, and I would say that

1 over the last 10 years there have been significant gains in
2 this regard, especially through the wide reforms adopted in
3 C-59. But the fact remains that this is an area where the
4 stakes are very high, the powers are extensive, review is
5 mitigated at best, and the cost of getting it wrong can be
6 incredibly serious, both for individuals who are affected and
7 for the integrity and legitimacy of our public institutions.

8 You know, over the summer we saw a rush to
9 pass a series of complex legislative reforms under the banner
10 of C-70, despite real and legitimate, I think, concerns from
11 a broad spectrum of civil society groups that there was not
12 adequate consultation or review regarding those powers, and
13 concern that those new rules were complex, that they would
14 have significant implications for human rights and *Charter*
15 rights in Canada.

16 And I would just say that, as a result, no
17 matter how serious the threat, you know, and this is not to
18 call into question the seriousness of the threat or how
19 pressing the government's objective is, I do want to ask the
20 Commission to keep the *Charter* as well as fundamental
21 democratic principles like openness and transparency and the
22 rule of law at the very heart, at the forefront of its
23 analysis. We have to start from that place.

24 And in that spirit, it's obvious, but we have
25 to remember that the Constitution binds the entirety of the
26 state in Canada including Canada's national security bodies.
27 You know, while the Supreme Court's approach to the
28 extraterritorial application of the *Charter* leaves something

1 to be desired still, I think Dr. West, I agree with her work
2 that -- to the extent that there should be a sort of *Charter*
3 unless approach. It's the only coherent way forward, but,
4 you know, apart from that issue, there's really no doubt that
5 the *Charter* does apply to everything, everything Canada's
6 intelligence agencies do in Canada in relation to people in
7 Canada, and in relation to infrastructure in Canada.

8 And so that means that not only do any new
9 powers need to be restrained by our Constitution and the
10 jurisprudence that interprets the scope of *Charter* rights,
11 but also that those powers need to be meaningfully subject to
12 real *Charter* review by the courts, through real adversarial
13 processes, with real remedies available when the state gets
14 it wrong. And there's surely work to do in that regard.

15 So in a similar vein, I want to make things a
16 little bit complicated, I want to make a few comments about
17 the attempt to regulate and control specifically foreign
18 interference and influence from a *Charter* perspective. And
19 this is because in this -- in these conversations, the scope
20 of *Charter* applicability can sort of sit uncomfortably
21 alongside some of the ways that we talk about foreign
22 interference and the role of Canada's intelligence agencies.
23 Of course, we don't think of foreign states as having
24 constitutional rights in Canada. They certainly don't. But
25 when we're talking about foreign interference, we know that
26 states ultimately operate through people, and it is so -- so
27 it's through people in Canada, you know, it's those people in
28 Canada who are subject to suspicion, to surveillance, to

1 intelligence gathering, to investigation, to threat
2 disruption activities, immigration consequences and criminal
3 investigation and sanction. And those people have
4 constitutional rights.

5 So when we talk about the influence -- when
6 we only talk about the influence of foreign states, we sort
7 of abstract away that reality. We tend to talk about the
8 rights engaged by these issues through the lens of
9 citizenship, or through the lens of the interests of
10 Canadians. But for almost all constitutionally protected
11 rights, with only a few exceptions, the *Charter* doesn't apply
12 to Canadians. It applies to everyone, to everyone. So
13 there's no second-class rights framework for non-citizens as
14 far as the *Charter's* protections, for freedom of expression,
15 for privacy, for security of the person, for equality are
16 concerned.

17 And obviously, no one here is arguing that
18 foreign interference is not a serious threat, but that fear
19 can't legitimize a political or legal narrative that would
20 rationalize a discount on the *Charter* protections available
21 to non-citizens in Canada. That's not just a question of
22 principle, it's also because the stakes can be high and
23 because that issue goes really to the legitimacy of our
24 intelligence agencies, the legitimacy required to be able to
25 do effective intelligence work.

26 So finally, I want to summarize some of
27 Citizen Lab's recent research on digital transnational
28 repression in Canada, particularly as detailed in a 2022

1 report that I'll include in my written comments from my
2 colleagues Noura Al-Jizawi, Siena Anstis and others, and I
3 want to invite the Commission to really look seriously at
4 this question in its final report. We all know that
5 authoritarian states don't stop at their borders when
6 attempting to suppress dissent and criticism. We know this
7 from publicly reported cases, as my colleagues mentioned, of
8 foreign states working to silence or coerce nationals working
9 on human rights issues in particular outside of their
10 territorial reach, including Saudi Arabia, Rwanda, China,
11 others. In this way, the Lab's research really builds on
12 that body of work related to transnational repression and
13 explores the ways in which it evolves through digital
14 technologies, and we think this is really, really critical to
15 understanding the next few years.

16 And the team's research demonstrates that
17 digital transnational repression is rapidly becoming the
18 cornerstone of everyday transnational repression, and it's a
19 particular threat to the rights and freedoms of dissidents
20 and activists living in exile. We're really talking here
21 about a constellation of activities, online harassment,
22 intimidation, threats, doxing, surveillance, use of spyware
23 and malware, targeted leaks and hacks, coercion by proxy,
24 including through intimidation of allies, friends, and family
25 back home. And I guess noting importantly that digital
26 technology gives authoritarian states just huge new
27 visibility into those relationships and into the most
28 intimate spheres of people's lives.

1 This kind of activity is both enormously
2 common and it's particularly challenging, because unlike
3 direct human interactions, the digital context is seen as
4 lower cost, as scalable, as harder to detect, and accompanied
5 by lower risks of sanction or accountability for state actors
6 that engage in it, both because attribution is difficult and
7 because these behaviours may be more -- less likely to be
8 seen as an attack on sovereignty.

9 I would add that women in particular face
10 qualitatively and quantitatively different kinds of risks in
11 terms of digital transnational repression, and this is an
12 area of the Lab's future research that I think is
13 tremendously important.

14 In Canada, the research demonstrates this
15 kind of foreign interference has very serious impacts on
16 activists and dissidents in diaspora communities, including
17 on their ability to undertake transnational advocacy work
18 related to human rights, which, of course, goes to Canada's
19 interest abroad as well.

20 In addition to direct threats to safety and
21 security, the result of these activities is a global chilling
22 of political and social speech that disproportionately
23 impacts the freedom of certain groups in Canada, so not just
24 what you're going to say at a local meeting, but also what
25 you're going to say and do online, through communications
26 platforms, and the extent to which you can meaningfully
27 connect with collaborators and loved ones in your home
28 country and that disproportionate impact is serious.

1 The Lab's research concludes that support for
2 victims and the Canadian government's response in this area
3 has been seriously inadequate. It's partly because in Canada
4 the focus on foreign digital threats has overwhelmingly been
5 in relation to formal democratic institutions and economic
6 interest and critical infrastructure, but it's also because
7 these individuals and groups are already vulnerable and
8 marginalized in our society. They're already criminalized.
9 They're already underserved by our legal and political
10 institutions.

11 And so in addition to that marginalization,
12 these are now people who are still subject to the
13 consequences of authoritarianism, even after leaving their
14 country of origin, and are nonetheless taking often very
15 major personal risks to defend human rights and democratic
16 values at a personal cost, and we have to do more for these
17 people.

18 **MS. LEILA GHAAHARY:** Excuse me, Ms. Gil,
19 could you ---

20 **MS. LEX GILL:** Yeah.

21 **MS. LEILA GHAAHARY:** --- please slow down for
22 the interpreter?

23 **MS. LEX GILL:** No problem.

24 **MS. LEILA GHAAHARY:** Thank you.

25 **MS. LEX GILL:** Yeah, thank you. So the Lab's
26 report does detail a series of recommendations. Some of
27 those Canada has made some headway to adopt since the report
28 was published in 2022, including better coordination across

1 government bodies, and greater public communication, and more
2 support for victims. So too though on that list was the need
3 to ensure that the Canadian government's own use of digital
4 surveillance technology was transparent, is transparent,
5 lawful and rights respecting, as well as the need for greater
6 transparency from technology companies regarding how they
7 respond to government requests to remove content or access
8 user information as part of efforts to respond to digital
9 transnational repression.

10 Similarly, the Lab has said Canada needs to
11 do more to sanction companies and needs to refuse to do
12 business with companies involved in developing and selling
13 the technology that facilitates these abuses by authoritarian
14 regimes like spyware manufacturers.

15 And so in this sense, these recommendations
16 bring us back to my first point and perhaps the thing that
17 unites all of my comments this morning, which is really just
18 an observation about trust, legitimacy, respect for the
19 Constitution and the rule of law at home. Our research shows
20 that even, you know, for example, when somebody did choose to
21 reach out to CSIS or law enforcement in a case of digital
22 transnational repression, the result is that they felt it was
23 useless or even harmful, if they got a response at all.

24 As the Commissioner already knows, legitimate
25 concerns about abuse, overreach, discrimination and
26 criminalization all undermine any incentive that someone
27 might otherwise have to collaborate, leaving these
28 communities on their own and leaving us all less safe. And I

1 would just add, in that respect, that while maybe the people
2 at this table or the people in this room can make kind of
3 clear distinctions between different intelligence agencies,
4 or the difference between intelligence and law enforcement,
5 or the difference between intelligence and immigration, that
6 is not the case for ordinary people on the ground. It is the
7 state of Canada and the -- especially now that we're in an
8 environment where there is so much more information sharing,
9 I have to say that that distinction is less and less real
10 even within government. And so I think that we have to be
11 sensitive to the reality that that is the perception from
12 individual people who are affected by these kinds of abuses.

13 So, ultimately, I'm hopeful that the
14 Commission is going to conclude that the legal constraints
15 and democratic values that I'm talking about are worthy for
16 their own sake, and that they need to be a starting point for
17 any analysis, but it's also clear that without them Canada's
18 intelligence agencies and law enforcement authorities and
19 legal institutions are just going to lack the basic
20 legitimacy they need to act effectively.

21 So I think I'll stop there. It's really only
22 through a legal and political culture that's irreproachable
23 in terms of its respect for its constitutional obligations
24 and human rights and civil liberties that Canada's
25 intelligence agencies will be able to make meaningful inroads
26 in addressing these threats. Thanks.

27 **DR. LEAH WEST:** Thank you very much. I'll
28 turn to Mr. Jones.

---PRESENTATION BY MR. ALAN JONES:

MR. ALAN JONES: Thank you. Good morning, Commissioner. Thank you for the opportunity to speak. My panel of colleagues have covered a lot of ground, some of which I was going to cover, so I've removed some of that, so if I -- it appears a bit choppy, it's because I do not want to do -- repeat some of the things that I agree with from my colleagues.

The vast majority of foreign interference campaigns in Canada are not the most egregious criminal acts of some of which we've talked about in this past year with regarding Government of India and the murder of Mr. Nijjar. The majority of foreign interference campaigns are going to be conducted at a more subtle level, some involving intimidation broader, but not hitting that high bar that we have seen and have talked about this year. But there is a trend for adversary states to become increasingly aggressive and use tactics to cross red lines. Murdering people and violating sovereignty is not typical of what foreign interference campaigns have been traditionally, but they seem to be becoming more popular and there seems to be almost with a perceived impunity to be able to do this.

This disturbing trend was directly addressed recently by Ken McCallum, who's the Director-General of MI-5, the British security service, in a public statement the last couple of weeks, where he was referring primarily to the actions of the Russian government, including the murder of dissidents in the United Kingdom, also states such as Iran.

1 Mr. McCallum went so far as to say that
2 Moscow was seeking to cause mayhem on the streets of Europe.
3 It is a continent at war, and that war is touching Canada.
4 Canada is not immune to these types of threats.

5 There's been similar statements made by Mike
6 Burgess, who's the Director-General of the Australian
7 security intelligence organization. Australia created a
8 foreign interference threat assessment centre about three
9 years ago intentionally focused on the issue of foreign
10 interference, somewhat like a terrorism threat assessment
11 centre, but focused on foreign interference. And Mr.
12 Burgess's comment was that the average Australian would be
13 surprised at the depth and the breadth of foreign
14 interference that is occurring in Australia.

15 In the Canadian context -- that may be a
16 reference point to us, but in the Canadian context, I
17 completely agree with previous comments that this needs to be
18 addressed by not just government, but by civil society and by
19 academia. And I can give you an example of that,
20 Commissioner.

21 So when I retired from CSIS, I began working
22 with the University of Ottawa on a national security program
23 because I was of the view that there is a level of illiteracy
24 about the national security issue in Canada, writ large, at
25 every level, including at senior levels of government. I
26 blame no one for this. This is just part of our culture and
27 it's just part of the reality, but also in public as well.

28 There was a lot that we could talk about in

1 public that has not been discussed previously that we need to
2 talk about publicly. It's important to our democracy.

3 So we created a national security program at
4 the University of Ottawa Professional Development Institute.

5 One of -- or a couple of the areas that we
6 have been looking at is gender disinformation focused on
7 women and young girls as well as foreign repressive
8 governments targeting women journalists in the West. Freedom
9 of the press is integral to our democratic process.
10 Protection of women from gender disinformation is integral to
11 our democratic values.

12 Yesterday, the U.S. Department of Justice
13 laid charges against a senior General in the Iranian
14 Revolutionary Guard Corps, along with eight others, for an
15 assassination plot against an Iranian U.S. journalist named
16 Masih Alinejad.

17 Today, as we speak here or talking here, Ms.
18 Alinejad is speaking at the University of Ottawa. We brought
19 her up from the United States, police protection, and she is
20 holding an event where she is explaining personally what her
21 experiences are and what she has received in the form of
22 disinformation and threats from a foreign government in the
23 United States, and the same thing is happening here in
24 Canada.

25 That is the type of thing where you can have
26 government, civil society and academia collectively working
27 to shed light on issues such as this as foreign interference.

28 I'll also add that foreign interference in

1 the federal electoral process and democratic institutions is
2 only a part of foreign states' foreign interference
3 strategies. No state really has a strategy solely to
4 interfere in the election process in Canada. It's part of a
5 much larger process of their foreign policy of projecting
6 power and dealing with dissidents and changing the
7 environment to their advantage.

8 So we're entering a stark era where
9 traditional foreign interference has tended to be meddling
10 and with intimidation, is now including extreme acts of
11 violence and threats of violence. And as with most national
12 security threats, as Dick mentioned, these threats don't
13 replace traditional threats. They simply become yet another
14 layer on top of all the other threats that you have to deal
15 with.

16 Government of Canada's responses will need to
17 be as layered and as nuanced as the threat itself, from
18 subtle to sometimes blunt, i.e. arrests and law enforcement.
19 The law enforcement is going to be, I think, an exceedingly
20 rare occurrence in this space.

21 CSIS, the RCMP, CSE, in my opinion, have lots
22 of investigative powers. They have plenty of powers. But as
23 Dick said, they need to be -- they need to be maximized in
24 how they're used within constitutional law, within
25 constraints, within review.

26 Investigative powers is -- you know, is a
27 direct and somewhat easy way to deal with these issues. It's
28 far more complicated to build the expertise and develop

1 coherent frameworks around the investigation of threats from
2 foreign interference.

3 Coherent strategies require building and
4 maintaining expertise on complex issues such as ethnic,
5 political, irridentist trends amongst diaspora requires
6 specific focus on these issues. The knowledge to understand
7 what foreign interference is in its many forms and looks like
8 comes with experience. It's not formulaic, it's not binary.
9 It is not just one thing. It is not something that you can
10 easily identify.

11 This also means, in the national security
12 community, hiring people who are actually interested in these
13 types of issues and are not just generalists who are assigned
14 a file as they transit a particular operational area. Today
15 you're working in foreign interference, tomorrow you're
16 working on terrorism, tomorrow you're working on something
17 else.

18 It also means, for example, that CSIS
19 intelligence officers who traditionally spent time in
20 communities talking to representatives of diaspora, talking
21 to community leaders, talking to people who understood and
22 represented certain perspectives, this was done in the past.
23 The Service has gotten away from doing that. There is less
24 and less contact with representatives in diaspora
25 communities. I think we need to get back to that model.

26 There's a -- there's reasons for this. We're
27 all aware that after 9/11 and the emergency measures that
28 arose and excesses that are well documented sent a chill

1 through the community. This coincided with an erosion of
2 public trust in government institutions in general as a
3 result of divisive and partisan politics fueled by conspiracy
4 theories and enabled by the media and the internet. And this
5 severe chilling of CSIS officers spending time in communities
6 has had an effect on understanding what is actually
7 happening.

8 The purpose of intelligence service is to
9 give some forewarning and to understand the threat
10 environment. If you're not engaged with that threat
11 environment, you're not going to understand it. And you're
12 not going to understand it by Googling these issues. This is
13 a person-to-person type of phenomena, and those personal
14 relationships are vitally important.

15 I think we can -- notwithstanding the
16 excesses, the issues of the past, we can get back to that
17 model again and have more engagement with communities, if
18 it's done respectfully, if it is done mindfully to
19 constitutional freedom of speech and all those issues, but
20 somehow -- and it is being done with a more diverse
21 population of intelligence officers than in the past.

22 But if you do not have that level of
23 engagement with communities, you're not going to understand
24 what is happening and there will not be a level of trust for
25 members of ethnic communities and diasporas and others to
26 come forward and say that they have been subject to foreign
27 interference and when they call, someone has to answer the
28 phone. Someone's got to talk to them. Someone has to be

1 able to understand what they're saying and why, and how to
2 respond.

3 Short version is that foreign interference at
4 its core is a person-to-person problem. Yes, it's enabled
5 through technology and there are technological approaches to
6 social media and anti-harms legislation and others, but CSIS
7 officers need to get back in the street and do what an
8 intelligence service should do, which is to understand the
9 threat environment at an expert and personal level.

10 I have a deeper example of this, but I'll
11 keep that aside for questions later just in the interests of
12 time.

13 Greater engagement by government and agencies
14 is not without potential controversy. I think we all
15 recognize that. But acts of violence can't be the only
16 starting point for engagement. We can't wait until things to
17 get to a crisis level before there is a government response
18 and response by agencies essentially just acting as
19 spectators rather than trying to predict and counter.

20 Countering divisive messages require active
21 messaging campaigns, and I -- when I'm looking at the foreign
22 interference, I'm reminded very much of the terrorism threat
23 in the early 2000s in dealing with radicalization and how the
24 government was trying to develop effective approaches to deal
25 with radicalization messages on the internet and in another
26 forum and the extreme hesitancy and aversion to dealing with
27 civil society, dealing with ethnic communities, on how you
28 have that conversation about where legitimate freedom of

1 speech, freedom of religion ends, and radicalization begins.

2 I don't think we've sorted that out entirely
3 yet. I think there's still a lot of work to do in that area.
4 There's a very similar issue within the foreign interference
5 domain.

6 Disclosure is a very complex, you know,
7 issue. And when we talk about intelligence to evidence and
8 others, but public disclosure of more information in
9 illuminating these threats is extremely useful.

10 The U.S. has pioneered, somewhat, laying
11 charges against foreign actors, even though they know the
12 likelihood of arrest is almost zero. But the process of
13 laying the charge, the information that comes out in court,
14 the description of why the charges are being laid has been a
15 very, very useful mechanism to expose foreign interference.
16 As I said, the charges laid against this Iranian general,
17 against the threat against Ms. Alinejad, the likelihood of
18 him being arrested is extremely low, but the fact that the
19 charges can be laid, and the affidavit, and the court
20 documents explain exactly what their methodology is, what
21 their objectives were, what they've done, and who the victims
22 were. That is a tool that I think is useful -- can be useful
23 in Canada as well, the laying of charges.

24 And I know that there's a -- in a prosecution
25 service, there has to be a likelihood of success in a
26 prosecution, and if you're -- you know, you're -- the person
27 you're laying charges against is on the other side of the
28 world, and probably you're never going to reach them, the

1 likelihood of success is low, but there is a value in that
2 process of revealing that information.

3 There's also concept of strategic disclosure,
4 where a decision is made to reveal sensitive information
5 about a threat where a balance is struck between the loss of
6 secrecy versus the benefit of disclosure.

7 Very rare in Canada do we use this approach,
8 perhaps in part because we are so reliant on strategic
9 intelligence coming from allies who own the rights to it in
10 the first place, but the -- those types of decisions are not
11 going to be made at the agency level. They're going to be
12 made at very senior levels, as to taking in the full opinions
13 of everyone involved, yes, if this intelligence is revealed
14 publicly, there will be perhaps damage or some erosion to the
15 platforms or the ability to gather it in the first place, but
16 the consequence and the benefit of making that level of
17 disclosure may outweigh it for the general -- for the greater
18 good.

19 It's also important to bear in mind that our
20 foreign interference challenges are shared by our closest
21 allies, and therefore we have an opportunity to pursue a
22 common strategy with allies in countering foreign
23 interference.

24 As I said, the U.K., Australia, E.U., U.S.,
25 have all named foreign interference as a growing threat to
26 their democracies. We've all identified the same --
27 primarily the same adversaries and the same methodologies as
28 the source of threat, and so the value of a common cause I

1 think deserves more attention. There is probably more than
2 we can do. As everyone rallied in the post-9/11 to deal with
3 terrorism, there may be considerable advantage in an
4 international forum in dealing with this threat, at least
5 amongst liberal democracies.

6 I'm fond of disclosure, in along the lines
7 that the devil is often in the details. C-70 has got a lot
8 of amendments in it. It's a complex document and I do not
9 even remotely claim to understand all of it or the effects of
10 it. And I don't think even the agencies affected by it
11 entirely understand what it means yet. As with all new laws,
12 when they're rolled out, it takes years of implementation,
13 and court challenges, interpretations, amendments before it's
14 actually fine-tuned.

15 But there's one that stood out to me in the
16 legislation on the registry, Foreign Influence Transparency
17 Registry. In section 15, seems to be a gap, at least to me
18 there's a gap, is that there's a requirement for those who
19 meet the requirements of the legislation to register, and
20 then there will be data holdings and all this. In section 15
21 of that Act, it talks about the disclosure of that
22 information, and it can only be disclosed in the context of
23 investigation of a violation of the Act.

24 There is nothing in it that allows that
25 information, that data, to be accessed by CSIS or the RCMP in
26 the context of a broader foreign interference investigation.
27 It seems counter-intuitive to me to have what is described as
28 a tool in dealing with foreign interference, where the data

1 holdings in it do not appear to be available to the
2 intelligence service, which has written in its mandate to be
3 -- which is to investigate foreign interference, or to the
4 RCMP, which has national security investigations and requires
5 intelligence.

6 There is, in section 17, where it says that
7 the evidence used in a prosecution under that Act can't be
8 used as evidence in another prosecution, this makes sense in
9 a legal sense. I understand that. But the disclosure of
10 that information as intelligence is not going to be used as
11 evidence. It's not going to end up in court.

12 I could get into if, you know, as we go into
13 this, examples of what I mean by that, but my experience is,
14 if a piece of legislation does not explicitly say that that
15 information can be accessed by CSIS or the RCMP for its
16 investigations, or does not explicitly have a mechanism which
17 would clearly allow CSIS or the RCMP to fall under that
18 mechanism, then the policy interpretation is going to be if
19 Parliament intended for CSIS to have access to this, it would
20 have said so, but it didn't, so you can't have it. There are
21 any number of pieces of legislation that seem to fall -- that
22 I've seen that develop over the years.

23 So I'll leave it out there. Legal scholars
24 much smarter than me may understand this better and have a
25 solution to this, but I just wanted to put that down as
26 something that perhaps you could deal with earlier.

27 Another issue which has been alluded to a bit
28 is what I call the compression of the intelligence collection

1 timeline, which has happened over years as the threshold for
2 intelligence investigations and investigative powers to be
3 used increasingly nears criminal evidence levels, that
4 there's been -- and I've watched this happen over literally
5 30 years, of where an intelligence investigation is supposed
6 to start early and be contained under constitutional
7 restrictions within law as to what the results of what that
8 intelligence investigation is used for, is the threshold to
9 authorize those investigations to use the power has slowly
10 crept up towards what the police would have to meet under a
11 criminal investigation so that the product that is being
12 collected is creeping towards being viewed as criminal
13 evidence.

14 What that has been doing is moving the
15 timeline what I would call to the right, and that time for
16 forewarning is getting shorter and shorter as you continually
17 aren't able to start the intelligence collection earlier.

18 I'm not sure if this is intentional. It
19 might be. It may be the result of 30 years of jurisprudence,
20 and laws, and changes in policy interpretations, but you
21 could certainly feel it in investigations where you just
22 don't have on ramps, what I would call on ramps to
23 investigation, which years before you write it, the on ramps
24 don't exist. You're expected to somehow start well down a
25 line to almost an evidentiary level before you can get the
26 authorities you need to gather intelligence to get
27 forewarning.

28 The, you know, issue of intelligence to

1 evidence is relevant to the foreign interference
2 investigation. I'm not going to go through that. I think
3 we've talked about that quite a bit.

4 But I will talk about disclosure, and
5 something that as I was preparing to speak to you today that
6 I just happened to come across, which is on the MI5, the
7 British Security Service's website. And it says -- and I'll
8 -- some of it will be quote, some of it is just to set it up,
9 is that an incoming Prime Minister will be told about any
10 information it may have about a potential Cabinet Minister
11 that raises a serious national security concern and only if
12 it appears likely that the individual concerned will need
13 access to sensitive information. The site goes on to say:

14 "A similar arrangement has been in
15 operation for the Official Opposition
16 since 1992. The Leader of the
17 Opposition is briefed on any serious
18 security issue concerning a possible
19 member of the Shadow Cabinet. This
20 is necessary because members of the
21 Shadow Cabinet are often briefed on
22 security issues."

23 I found that to be an interesting piece in
24 the context of some of the discussions -- a lot of the core
25 discussions around the Commission, is that clearly others
26 were thinking about these issues and have ways of approaching
27 it. I don't -- I can't tell you what exactly happened in
28 1992 that is referenced on there. I know that around 1992

1 the UK authorities passed significant legislation around
2 terrorist threats, which were building in the UK, so it may
3 have flowed somehow out of that. But I think it may be
4 something worth looking at to see what is behind that
5 approach and why do they -- and it sits right on their
6 website, in a public website to address.

7 On the broader issue of the effectiveness
8 that Canadian national security apparatus -- Mr. Jean
9 discussed this in detail. I don't want to repeat it, but I
10 just think from a practitioner's perspective at times, there
11 was a sense that the approach to national security was very
12 uneven in Canada, even what national security is, it's kind
13 of an amorphous definition at times, but the approach seemed
14 to be uneven, particularly as you went from government to
15 government. That's the right. But that continuity and the
16 ability to follow an issue over a period of years where these
17 issues are often perennial, in 1997 -- 1987, I worked on the
18 investigation of foreign interference in Canada by the
19 Government of India. Thirty-seven (37) years later, we're
20 still talking about it. So the ability to track these issues
21 over time and deal with them may have in part a structural or
22 a systemic problem in Canada if we do not have -- and I don't
23 want to say that we should do what the Americans do, have a
24 National Security Council, but a National Security Council is
25 somewhat different than the functions of the -- for example,
26 the Privy Council Security Intelligence Secretariate, which
27 is the Secretariate the Cabinet functions. They have
28 different objectives, they have different staffing levels,

1 and they have different continuity. And many times over the
2 years I would deal with representatives from the United
3 States, from the United Kingdom and often Australia at senior
4 Public Service levels, who had been working these files for
5 years, and the Canadian representatives had been kind of
6 moved in quickly to deal the file as just one of the many
7 issues that they had to deal with on their plate. And there
8 seemed to be a lack of a structural approach to this, which I
9 think may have some knock-on effects to some of these broader
10 issues.

11 With that I'll end my comments and happy to
12 take questions. Thank you.

13 **COMMISSIONER HOGUE:** Thank you.

14 **DR. LEAH WEST:** Thank you very much.

15 Professor Carvin?

16 **--- PRESENTATION BY DR. STEPHANIE CARVIN:**

17 **DR. STEPHANIE CARVIN:** Thank you. So I kind
18 of went question by question process. So does Canada -- do
19 Canadian intelligence agencies have the legal authorities,
20 technical capabilities and resources necessary. I think
21 there's broad consensus on this panel that most of the legal
22 authorities are there. This is not a problem of law. This
23 is now a problem of enforcement, making policies, review
24 practices, all of this kind of thing. I will make two
25 possible observations, perhaps in direct opposition to the
26 very passionate discussion by Lex, which I very much agree
27 with, but one of the things I noticed about our foreign
28 interference transparency registry is that it looks at

1 sectors that lobby the government, right, the political
2 level. It does not look at other institutions like the
3 media, and that is such a third rail to touch. But I would
4 note that, you know, the recent reporting out of the United
5 States, which, allegedly -- I emphasize allegedly -- may
6 reflect Tenet Media, there's foreign interference -- you
7 know, there's clearly foreign states that want to impact
8 media, the way it's perceived and things like this. Do we
9 need to think about that in terms of our legislation, or are
10 there other mechanisms we can do?

11 The other issue I wanted to just touch on
12 briefly because I do think it's a whole can of worms that is
13 outside the scope of this particular conversation, but the
14 intelligence-to-evidence issue was not addressed in Bill C-
15 70, and I do believe it continues to be a missing piece of
16 the legislative puzzle and should be addressed in the future.

17 On the issue of recruitment, retention and
18 training, I do have concerns about the capacities and
19 resources. I don't think I need to go over the multiple
20 reports. I believe there's now been 10 on RCMP policing, and
21 the fact that they are simply unable -- and Mr. Jean said
22 that fairly importantly, I think, but the fact is that the
23 contract policing is really inhibiting national security
24 investigations. So, you know, I don't want to get into this
25 issue further, but just to note that I think it's one of the
26 largest structural issues that we actually have.

27 The point that I think Lex made about, you
28 know, diaspora groups contacting the police about their

1 concerns, and then nothing happening, or them not being aware
2 of the situation, or questions of jurisdiction I think
3 somewhat tie into this.

4 But I also have similar HR issues about the
5 intelligence community at present. As far back as 2018 as
6 part of a research project, I interviewed someone who worked
7 in the community who said their organization identified
8 recruitment as one of their top challenges, and this has only
9 gotten worse in the years since. There's budget cuts, a
10 paralyzed -- the security clearance process to me in the last
11 year has been described to me as completely paralyzed; right?
12 This is huge. It can take up to two years. There's
13 retention issues that's seriously hampering the ability for
14 the community to do its job.

15 And I don't know to the extent that, like,
16 very specific HR practices are going to be a part of your
17 final recommendation, but I do note that if you do not have -
18 - or if you have a burned-out community because you can't
19 replace people, there's insufficient staffing, if people are
20 acting in more than one position for periods of time, this is
21 ultimately going to impact our ability to do the job.

22 And then both the RCMP and CSIS, to a certain
23 extent, have a generalist model, right, in terms of their
24 recruitment. You know, if you're in the RCMP, you show up at
25 Depot, you do your training there, and then you go off and
26 work in, I don't know, murder investigations in Newfoundland
27 for a long period of time, and then you may be brought onto a
28 national security investigation, and then you probably work

1 there for a couple years, and then you're back to the
2 province. I do worry that -- you know, we've all talked
3 about the fact and, you know, Mr. Jones just said I think
4 really well that there's this issue of focus, and he referred
5 to a National Security Council. But I also think, like,
6 allowing individuals to develop specializations like they do
7 in other Five Eyes countries would be a good idea. We need
8 less of a generalist model. And the ability for people to
9 develop that expertise over a period of time.

10 The second question is what measures can be
11 taken to make the relationship between Canada's intelligence
12 agencies and government policy makers effective and more
13 efficient. So I wrote a book on this, so I can't submit the
14 book, I don't think. It wouldn't really be fair ---

15 **COMMISSIONER HOGUE:** I've read it.

16 **DR. STEPHANIE CARVIN:** Oh, wow, there you go.
17 Okay. So impressed. Awesome. That's going in the promotion
18 file.

19 And I wrote it with my friend Thomas Juneau.
20 Basically, to summarize, we conclude that intelligence
21 literacy in the policy community remains low. You know, the
22 courses that are being developed at PDI, University of
23 Ottawa, are trying to solve this challenge, and Mr. Jean as
24 well, working on that. But a lot of times individuals would
25 talk to us about the intelligence being in a black box, not
26 knowing how it was made or where it was coming from. And
27 there's also a sense that the policy community needs to
28 improve -- sorry, the policy community needs to improve its

1 strategic understanding to understand what the roles of the
2 different departments' agencies are in our national security
3 process.

4 Like it or not, and there's a lot of reason
5 not to like it, but, you know, I tell my students now, I'm,
6 like, if you want to fight espionage and foreign
7 interference, go work at ISED, go work at Innovation, Science
8 and Economic Development Canada, right, because they have the
9 *Investment Canada Act*. This is one of the most powerful
10 pieces of legislation we actually have. So we need to make
11 sure that all these departments and agencies know their
12 roles, responsibilities and limits.

13 But also, policy literacy is lacking in the
14 intelligence community, and I think to a certain extent it's
15 true that intelligence agencies, managers, analysts do not
16 understand their clients and do not understand their
17 priorities as well as they should, and this means products
18 are crafted in ways that don't speak to them, or are too
19 long, or are not timely. And it is a good thing that there
20 is tension in the relationship. There should be -- someone --
21 -- you'd mentioned challenge function. You know, we want that
22 challenge function to be there, but that's going to -- so I'm
23 not saying there should be, like, perfect harmony between the
24 two communities. I don't want that at all, but I think that
25 two communities that understand each other better are going
26 to have that more dynamic relationship. That challenge
27 function is going to function better and produce better
28 products. And I think that some of the steps that could be

1 taken would be to better train analysts to produce contents
2 that better spoke to their clients. Certainly, our client --
3 I think our Five Eyes partners do a better job with this than
4 we do.

5 And secondly, we need to do a better job of
6 utilizing secondments in our national security agencies and
7 in our policy communities. Right now, I mean, I'm going to
8 be blunt and just say secondments are used to get rid of your
9 worst employees. And it's, like, who can I get rid of for
10 two years? Oh, this person. Great. That's not the way it
11 should be. It should be our best employees that are being
12 put forward to learn about other communities, so that when
13 they come back, the relationship will hopefully be better.

14 And we need to find ways to make it easier
15 for policy analysts and their senior clients to access
16 classified information. You know, we heard -- if I followed
17 the news correctly, there were challenges in getting certain
18 Ministers classified information during the pandemic. But
19 right now, even just accessing a SKIF, like the classified
20 information facilities is hard. You have to leave all of
21 your -- you know, you're a Deputy Minister. You have to
22 leave all your electronic devices behind. You're being
23 pulled away from any other ---

24 **MS. LEILA GHAAHARY:** Ms. Carvin? Excuse me
25 sorry.

26 **DR. STEPHANIE CARVIN:** Am I speaking too
27 fast?

28 **MS. LEILA GHAAHARY:** Yes, please could you

1 slow down?

2 **DR. STEPHANIE CARVIN:** I'm sorry.

3 **MS. LEILA GHAAHARY:** Thank you.

4 **DR. STEPHANIE CARVIN:** Pity my students.

5 Thank you. I am sorry.

6 Anyways, so they have -- once they have this
7 information, you know, they're pulled effectively from their
8 -- all their -- everything that's on fire, and then they're
9 having to read this information, find it on a computer that
10 was probably from 2008 and takes like 10 minutes to start up,
11 and once they have this information, it's difficult for them
12 to share what they know, even if they can act on it.

13 We need better coordinations of our
14 institutions. We need to -- we need to do a better job of
15 feeding intelligence up the chain. That's probably one of
16 the biggest themes coming out of this entire Commission.
17 This was also found in the Johnston report, which found the
18 government is missing effective protocols on information
19 sharing, intelligence gathering, and distribution.

20 I'm pleased to say that I think there have
21 been steps taken to improve this recently. There's more DM
22 and ADM committees, there's now a Cabinet committee, although
23 I agree it's way too early to say if it has or hasn't been
24 effective at this point.

25 Then this brings us to the interesting
26 question, the NSIA, and whether that office should be
27 strengthened.

28 I'm sympathetic to the view that, you know,

1 maybe legislation is not going to be the perfect fix, but I
2 do believe the NSIA needs a better and bigger staff and -- or
3 at least a secretariat, and that there should be at least
4 some kind of entrenching of the functions of the ability to
5 coordinate the intelligence community in Canada.

6 One of the things we found in our book, the
7 one I wrote with Thomas, Thomas Juneau, is that a lot of the
8 community in Canada is personally driven. It's driven by
9 personalities, and when those personalities move, some of
10 those initiatives can be lost. So the more I think we
11 actually entrench some of these ideas, whether through
12 legislation, or far clearer policy directives, or something
13 like that, I think for the better.

14 So I kind of lumped under our section
15 questions three, four, and five, and I'm just going to talk
16 briefly about two things. One is open-source information,
17 and secondly, learning to communicate better with affected
18 communities.

19 On the issue of open-source, I think this is
20 actually one of the best ways that we can actually -- you
21 know, this challenge of information sharing. If we can do a
22 better job of open-source, I think that this would take care
23 of a lot of our problems.

24 You know, like Thomas and I -- I should say,
25 Thomas Juneau and myself have -- we estimate that somewhere
26 between 70 to 80 percent of classified information probably
27 is available in open-source somewhere; right? That's not a
28 perfect measurement, but certainly this information could be

1 used to communicate with those without clearance. There was
2 actually really good steps taken on this during the pandemic;
3 right? Where people couldn't actually access their
4 classified information, so there was kind of a flourishing of
5 open-source products, which was really good.

6 But basically, Canada needs a centralized
7 body with a mandate to collect -- I appreciate that some of
8 my colleagues have challenged the need for new institutions,
9 but hear me out.

10 Canada should have a more, let me say
11 centralized approach, to collect open-source information from
12 across the Canadian intelligence community to maximise the
13 potential of modern OSINT collection, tools, and products.
14 To be effective, the body needs to have the mandate to
15 develop and share OSINT across all levels of governments,
16 become a federal policy leader and centre of excellence for
17 OSINT collection, training, and analysis, and I appreciate
18 there would be significant legalities and legal processes
19 needed around this too, and could work to improve the
20 coordination and breaking down of current OSINT silos. Right
21 now a lot of the agencies out there do do some kind of OSINT,
22 but it would be great if we could kind of unite this
23 together, and it would enhance Canada's OSINT culture and
24 capability.

25 And I should say that Professor West and
26 myself, we have a chapter coming out in -- I'm really just
27 using this platform to promote my work. Sorry. But
28 basically the Integrated Terrorism Assessment Centre might

1 actually be the appropriate body to do this. I think ITAC,
2 it would be -- especially since it was originally created
3 with this mandate of doing more interaction with front-line
4 communities, and that would be impossible -- that would be
5 possible to do under an enhanced NSIA role or office,
6 discussed earlier.

7 And the final thing I'll talk about is
8 learning to communicate with effective communities.

9 You know, we're doing this at a time -- this
10 conversation at a time when I do want to note that hate
11 crimes against Asian Canadians, and I would say Indo
12 Canadians and South Asian Canadians, have surged.
13 Particularly in the wake of COVID-19, and sensitivity to this
14 reality is important and needs to be reflected into
15 operations of those institutions taxed with combatting
16 foreign interference. It needs to be at the heart of our
17 understanding.

18 We can't -- I don't think we should approach
19 foreign interference out of fear. I think we need to do it
20 out of empathy; right? And from the view of the communities
21 that are primarily effective.

22 Unfortunately, the generalist model that I
23 discussed earlier used in the national security communities
24 with the lack of specialists within these organizations may
25 be hampering outreach, although, you know, I take all the
26 points made by Mr. Jones as well.

27 Often, you'll find, you know, the roundtable
28 approach. "Hey, everyone, come together. We're going to

1 talk about foreign interference in communities." That's not
2 going to work if people are terrified to speak out.

3 So, you know, we have to find ways to reach
4 communities in ways that people who do speak up are not doing
5 it in front of everyone else, that you do have these secure
6 ways of managing these issues.

7 And I also take very much Lex's point that
8 the communities themselves don't understand the institutions
9 that are out there. It doesn't help in our very federal
10 system when you have someone reach out for help and, you
11 know, you call CSIS and CSIS says, "Thank you for the
12 information. There's nothing we can do. Contact the RCMP."
13 The RCMP looks at it and then says to contact your local
14 police. And you contact the local police and they're not
15 being briefed on any of this, so they don't understand the
16 global context, right, and just say, "Well, there's nothing
17 really we can do." I can't imagine a more alienating
18 feeling.

19 We need to take care when we're crafting
20 materials to do outreach to these communities. We can't just
21 ChatGPT our documents into Chinese and literally translate
22 them and expect that you're capturing the nuances of all the
23 language. So we need to actually hire people who understand
24 these communities, who speak the language, ensure that we are
25 taking care when we're translating the documents that we're
26 putting out there to reflect the nuances of languages and
27 customs.

28 And then finally I'll just say, to the point

1 of community engagement, that there's been a lot of criticism
2 of the community and the way it engaged with diaspora
3 communities, particularly the Muslim communities in the post-
4 9/11 era, and I don't know if we've done a good job of
5 listening to what those concerns actually were. And for the
6 reasons -- some reasons that Mr. Jones mentioned, but
7 practices like just kind of showing -- door knocking, showing
8 up at places of employment, these were highly criticized
9 practices, and I don't know to the extent -- you know, as
10 we're right now realizing we need to re-engage with these
11 communities, I don't know if we've done it with a view of
12 learning the lessons of the past two decades of
13 counterterrorism. We need to, like, actually reflect on what
14 happened, figure out, you know, are there better ways of
15 engaging with these communities than just kind of showing up
16 and knocking on the door? Sometimes I feel like IOs only
17 kind of have one method of engagement, which is the door
18 knock approach, and I think maybe we could do better.

19 So let's take these concerns, especially
20 those raised by, you know, the Muslim community, the Sikh
21 community in the wake of -- you know, during the passage of
22 C-70, seriously, or else I take the point there's just not
23 going to be sufficient trust to communicate with these
24 communities as we go forward and try to address this problem
25 of foreign interference.

26 Thank you.

27 **COMMISSIONER HOGUE:** Thank you.

28 **DR. LEAH WEST:** Dr. Robson-Morrow?

1 **--- PRESENTATION BY DR. MARIA ROBSON-MORROW:**

2 **DR. MARIA ROBSON-MORROW:** Thank you very
3 much. Thank you, Madam Commissioner. Thank you, fellow
4 panellists. And to the Commission for the invitation.

5 I do need to note right off the bat that the
6 views expressed here are my own and not those of my employer.

7 I also want to do a time check. May I still
8 take approximately 12 minutes or should I try to ---

9 **DR. LEAH WEST:** No, take as long you ---

10 **DR. MARIA ROBSON-MORROW:** --- leverage my ---

11 **DR. LEAH WEST:** --- have prepared for.

12 **DR. MARIA ROBSON-MORROW:** Thank you. So I
13 have two core arguments, underlying principles, for my
14 remarks today that I believe will align with what my
15 colleagues have said.

16 The first one is, as Mr. Jean mentioned, the
17 Crown Jewels are not all in the hands of government. They're
18 certainly not all in the hands of the national security
19 agencies. And Canada's national security apparatus must
20 provide mechanisms for effective trusting two-way engagement
21 with external parties. And critically important, this
22 national security apparatus must treat these parties as
23 potential partners, not just victims. They have pieces of
24 the puzzle as well. We're not just there for one-way
25 directional briefing to them. It has to be an engagement.

26 Second is that we are not the only ones
27 facing these challenges, and as Mr. Jones mentioned, our
28 allies, particularly our intelligence sharing partners within

1 the Five Eyes have a lot of models, they're tackling this as
2 well, that are relevant when applied in a Canadian context.

3 So I will have those two underlying
4 principles or arguments here, and my remarks are structured
5 in three different categories of engagement.

6 The first one is duty to warn or duty to
7 advise. The second one is engagement models with external
8 parties that focus specifically on foreign interference. And
9 the third is engagement models writ large with a security
10 focus, but not necessarily foreign interference, but they
11 have characteristics for successful engagement that are
12 relevant for us for the purposes of the Inquiry and the
13 Commission.

14 And for this one, I'll be drawing on eight
15 years of research and, like Professor Carvin, interviewing
16 practitioners in the community and drawing lessons from their
17 experiences.

18 So the first category of engagement is duty
19 to warn or duty to advise.

20 Most of the Five Eyes countries do not have a
21 formal duty to warn. It rests within law enforcement
22 entities, so the RCMP has its obligation here.

23 We see this across the Five Eyes. The
24 country that does have a formal duty to warn for the entire
25 intelligence community is the United States, with
26 Intelligence Community Directive 191, and it's a relevant
27 model for us to look at.

28 It focuses on threats to life. However,

1 there are aspects of the directive that I'll posit today are
2 relevant for us when thinking about potential duty to warn in
3 a foreign interference context.

4 The directive is very specific, and it's
5 available to the public. It's online. It's slightly
6 redacted, but most of the content is available. And it
7 stipulates that any intelligence agency in the United States
8 that collects or acquires credible and specific information
9 indicating an impending threat and, in this case, it's to --
10 it's for intentional killing, bodily injury or kidnapping --
11 directed at a person or a group of people shall have a duty
12 to warn the intended victim or those responsible for
13 protecting the intended victim as appropriate.

14 And there are a few salient aspects of the
15 directive, including the fact that it's to warn those
16 responsible for protecting, not just the victim themselves.
17 Also, it explicitly states in the directive that tear lines,
18 so the information that's shared must omit information that
19 would compromise sources and methods. This goes to the
20 intelligence evidence problem.

21 But what's important here is that Directive
22 191 is frequently acted on. This isn't a crutch to avoid
23 warning. Rather, the expectation is warning shall be done,
24 so we must do it in a way that protects sensitive
25 information.

26 It also does clearly stipulate that warning
27 can be waived under certain conditions, and I think this is
28 really important. It goes into details as to why warning

1 might not be possible. And to me, that's critical because if
2 we discount the possibility that warning might not be
3 feasible or there might be a very, very good reason not to
4 warn, then it invites non-compliance because there will
5 always be cases in which warning can't be done. But what we
6 see with Intelligence Community Directive 191 is that, often,
7 it is done.

8 There is warning with a risk calculation,
9 with appropriate safeguards in place, so that's why I think
10 this directive is an interesting model for us to look at.

11 So what we see here in Canada with C-70 is an
12 open-ended ability to warn with flexibility. That's
13 important, but also, with flexibility and open-endedness can
14 come some confusion and even the potential for preferential
15 treatment, so this is where having some specificity can
16 actually help avoid some outcomes we might not want.

17 The other piece of relevant literature in
18 Canada I want to point to on the legislative is the directive
19 -- Ministerial direction from the Minister of Public Safety
20 in May of 2023 regarding threats to the security of Canada
21 directed at Parliament and parliamentarians, which requires
22 CSIS to ensure parliamentarians are informed of threats as
23 well as working through the RCMP, law enforcement agencies
24 and other departments.

25 So there is a requirement here, but it is not
26 as specific, so again, there's some value in flexibility. We
27 heard about interpretation. However, our partner countries
28 do have some models that have these guardrails or these

1 specifics in place that can be useful. So that's duty to
2 warn.

3 The second category is engagement with
4 external parties specific to foreign interference. And Mr.
5 Jones has mentioned a bit of this, so I'll go into a few
6 details that will be similar and build on what you mentioned.

7 We were asked on the panel whether and how
8 Canada's national security and intelligence agencies should
9 communicate with the public on foreign interference. And my
10 answer is yes, they should, and there are models within our
11 allies and partners as to how this can be done, recognizing
12 this is very nascent and no one has all the answers and
13 they're still figuring it out.

14 So Australia and the United States both have
15 these centres that have been established to tackle foreign
16 interference and to share externally. Australia established
17 their counter foreign interference coordination centre back
18 in 2018, and this supports the National Counter Foreign
19 Interference Coordinator. And I know the panel yesterday
20 actually discussed the potential for a coordinator, so there
21 is a model in Australia that's a few years old that is, as we
22 heard, relevant for us to look at here.

23 The centre has a whole-of-government approach
24 and it also, critically importantly for us, works with the
25 private and civil sectors, the wider community and
26 international partners to strengthen Australia's response and
27 resilience to foreign interference. It includes a hotline.
28 As we heard from Professor Carvin, a hotline is not

1 necessarily the answer. It depends how it's used. But there
2 is this track record in Australia of use. We could talk to
3 them about it. But also, two-way engagement with external
4 parties.

5 In the United States, the equivalent is the
6 Foreign Malign Influence Center within the office of the
7 Director of National Intelligence, which was activated in
8 2022. And the Center was established because of a
9 recognition, and this goes back to what Mr. Fadden said at
10 the beginning, about the idea that foreign interference
11 targeting democratic processes is not just in the context of
12 elections. It's 365 days a year. It's every year, there
13 needs to be an ongoing model, and so that was the basis for
14 establishing a permanent centre.

15 There are two aspects of the Foreign Malign
16 Influence Center that I believe are important for us. The
17 first is that it's not just for internal assessments of a
18 threat. There is a public notification protocol that is
19 really emphasized as part of their mission activities,
20 notifying victims and, when appropriate, the public through
21 advisories.

22 And there's risk calculation to ensure not
23 just that sensitive information sources and methods are
24 protected, but also that notification doesn't do the work of
25 the adversary, that it doesn't actually amplify the messages
26 of foreign interference. And that's explicit in the
27 documentation of the Center.

28 And then the second key aspect is that one of

1 their key pillars is external engagement, including
2 information exchanges, so it's not just about pushing
3 information. It's really about engaging, recognizing, again,
4 that the pieces of the puzzle are not all in the hands of
5 government. They're also in the hands of external parties,
6 civil society, government partners and industry.

7 So I mention these two models again to say,
8 as Mr. Jones said, that our allies are attacking similar
9 challenges in their models that are relevant for a Canadian
10 context.

11 The final category is engagement models writ
12 large looking at security issues and key characteristics in
13 them that can lead to success. And one of the exemplary
14 models here is the U.S. State Department's Overseas Security
15 Advisory Council.

16 This is an organization that's existed since
17 1985 with a mission to promote security cooperation by
18 fostering a global network of security professionals who
19 exchange timely information and security best practices. And
20 although it focuses on industry, it also includes non-
21 profits. It includes those who have pieces of the threat
22 picture, and it's been very adaptive over time to include
23 those who have pieces of the puzzle.

24 It includes Canadians, Australians, French
25 members and others who all have some relevance for the
26 security of U.S. persons.

27 And this model came up at a Public Safety
28 funded study conducted by the Conference Board back in 2017

1 that asked how Canada could improve information sharing
2 between the government and non-governmental parties. The
3 report has a lot of relevance to what we're talking about
4 today, and it was -- they surveyed Canadians. There were
5 recommendations for Canadians about Canadian institutions,
6 and yet they mentioned the State Department's Overseas
7 Security Advisory model as a model that has relevance for us.

8 The Australians also took note of this model
9 and they went to the Overseas Security Advisory Council,
10 learned from them and built their own institution called ASIO
11 Outreach. It's the Australian Security Intelligence
12 Organization Outreach branch which sits within the
13 intelligence agency but has an external engagement remit and
14 has productive conversations with businesses and civil
15 society on security questions.

16 So both of these models recognize that there
17 are external parties who want to engage who have pieces of
18 this puzzle.

19 So what are the keys for engagement? And
20 this is how I'll wrap up my discussion.

21 The successful models like the Overseas
22 Security Advisory Council, they build trust. As Mr. Jean has
23 mentioned, there's a need for a culture of engagement that
24 goes beyond just what the law permits, but actually what
25 organizations seek. And the Overseas Security Advisory
26 Council model, the agenda is driven by the external parties,
27 not just by what the government believes they want to hear.

28 The external members actually help set the

1 agenda, determine the priorities that are tackled, and that's
2 part of their success.

3 So to conclude, I have four key
4 characteristics that I've noticed across these different
5 models for effective external engagement.

6 The first one is repeat interactions when
7 possible, not one-offs. Repeat interactions build
8 credibility and build trust. That's number one.

9 Number two is two-way interaction. So
10 defensive briefings have a role to play, but two-way
11 engagement, again, builds more trust, adds more value and
12 many of my research interviewees expressed dismay at being
13 briefed one way and not being able to share back because they
14 actually did want to share back.

15 The third is building mutual understanding.
16 This was a key theme of -- in my interviews, was it's
17 important to foster knowledge of each other's knowledge,
18 capabilities, priorities and pain points. This leads for
19 better information exchange. Understanding what the
20 government can or can't do, can or can't share, can or can't
21 actually collect is really important.

22 This may not apply to briefing policymakers
23 on specific threats, but it definitely applies for engaging
24 civil society, industry and diaspora groups.

25 And then the final one, number four, is when
26 possible, leveraging already existing organizations. There
27 are recent studies that talk about the erosion of trust in
28 federal institutions, but the endurance of trust in local

1 institutions and local government and civil society groups,
2 industry groups, and the Public Safety funded study by the
3 Conference Board that I mentioned, they talk about this focus
4 on associations, pre-existing organizations, is more trusted
5 than government, and when government engages through those
6 groups to the extent possible, that results in a more
7 productive dialogue and engagement, and this goes to the
8 point by Mr. Jean about horizontal networks of engagement as
9 well being really important.

10 So to conclude, effective engagement includes
11 external parties who have pieces of the puzzle. They're not
12 just there to be briefed. It has to be two-way. They often
13 do want to engage, but as we've heard, it actually has to be
14 a genuine engagement. And our partner countries have models
15 that are instructive and have some value when we look at them
16 in a Canadian context.

17 Thank you.

18 **COMMISSIONER HOGUE:** Thank you.

19 **DR. LEAH WEST:** Thank you. I think this will
20 bring us to the end. We'll take a break.

21 **COMMISSIONER HOGUE:** Yes. And I will say
22 there's a lot to look at, so we'll take 30 minutes, but we'll
23 be together. We'll be able to review questions received from
24 participants and then we'll come back. So roughly we should
25 be able to resume at 11:10/11:15.

26 --- Upon recessing at 10:39 a.m.

27 --- Upon resuming at 11:26 a.m.

28 **COMMISSIONER HOGUE:** We have a lot to

1 discuss, so I suggest that we start right away.

2 **--- OPEN DISCUSSION:**

3 **DR. LEAH WEST:** So there are many questions
4 that came in, and so we're going to kind of group them
5 thematically.

6 And one of the first things actually harkens
7 back to what Mr. Fadden started off with, which is this
8 culture of understanding the threat. Canadians understanding
9 what it is that FI is and who to talk to, and understanding
10 the intelligence that is being put out, and trying to improve
11 that understanding. And so this goes a lot to the education
12 of the Canadian public about this threat.

13 So I'm going to actually ask Dr. Carvin, if
14 you'd like to start, and talk about how the community, the
15 intelligence community, can do a better job of educating the
16 public about this threat so that there is better engagement?

17 **DR. STEPHANIE CARVIN:** Thank you for your
18 question. So there's a number of steps that I think could be
19 taken. First of all, I think better communication depends on
20 better understanding; right? So I think the community itself
21 needs to educate itself on the communities it wishes to speak
22 to; right? There's going to be differences. Even within
23 communities there's going to be big differences. Like, if
24 you're, you know, I don't know if the community has come up,
25 but, like, there's been talk of foreign interference in the
26 Eritrean community. There's a lot of division and
27 differences in that community, and knowing how to speak to it
28 I think is going to be very important.

1 Now, are you going to have someone who is
2 just able to speak that language and do -- it might be asking
3 a lot of a very small community. But there's a lot more that
4 we can do.

5 So secondly, I think it requires
6 specialization. I spoke earlier about the issues with
7 generalists and the need for more specialization. Again, we
8 are a small community. This will be difficult to do. But
9 the community itself needs to find the capacity to develop
10 that expertise within, and that might be perhaps looking
11 outside the normal kinds of areas of recruitment, more
12 anthropology, more -- and perhaps even social work at some
13 point. You know, like, kind of thinking outside the box in
14 terms of how you go and work with these communities I think
15 would be fundamental. And I appreciate that this is a
16 challenge.

17 So those better understanding -- and then the
18 other points I raised in my commentary was the need to craft
19 products that are nuanced, that are in the language of the
20 communities, that you need to take -- that they're not just
21 direct literal translations of those documents.

22 I have spoken to people in the Chinese
23 diaspora, and they're like, "Yeah, we can tell when someone -
24 - when something got put through, you know, ChatGPT or Google
25 Translate." It's not going to cut it; right? Those nuances
26 need to be there.

27 And then finally, there is an issue with
28 regards to how -- the actual means of communication. And I

1 appreciate that, like, you know, there's some talk of doing
2 more reporting and stuff like this. If we generate another
3 200-page report that's available in English and French, yes,
4 some people may read it, but we need to be thinking about
5 better crafted documents, reports, for how we do this, and
6 possibly utilizing new means of communication. I appreciate
7 not everyone agrees, but being able to take the key messages,
8 right, maybe just the key messages and putting those into
9 some kind of video. Not necessarily on the threat. I guess
10 the model I would put out is, that you and I would be
11 familiar with, Professor West, would be the three minute
12 thesis; right? The three-minute thesis is -- you don't get
13 all the nuances of someone's PhD, but they should be able to
14 convey to you the key messages of your PhD in three minutes.
15 That's the idea of that.

16 And, you know, I think that might be not the
17 model, it would a tool in a toolkit that then might help get
18 people to understand what some of these issues are, and then
19 provide access to resources and other pathways that they
20 could learn more about the threats, or perhaps even bring
21 some information that they had forward.

22 **DR. LEAH WEST:** Mr. Fadden?

23 **MR. RICHARD FADDEN:** Thanks. I'd like to try
24 to approach this from a slightly different perspective,
25 although I agree with what Stephanie was saying, except her
26 three-minute specials, but that's for another day.

27 We have to remember that public officials who
28 are operating in all of these agencies actually work for

1 Ministers. And aside from the cultural change issue, there's
2 a real risk aversion on the part of Ministers which has grown
3 tremendously over the course of the last 20 years. And
4 people don't want to take any chances.

5 So one way of encouraging public education,
6 more discussion, would be for the government of the day,
7 whoever forms that government, to clearly indicate that
8 they're willing to encourage this. And if they take all of
9 this seriously, they should do that.

10 The other way of doing this, and I would note
11 that agencies, as opposed to departments, are much more
12 closed than departments. It's harder to change them. And
13 one way of doing it is through the issuance of very, very
14 clear instructions.

15 I'll give you an example. I've headed two
16 agencies, and in one of them, something that had never been
17 done before, they didn't want to do, it was against their
18 professional judgement, I got a call from the Clerk who said
19 he had been speaking to the Prime Minister, blah, blah, blah,
20 blah, and by the time we were finished, a quarter of a
21 billion dollars had been spent with very, very clear
22 instructions that that agency had to do A, B, C.

23 If you tell the head of head of CSIS, the
24 head of CSE, of FINTRAC and whatnot, clearly, unambiguously
25 -- tie their bonus to it if you want to -- that they have to
26 come up with concrete examples of how to communicate, that
27 would go some distance. But I think though that you have to
28 acknowledge that the Commissioner's recommendations in the

1 short-term cannot rely on cultural change. They take time.

2 So I would substitute that with, you know,
3 sort of beating Ministers about the head to be very
4 supportive and issue very clear instructions that you want A,
5 B, C done.

6 One thing agencies tend to do well is if
7 they're given very clear instructions, they tend to obey.
8 And it's a poor substitute for real cultural change, but in
9 the short to medium term, you may actually get some movement.
10 This along with the things that Stephanie's talked about.

11 **DR. LEAH WEST:** Dr. Robson-Morrow?

12 **DR. MARIA ROBSON-MORROW:** Thank you very
13 much. To add a third perspective that tackles a different
14 part of the educating question, we've heard about engaging
15 community elements, engaging diaspora groups. There are so
16 many different threat vectors in terms of how foreign
17 interference can manifest, who the targets are, and so
18 there's a risk in broadbrush approaches. There's public
19 advisories, but often they're not really targeting one
20 particular group and there's a limit to who will actually
21 access them, or be interested in them, or really understand
22 what the message is.

23 But one aspect I wanted to highlight was
24 engaging with universities, because I think this is a really
25 important aspect of the attempts to counter foreign
26 interference in Canada and elsewhere. So CSIS has been more
27 actively engaging. I know Global Affairs Canada also engages
28 with universities on research security. And I know the

1 Commission's focused specifically on democratic processes.
2 But I think it's all interrelated. It's all different ways
3 that adversaries can target our institutions and intellectual
4 leaders and students and so forth.

5 But we mentioned the Australian models
6 earlier, so I wanted to come back to Australia, because
7 Australia, in addition to the Centre we talked about earlier,
8 has a university task force that was established in 2019 that
9 engages government that's engaging directly with the
10 universities to try to build this understanding of foreign
11 interference, what it means for research for educational
12 institutions. And so I think that's a relevant model. And
13 also just a broader message of when we think about engaging
14 the public, there are all these different elements to the
15 public to think about.

16 **DR. LEAH WEST:** Just to follow up on that,
17 when you mean they're engaging with universities, is it only
18 on research security, or also to deal with foreign students
19 and the vulnerabilities there?

20 **DR. MARIA ROBSON-MORROW:** I think I'll not be
21 the only one to speak to this, but much broader than just
22 research development and research security. Certainly
23 foreign students, I don't want to speak too much outside of
24 my experience on this issue in talking to practitioners on
25 this issue, but I believe the emphasis on focusing the
26 culture of international students being welcomed and part of
27 the university fabric while still recognizing risks that they
28 might be targeted, foreign interference risks that

1 adversaries might be targeting the universities, so certainly
2 broader than just research.

3 **DR. LEAH WEST:** Thank you.

4 Mr. Jean.

5 **MR. DANIEL JEAN:** Maybe I can talk about
6 Australia, but start from the big picture to go to where they
7 are now.

8 In 2017, Prime Minister Turnbull basically
9 realize that Australia were up to their elbows into Chinese
10 foreign interference. And the move that he did, which was a
11 very interesting move, is he basically went and hired as a
12 special advisor, John Garnaut, who was journalist, lawyer by
13 training, who was covering China, sinologist. And he brought
14 him in, gave him all the security clearance and he paired him
15 with the Director of ASIO, who is the CSIS equivalent. And
16 he was basically given the task to internally look at all the
17 stones of foreign interference in Australia. At that time
18 they were focusing on some politicians, political donations,
19 that's the thing that you saw in the media, 2017.

20 When John Garnaut started to work with Asia
21 on all of those things, this is when he started to realize,
22 oh my God, our universities, particularly the Tier 2, the
23 ones who are struggling more for money. Students in
24 sensitive programs, this is when they started to see the
25 issue of diaspora intimidation and monitoring and all that.

26 So the first wave of measures were to deal
27 with their biggest issues. So they dealt a lot with, you
28 know, political donations, foreign -- they reinforce their --

1 the equivalent of what is -- over there it's one function,
2 the Election Director General and the Commissioner for
3 Elections; they reinforce that. They took a lot of measures.

4 John Garnaut actually, once this report was
5 done -- because what happened after that is the Cabinet look
6 at the threat assessment, they went with this and they
7 adopted all these measures, they started to come publicly.
8 At some point there's a Chinese affiliation that came to
9 this. John Garnaut, by the time that he was leaving was
10 actually hired by the universities to do their reviews
11 because of some of the things that had been identified.

12 So I'm just saying there that you've got to
13 understand the context of Australia, this came -- like, in
14 this Inquiry, we find intimidation of the diaspora is a big
15 issue, much bigger issue than what the common people know.
16 For the experts, not a surprise but the common people in
17 Canada.

18 But in the assessment in Australia this was
19 not the biggest issue at the time. They had much bigger
20 things. But through this they discovered that, and it became
21 in their second wave. Like, for example, they have their
22 first trials right now, they've been successful in the
23 Foreign Agents Registry, which was also created in 2017. So
24 my advice on this is you've got to make sure that what you're
25 creating is the right remedy for the -- right cure for the
26 illness that you have.

27 What I'm worried about when I hear the
28 conversation here is, yes, culture takes a long time, and

1 yes, you can take some short-term measures like what you're
2 proposing, Dick, but if it's only driven with a whip, it's
3 not something that they build and make it part of their DNA
4 that they're going to engage regularly, proactively, they're
5 going to be more sensitive to what the diasporas are, that's
6 going to be a problem. In the same way communicating to the
7 public you need to find a way to communicate that the
8 ordinary citizen understand why they should care.

9 You know, I see all the experts who say, "We
10 want a threat assessment, we want this"; I'm not saying it's
11 not necessary, but that's not what the ordinary citizen is
12 going to read.

13 So there is a way to come up with some ways
14 to get the citizen interested in to why they should care. Is
15 that -- you said three minutes, video-type approach where you
16 get to a case for them to understand why it is a concern that
17 they should care. Using credible third parties is very
18 important for all communication. But I'll leave it there.

19 **DR. LEAH WEST:** So this goes to my -- the
20 next kind of theme was that talk about culture change within
21 the organization. So not just making sure Canadians
22 understand the threat better, but that the organizations
23 understand the threat environment better so that they can do
24 their jobs, but then that level of culture change down on the
25 ground and engagement. And I guess I'm wondering what
26 advice, Ms. Gill, you would have for people thinking about
27 that kind of engagement that people on this panel all seem to
28 agree is necessary.

1 **MS. LEX GILL:** Yeah. It's interesting, I've
2 been thinking a lot about this since Mr. Jean's comment
3 regarding having sort of boots on the ground and going back
4 to tactics that might have been more commonplace in the past
5 around door-knocking, getting directly in touch, face to
6 face, with communities.

7 I mean, I have some real concerns about those
8 practices. I think Professor Carvin did a really great job
9 sort of articulating some of those concerns.

10 The reality is, you know, the trust in these
11 agencies is extremely low among civil society groups, among
12 diaspora groups, among human rights defenders, and that's not
13 for no reason. That's because, unfortunately, there have
14 been situations of abuse, of overreach, of surveillance of
15 Indigenous and environmental groups, of human rights and
16 anti-war groups, and the long shadow of the post-9/11 era.

17 And I think that it's important to understand
18 that some of those tactics are still taking place in ways
19 that are inappropriate, the sort of door-knocking and stuff
20 like that. And I think that we really need to have a totally
21 different perspective on how to build these relationships and
22 rebuild these relationships, you know.

23 And I think that sometimes when I hear people
24 -- and I say this with a lot of respect, when I hear people
25 sometimes from the intelligence community talk about the sort
26 of -- the frustrations around these tactics as a sort of
27 like, "Oh, that's a post-9/11 thing," like almost like people
28 need to get over it, we need to move -- this is not ancient

1 history in these communities. There are -- you know, and I
2 don't want to speak on -- you know, on behalf of Arab,
3 Islamic, and Sikh people, but what we hear from those groups
4 is the issues continue. And look, I mean, today also those
5 issues are also informing how those communities are
6 experiencing, like, government action around Palestine, which
7 I think is enormously complex and -- you know, I'll give a
8 very specific example. There was an entity recently added to
9 the Terrorist Entities List, okay? And without taking any
10 position on whether that entity should be on that list or
11 not, what I can say is that there has been a tremendous
12 failure of communication around that listing to the extent
13 that, you know, organizations that are organizing, like,
14 Shabot dinners for peace, all of a sudden think that, you
15 know, they might be treated as terrorists by their own
16 government.

17 And so the sort of chilling effect of these
18 kinds of decisions when they're not properly communicated,
19 when there isn't effective, meaningful, transparent
20 relationships with communities that are affected by the work
21 of our intelligence agencies, there's really serious
22 consequences for that.

23 And so in a context where the trust is very,
24 very low, the best practices look like dealing with
25 established leadership of these groups, of groups in these
26 communities, in transparent, open ways. And not showing up
27 at the mosque to talk to the person who's sitting next to you
28 in line, and not hanging out on campus at the vegan soup

1 kitchen or whatever to see what you might learn, because the
2 reality is those kinds of tactics, no matter how well-
3 intentioned, are going to create paranoia and mistrust and
4 anxiety that can be almost as intense and harmful as the
5 paranoia and mistrust and anxiety being created by the
6 foreign interference, so...

7 **DR. LEAH WEST:** Mr. Fadden, then Mr. Jean,
8 then Mr. Jones. So if you can keep your interjections brief.

9 **MR. RICHARD FADDEN:** I guess I'd just like to
10 present somewhat of a different side of the story that Ms.
11 Gill was just articulated.

12 There are occasions when knocking on a
13 person's door, when the person does not know you're coming,
14 could prevent a loss of life. There are occasions when it's
15 absolutely necessary, and I hope you're not excluding that in
16 every single case. But it seems to me, though, that the only
17 way that we're going to change -- we're talking about
18 bureaucracies here, we're talking about hundreds and
19 thousands of people.

20 So I think culture change is necessary. I've
21 tried to effect it in every job I've had, but if you're going
22 to change how CSIS interacts with members of the diaspora
23 community, the Director of CSIS is going to have to issue a
24 series of broad instructions about the range of tactics they
25 can use, when they can use them, and why. That will have
26 more of an impact than all of us, including myself, going on
27 and on in front of the Commissioner talking about cultural
28 change. We're dealing with bureaucracies. That's not the

1 same as a small law firm where you have 10 people or, you
2 know, an engineering firm, you have five people and you want
3 to change things. At some point you have to take whatever
4 the heck you're talking about and reduce it to standing
5 operating procedures, and I think in the end, that has to
6 come from Ministers telling the agency and the departmental
7 heads they have to do it.

8 I go back -- I mean, I agree with what Daniel
9 said. It's not ideal. I think cultural change from the
10 bottom is wonderful, but it is so slow, we need to find
11 alternatives to move it a little bit in the direction of
12 better practices, sooner rather than later.

13 **DR. LEAH WEST:** Mr. Jean?

14 **MR. DANIEL JEAN:** So to echo some of the
15 comments that Lex has made, I sit on the Transparency
16 Advisory Committee of the Deputy Minister of Public Safety
17 and we've issued a report on racialized and marginalized
18 communities, and when we were doing this report, we met with
19 a lot of the communities who are raising these concerns here,
20 and also we've met with the senior officials of the various
21 agencies.

22 For me, and by that time I was five years out
23 of government, so I feel as much as a civil person as I used
24 to for a long time to be a bureaucrat, and I just couldn't
25 believe the distrust. I basically felt that the way the
26 communities were describing what were my colleagues, I know
27 they're not that bad; right? And we've got to be careful not
28 to take the one thing that goes wrong and generalize that in

1 everything. It's true in every daily activity.

2 And then on the other hand, I could see that
3 there was efforts by the agencies to which they're engaged,
4 but they still saw that very much as engagement of we meet.
5 You know, it's punctual, it's not meaningful engagement, and
6 trying to change the culture of the organizations too. But
7 they're real efforts.

8 You know, Director Vigneault was very clear
9 to the Muslim community, "We need to protect you. You know,
10 look what's happened in Quebec. What's happened in London.
11 We want to work with you." Right?

12 So you need to close that gap, and you're
13 absolutely right, because we heard that as well, that they
14 still see that if they're coming to meet them, they're more
15 to get information than to give them information or to
16 respond to some of their grievances. So that part is very
17 much there.

18 These agencies, they do incredible
19 recruitment efforts to be representative of Canada. In fact,
20 CSE has a real challenge because in the computer science
21 thing, the labour market availability of people from visible
22 minorities is so high in Canada that CSE is very high, but it
23 keeps trying to jump. CSIS is doing some real efforts, but
24 sometimes people that would be very helpful may not wish to
25 come. I was sharing an anecdote of brilliant Sikh analyst
26 that worked with PCO wanted to go work for GAC. I said,
27 "Getting a job at GAC is like winning the lottery. Here are
28 all these organizations that have international --" and then

1 when I said, "CSIS, they could really use somebody like you
2 for what we're discussing today," and he looked at me, and,
3 "I could never do that."

4 We have to find ways to change this distrust,
5 because otherwise it's not going to happen.

6 **DR. LEAH WEST:** Mr. Jones, and then Ms. Gill.

7 **COMMISSIONER HOGUE:** I think, because I'm
8 looking at the clock, there's one question that I would like
9 you to address in connection with this one, because you're
10 focusing on the various communities, which is absolutely
11 useful, but I would like also to get your views as to whether
12 you think we also need to engage in, and to a certain extent,
13 educate the Canadian in general about what we are speaking
14 about? What is national security, what CSIS is doing, what
15 CSE is doing. So I'm asking the question. Anyone can
16 answer.

17 **DR. LEAH WEST:** Mr. Fadden?

18 **MR. RICHARD FADDEN:** I think absolutely. The
19 issue is not whether we should do it, it's how we do it. I
20 think it goes to the definition of national security.
21 Shantona and I were talking in the meeting room about the
22 definition of intelligence. Nobody understands what the
23 devil intelligence is, and the minute you say "intelligence",
24 everybody's blood pressure goes up, you know, by 50 percent.

25 So even something as simple as that, so the
26 question is who can do it effectively, and using what medium?

27 If you -- you will have gathered from my
28 earlier comments that I think that a lot of these issues, the

1 further you keep Ministers from this, the better off you are.
2 Not that they're not ultimately responsible politically, but
3 if you have, within the Public Service, for example, a
4 requirement that for all of the kind of communications,
5 Commissioner, that you're talking about, they would have to
6 be reviewed by Ministers, and depending upon the time of
7 year, the period in the electoral cycle, risk aversion would
8 prevail and we would go off on a tangent.

9 To pat myself on the back, I think my panel
10 of the great and good have given sufficient resources and a
11 mandate at some distance from government, and I mean a mixed
12 panel, I don't mean people from the security community, would
13 be better placed to start doing all this kind of
14 communications, using government resources if need be, but
15 the planning and the strategy being taken a little bit out of
16 government because it's the sort of thing that if you're a
17 Minister, there's no win. There's no way you can have this
18 communication without having somebody somewhere accuse you of
19 all sorts of nasty things. So I would say absolutely yes.
20 Who? Some distance from government.

21 And it's the sort of thing where you're going
22 to have to repeat it until you want to kill yourself almost,
23 because people do not register these things initially. It
24 would have to be an ongoing campaign modified over time.
25 It's just -- people just don't remember these things unless
26 it affects them personally. So it would have to be an
27 ongoing permanent effort, I would submit.

28 **DR. LEAH WEST:** Dr. Carvin, I just want to

1 add to that, on top of that, we've heard a bit about
2 different institutions or organizations that could be
3 proposed to do this. So we've heard about changing the role
4 for the Panel of Five. We've also heard about the Australian
5 model for Centre for Foreign Intelligence, National Security
6 Council, and, you know, there's two other things I want to
7 put on the table about organizations that we haven't talked
8 about that might be models.

9 One is, is there a need for a foreign
10 intelligence agency? How would that come into play here?
11 That is a question we have received.

12 And the other one is thinking to the Canada
13 Centre for the Prevention of Violent Extremism and its model
14 of funding and education and whether or not that might be
15 something useful in this space.

16 So Dr. Carvin?

17 **DR. STEPHANIE CARVIN:** I will address those
18 two points, but just coming off the question about who should
19 do education, I think I spent the first part of this panel
20 promoting my research, and now I'm going to ask for funding.

21 So we can also ---

22 **COMMISSIONER HOGUE:** I'm not the one who can

23 ---

24 **DR. STEPHANIE CARVIN:** Just if anyone is out
25 there. Government.

26 But the -- not just entirely self-serving,
27 but it's also about, you know, how do we better -- how do we
28 get Canadians to better understand this?

1 I mean, there are very few programs out there
2 at the secondary educational level that really deal with --
3 or sorry, second or third tertiary education that teach these
4 issues; right? I mean, we could start with, like, just basic
5 civics would be helpful I think generally in understanding
6 our democracy better, and strengthening our democracy goes a
7 long way just to do that. That's probably outside the scope
8 of the Commission, but, you know, better funding programs
9 that deal with security intelligence issues.

10 It's sometimes hard to get funding. I
11 understand, because sometimes the research bodies say, "Well
12 this should be funded by the government," then the government
13 doesn't really necessarily want to fund a bunch of -- I'm
14 tempted to use -- I'll just say academics, because we're
15 academics. And I get that too.

16 But I think even just creating better
17 education about these issues at, you know, the graduate
18 level, the undergraduate level, even perhaps having more
19 experience in high schools I think would -- or CEGEPs would
20 be helpful on that.

21 So I think, like, just creating, again, more
22 -- is there a need for courses on foreign interference? Is
23 there a need for courses on the diaspora experience? Right?
24 Better understanding what these -- who these diaspora are and
25 what their experiences are. I think it doesn't just have to
26 be from a security lens. It could be from, like I said,
27 anthropological, social work, all those other kinds of
28 things.

1 Regarding a foreign intelligence agency, wow.
2 I mean, like, if we're playing fantasy national security,
3 sure, it would be great to have a foreign intelligence
4 agency.

5 One of the things you hear in talking to our
6 allies is, you know, you often hear kind of talk about how
7 bad Canada is at national security and how our institutions
8 are a joke and we're going to be kicked out of the Five Eyes.
9 And I want to stress how much that's not true, that actually
10 Canada is respected in the Five Eyes.

11 The problem isn't that we're not respected,
12 the problem is they want more of us; right? They want us to
13 do more. They -- you know, this is often what you hear from
14 our Five Eyes partners.

15 So yeah, a foreign intelligence agency would
16 be great. Is it the best place to put limited resources now?
17 I don't know.

18 Where would that intelligence agency go?
19 Would it be part of GAC? Would it -- you know, people think
20 you can just kind of tack it on to CSIS, but it would be
21 operating under an entirely different legal regime and I
22 think it would put real strains on that organization.

23 It's a really difficult, perplexing
24 challenge, and as we are confronting the threat of foreign
25 interference -- yeah, I think -- the benefit of a foreign
26 intelligence agency would be that you would -- we're so
27 heavily reliant on other countries that when we get their
28 intelligence, we're getting it from their perspective. It

1 reflects their interests, it reflects their priorities.

2 If we were thinking about how foreign
3 interference would help us, yes, it would give us a better
4 understanding, I think, of what the priorities of those
5 governments engaging in foreign interference in Canada
6 actually is, but I'm just not sure it's the best use of our
7 money at this time as much as I think it would make our
8 allies happy and possibly add a little bit of understanding.

9 But I think the priority needs to be just
10 fixing the mess we're in now, and I'm not sure the foreign
11 intelligence agency would do that.

12 I'm a fan of the Canada-centre model. The
13 Canada-centre model is where it's kind of foreign -- like
14 they say it's at the national level. It provides funding at
15 provincial level, provincial level -- I think there's five
16 institutions that it presently provides money to. There's
17 Shift B.C., there's one in Alberta. I think the Organization
18 for the Prevention of Violence. There's the Yorktown Centre
19 in Toronto. And then there's two in Quebec.

20 It's good, right. I mean, the issue with
21 those organizations is how well they have done in terms of --
22 you know, they're more in demand. Like they actually need --
23 they need more resources, not less.

24 They've actually done well, and communities
25 have learned that they can go to those organizations because
26 they're not the police, right, even though sometimes they're
27 referred to -- in cases they're referred to by police, and
28 they get the help from a public health perspective, not a

1 security perspective. And I think that's really important.

2 So there's lessons to be learned there.

3 But that being said, foreign interference is
4 very, very different from radicalization, right. And you
5 know, with radicalization you're trying to get people help
6 and interventions and counselling and things like this. So I
7 don't know what it would do other than kind of be a
8 repository for information.

9 It might be a better model for community
10 engagements because it's not CSIS and people might feel safer
11 going to those organizations knowing they're talking to the
12 government. Maybe you could triage it.

13 But we'd have to put some thought into it. I
14 don't think it's an automatic cut-and-paste model you could
15 just kind of throw into the provinces.

16 **DR. LEAH WEST:** Dr. Robson-Morrow and then
17 Mr. Jean.

18 **DR. MARIA ROBSON-MORROW:** Thank you very
19 much.

20 This will be a brief point going back to the
21 discussion of building and understanding of the intelligence
22 agencies, the idea that we on the panel may understand the
23 differences between CSIS, CSE, what they do, what
24 intelligence is. This is not something we should take for
25 granted.

26 On that point, there is discussion the Five
27 Eyes have about proactive disclosure of intelligence and the
28 idea of disclosing successes, not just allowing the narrative

1 to be around failures or shortcomings. So I did want to make
2 sure we touched on that, this idea of encouraging more of a
3 culture of highlighting what intelligence can actually do in
4 a way that does touch communities, touch Canadian democratic
5 processes, protecting the public because intelligence risks
6 being the goalie. No one remembers the shots that don't go
7 in, remember the failures. We don't necessarily remember or
8 know about or be able to know about the successes.

9 And going back to Mr. Fadden's comment about
10 us being risk averse, we talk about the culture of secrecy.
11 CSIS was born out of the perceived overstepping out of the
12 MacDonald Commission, was born deliberately with safeguards
13 and constraints on it, so I think there's value in thinking
14 about ways to disclose intelligence.

15 Just in the past few years, we saw in the
16 lead-up to the Russian invasion of Ukraine the Five Eyes
17 proactively disclosing intelligence, revealing the game play
18 in a way that this was in the news, particularly when Ukraine
19 was invaded. It was all over the news, and so there was an
20 understanding of what intelligence agencies have been doing
21 behind the scenes to try to effect an outcome that we all
22 understood to some extent.

23 So just thinking about -- I'd suggest that we
24 should think about -- the intelligence community should be
25 thinking about ways to proactively disclose this type of
26 thing.

27 We can remember the Toronto 18 as a rare case
28 where we actually understand that intelligence agencies

1 contributed to a positive public security outcome, so
2 thinking about more ways to build credibility and build an
3 understanding of what intelligence is and what the agencies
4 do.

5 Thank you.

6 **DR. LEAH WEST:** Mr. Jean?

7 **MR. DANIEL JEAN:** Reacting to a few of these
8 points.

9 First of all, Panel of Five, agree on
10 independence, but we've got to be careful to see, first of
11 all, whether there's existing mechanisms in place,
12 independent mechanisms in place like Director of Elections,
13 Commissioner of Elections that can take some responsibility,
14 and then what's left.

15 I agree with the objective on communication.
16 I have my doubts that if you were to create the organization
17 they would communicate differently than our review mechanisms
18 that exist do, which is the same, issuance of reports that
19 are not read.

20 I applaud their work. I read it. But to the
21 citizens, they don't read it.

22 So I like the -- what -- your question about
23 the radicalization council. I've been exposed to it. What
24 is interesting is that model is because you go try to
25 leverage people closer to the citizens or to the community,
26 so you really leverage these third parties which I was
27 referring before.

28 I said before, be very careful. There's a

1 bit of an habit of where we have a problem, let's create a
2 structure, right. And most of the time, it takes a lot more
3 than structure to create problems.

4 We're also in an environment where money is
5 going to be rare, I think, here, given our fiscal situation.

6 And there's also -- the other thing that you
7 hear very often is centralization, everything in PCO. You
8 know, PCO would become the department of all departments.
9 But the resources are in organizations.

10 After 9/11, it was probably a normal reflex,
11 we centralized a lot of things in PCO and then we suddenly
12 found if you want things to be happening, PCO has to play its
13 role, but the energy, the efforts, the talent is in the
14 department. You need to responsilize [sic] them in doing
15 that.

16 The foreign intelligence Five Eyes, I love
17 what you said. I travel -- you think the NSA doesn't stay in
18 place too long in Canada? I had four U.S. NSAs during my two
19 years' term as NSA in Canada.

20 I met a lot of the NSAs around the world,
21 these agencies, and what I hear is what Stephanie described,
22 which is to say, Five Eyes is a work-sharing mechanism.
23 Their expectation is not that we're going to produce the same
24 volume or the same thing they produce. A work-sharing
25 mechanism is that you bring the expertise in a complementary
26 way and what they love is we bring added value. As long as
27 we bring added value, we'll be welcome.

28 My concern with the foreign intelligence

1 agency has always been the same. We are very good, I said
2 that earlier, at the beginning. We create structures, we
3 don't resource them, and we wonder why they don't work.

4 So I would much rather have a very strong
5 national security apparatus that functions well, that does
6 well, that provides its added value to our allies and
7 partners like the Five Eyes than rather to create another
8 structure but not equip them to be able to do what they need
9 to do.

10 **DR. LEAH WEST:** Ms. Gill.

11 **MS. LEX GILL:** Yeah, it might be a minute
12 since this was like really relevant, but I do just want to
13 offer like a little bit of a synthesis of some of the themes
14 that are coming out here in the sense that I think that
15 sometimes there is this tension or conflict that's being
16 presented between being transparent and being effective or
17 respecting human rights and being effective as an
18 intelligence agency, and I think that, in fact, a lot of the
19 comments are really circling around this idea that one can
20 feed the other in the sense that, if there is proactive
21 disclosure, if there are strong relationships that are built,
22 if there is really a robust culture of justification, of
23 transparency, of openness, of explaining what it is that
24 these agencies do to the public within government, then that,
25 over time, can build a foundation of trust and legitimacy,
26 and that becomes self-reinforcing.

27 And so I think that it's important for us to
28 step away from a paradigm where these things are necessarily

1 in conflict and, instead, look to ways in which they can be
2 more reinforcing.

3 So I just think it's -- it would be helpful
4 in the Commission's work to think about that not as a zero-
5 sum conflict.

6 **DR. LEAH WEST:** Going back to the
7 Commissioner's question about education, one of the questions
8 from a party was about the idea of doing a national threat
9 assessment before Parliament, or something to that effect,
10 where there is an annual kind of airing of threats to the
11 Canadian public.

12 Does anyone have any thoughts about the
13 success of that kind of mechanism?

14 **MR. RICHARD FADDEN:** To be honest, it's
15 something that's been advocated for the last 15 years, not
16 exclusively with respect to foreign interference, but more
17 broadly in the national security area.

18 We've never succeeded in doing it. I mean,
19 CSIS produces something, Defence Department produces
20 something, FINTRAC produces something, and you know,
21 sometimes the assessment unit at PCO sort of pulls things
22 together for internal use, but Ministers have very strongly
23 resisted doing a global threat assessment, certainly in my
24 time, despite the fact that all of our allies, to one degree
25 or other, do it. I personally believe that we're barking up
26 the wrong tree if we're suggesting this.

27 Also, because anything that has to be tabled
28 in Parliament becomes so milquetoast by the time it's gone

1 through the various, you know, checks and balances for
2 partisan purposes. If it's done, it's not going to harm
3 anybody. And it may well help. But if we put all of our
4 money in that particular approach, I don't think it will have
5 the practical effect.

6 For us in the bubble? Absolutely. For a few
7 of you in universities? Absolutely. A few journalists. I
8 was in Toronto recently on something totally unrelated to
9 this, and I started talking about some of this, and all I
10 got, from very intelligent, well-educated people, utterly
11 blank face. My son lives in Vancouver, exactly the same.

12 So, a parliamentary report on threat
13 assessments, I think it's a good idea in and of itself, but
14 it's not going to, I think, solve the problem that we're
15 talking about.

16 I think -- I'm old enough to remember
17 Information Canada. I don't know if any of you do? It was a
18 funny agency that I think the first Trudeau Government
19 created to try and get governmental information out. And I
20 think, on balance, because that's all they did, and they had
21 a fair bit of resources, they had some measure of success.
22 It was outside of any particular department and agency, but I
23 think -- at least in the short to medium term, maybe that's
24 somewhere to go, or add that on to another department or
25 agency.

26 But it's going to take, I would argue, a
27 standalone effort, whether it's within an agency or in a new
28 agency. And I come back to my point, I apologize, it has to

1 be at some arm's lengths to Ministers or everything that's
2 produced will be so risk averse and so diluted that nobody
3 will read it.

4 **DR. LEAH WEST:** Mr. Jean?

5 **MR. DANIEL JEAN:** If you want a more
6 effective communication with the citizens, you have to be
7 able to show them why they should care. And we've had a very
8 interesting experience like when we did the Graduate School
9 of Ottawa U Report on National Security about two years ago,
10 Dick was on it as well, co-authored by Thomas Juneau. When
11 we released our report, the biggest coverage, all newspapers,
12 some television, some continue to quote it in Quebec.

13 And as a Quebecker, I personally think that
14 one of the reasons why Quebeckers care more and their
15 journalists care more about this report than in some of the
16 rest of Canada, because Quebec is not -- Quebec is not the
17 most sensitive province with regards to Canada's national
18 security. But why were they interested in this specifically?
19 Because it is a province that is very dependent on export
20 towards other countries, mainly the US. Our journalists are,
21 you know, dealing with that because they care. It's their
22 job that depends on that. So hence what I'm trying to say,
23 we have to find why Canadians should care about that. And we
24 have to speak into a simple language with images using third
25 parties also because otherwise it's going to be totally
26 useless.

27 **DR. LEAH WEST:** Commissioner, did you have a
28 question that you'd like to ask? If not, I have many, but

1 I'll turn it to you.

2 **COMMISSIONER HOGUE:** No, go ahead, and I'll
3 ask my question -- I find a way of asking my question.

4 **DR. LEAH WEST:** There's been a lot of
5 discussion over the past few weeks about who read what, when,
6 how, whether or not it was sufficiently communicated, whether
7 or not the analysis was reflective of the issue, people
8 digesting the intelligence, et cetera. So, the nitty-gritty
9 of intelligence analysis and digestion and sharing of
10 intelligence analysis. We did hear a bit about it from
11 Dr. Carvin and Daniel Jean, but I was just wondering if
12 anyone else wanted to speak to that issue in particular,
13 about augmenting Canadian intelligence analysis capacity,
14 centralizing it, et cetera.

15 Anyone? Mr. Fadden.

16 **MR. RICHARD FADDEN:** I'm going to, to some
17 degree, reverse what I've been saying about Ministers. I
18 worked off and on in national security since Mr. Chrétien and
19 9/11. And the extent to which the community is a resource,
20 the extent to which the community is listened to, the extent
21 to which they can have an impact, is almost exclusively
22 dependent upon the views of the Prime Minister of the day.

23 I would argue, with great respect, the
24 current Prime Minister is not particularly interested in
25 national security, and that permeates the system. I'm not
26 saying he's disinterested, but he's not particularly
27 interested.

28 Somebody was saying a little while earlier

1 about, you know, getting information up and making sure it
2 goes. I was in PCO during the end of Mr. Harper's time, and
3 we were still involved in Afghanistan, and let me assure you
4 that if the community had anything on Afghanistan, he got it.

5 So, I cannot overstress the importance of the
6 *tournure d'esprit* of the Prime Minister, because he does have
7 a special role in national security. And because political
8 power is so centralized in Canada, even if you have a Public
9 Safety Minister who's the most enthusiastic man or woman on
10 the planet, if the PM ain't interested, you can create new
11 assessment regimes, you can create new -- I think Daniel and
12 I disagree a little bit, I think the National Security
13 Council is smoke and mirrors. If the Prime Minister is
14 interested in national security, you can have the effective
15 conversation around a coffee urn. If he is not interested,
16 you can create all sorts of institutions, which may help, but
17 won't solve the problem.

18 So, I think in the final analysis, you know,
19 more assessment units, better communications, all fixable up
20 to a point beneath the level of Ministers. But if the Prime
21 Minister or the government of the day, unlike the United
22 States, unlike the United Kingdom, unlike France, not
23 fundamentally interested, it's sort of like pushing
24 spaghetti, if you'll forgive my use of the analogy. They are
25 really critical in this.

26 And the counter to this is that when we have
27 a real crisis in Canada, it's amazing how we galvanize
28 ourselves. But people have not come to the conclusion yet

1 that FI is a real crisis. 9/11 was a real crisis. SARS, to
2 your point, was a real crisis. And I think, I hope,
3 Commissioner, you can factor some of this in your
4 recommendations because if the PM of the day, whether it's
5 Mr. Trudeau or Mr. Poillievre, are fundamentally disinterested
6 and we can't convince them that it's worth doing something,
7 yes, some change will take place, but, boy, it's going to be
8 an uphill battle.

9 **MR. RICHARD FADDEN:** Mr. Jones.

10 **MR. ALAN JONES:** Thank you. If I could
11 follow on to what Dick and Daniel have said, I think there's
12 multiple layers to how you respond to foreign interference or
13 any other national security inquiry. Absolutely, if a Prime
14 Minister is marginally interested or not interested, it has
15 an effect. Or if a Prime Minister is really interested, it
16 has an effect.

17 But in -- and when I raised the issue of --
18 and I, you know, colloquially use the term National Security
19 Council, but some more permanent structure than we have, one
20 of the purposes of permanent structures is to even out those
21 waves, is so that the government, the operational arm of the
22 government, always remains capable of doing something,
23 regardless of whether the Prime Minister is super interested
24 or even marginally interested. And there is work that has to
25 be done every day because there is legislation.

26 I'll give a very quick example of the
27 question of variation of the Prime Minister as being
28 interested or not interested. I'm not going to say which

1 Prime Minister it is or which National Security Advisor it
2 was, but I was at PCO, my phone rang, I was in my car. The
3 National Security Advisor said to me, "I'm with the Prime
4 Minister. The Prime Minister is reading something on the
5 front page of *The Globe and Mail*. He wants to know if
6 someone is dealing with this, or does he have to give the
7 order for somebody to deal with it?" I said, "You can
8 reassure him, he does not have to give an order. There are
9 officials in government who are dealing with this already.
10 It's what they do every day."

11 So, the more -- the more effective that the -
12 - those daily operations are, the better off we will be in
13 terms of the quality information that is eventually provided
14 to a Prime Minister, whether they want it or not sometimes.

15 And when we talk about the quality of
16 intelligence, as I've said before, the quality of
17 intelligence reports going up often depends on the quality of
18 the requirements and requests coming down.

19 When we say, "What is it that they're looking
20 for?" And if you don't know exactly what they're looking --
21 what your seniors are looking for, you tend to write very
22 broad documents trying to, at some point, hit the mark
23 somewhere along the line to see whether they're in or not.

24 The more sophisticated they are -- and the
25 Prime Minister job and senior jobs are enormously busy.
26 There's an awful lot going on. And so, you're not going to
27 get much of their time, because they're trying to deal with a
28 lot of things. But if they're supported by a more, I don't

1 want to say professional, because people work extremely hard
2 in these areas, but a more permanent structure which can
3 manage some of these requirements as to what intelligence is
4 expected out of government.

5 And Dick has raised this earlier about
6 organizations getting orders and being told, "Do this." And
7 very broad intelligence priorities become very broad
8 generalized annual work plans. Politicians, elected
9 officials, and often senior government officials, are caught
10 in somewhat of a contradictory position where they want to
11 know more, but they're afraid to give specific direction to
12 an intelligence service or police agency to do specific
13 things. They don't want to be perceived as directing that an
14 investigation be conducted against an individual or a group,
15 because that would make it a politically motivated
16 investigation.

17 But at the same time, they know that they're
18 supposed to know more about this issue and need to do
19 something about it at a policy level, and they would like to
20 have more information than they did.

21 ITAC was created as a result of a Prime
22 Minister at the time, Paul Martin I think, who said, "I'm
23 tired of getting five or six different threat assessments on
24 the same issue which don't say -- are not a singular
25 authoritative voice on the issue." And of course, those were
26 very tense times, but that happens every day.

27 So there is a requirement to have better
28 quality intelligence, but also better-quality requirements,

1 and all of that requires, as Dick said, taking this more
2 seriously at multiple levels.

3 **DR. LEAH WEST:** I wonder if Professor Carvin
4 or Dr. Morrow, if you could speak to this idea of a more
5 empowered NSIA and how that might facilitate some of that?

6 **DR. STEPHANIE CARVIN:** Thank you. Sorry,
7 yeah, so it's Professor Carvin, just for the transcript.
8 Just to be sure.

9 So yes, in answering that question, I just
10 also want to touch on what was just said. The research I did
11 with Professor Juneau on our book really confirms what Mr.
12 Fadden said in terms, when we interviewed them, they read
13 intelligence because they thought the Prime Minister was
14 reading the intelligence; right? There is this real trickle-
15 down effect in terms of the community. You read what your
16 boss is reading. And so, you know, if your boss is
17 interested in sunny ways and national security is dark and
18 stormy, there's a tension there in terms of that, and I don't
19 think we see this in other countries where I think even if,
20 you know, Donald Trump was said to be not interested in
21 intelligence, there was a lot of people around him, and a lot
22 of people in the U.S. community that still were reading those
23 products. I'm not sure that's true in the Canadian case.

24 **COMMISSIONER HOGUE:** Do you have any idea why
25 it's different?

26 **DR. STEPHANIE CARVIN:** Our community is much
27 smaller. Our political -- our politicians don't necessarily
28 have clearance. I think Cabinet generally -- until -- this

1 is where I'm really curious to see if the Committee plays a
2 role in educating more Cabinet Ministers about intelligence
3 and how it's used and how it's made and what those issues
4 are. This, I think, is going to be a real test, to see what
5 the pull of the -- we can push -- as, you know, Mr. Fadden
6 said, it's -- you can push spaghetti all you want, but we
7 need them to pull the noodles. If they're going -- this is a
8 terrible analogy, but, you know, we need our Cabinet
9 Ministers to do more pulling of products, and that's the key
10 test. And I think that's going to be one of the key metrics
11 of the National Security Council. Do we see more departments
12 and agencies pulling products that are related to their
13 mandate?

14 And I would agree that -- and then hopefully
15 that would trickle down into the intelligence requirements
16 process.

17 One of the key problems, and the NSICOP did a
18 brilliant review of the intelligence requirements process, I
19 think back in 2017/2018, and they showed that one of the key
20 challenges there is that with the intelligence requirements,
21 everything was, like, a number one priority. Like, if
22 everything is a priority, nothing is a priority. So
23 encouraging, you know, better understanding of how the
24 community works would, I think, help that as well. And that
25 is, I think, another area where the NSIA would come in in
26 helping to perhaps provide more guidance on those processes
27 around the intelligence requirements.

28 The other area where I think a more empowered

1 NSIA could play a better role in this is being a better
2 facilitator of communications.

3 One of the things that has really struck me
4 about what we've learned about foreign interference is how
5 CSIS and other intelligence agencies have been trying to
6 communicate this to the government. And you know, CSIS was
7 basically portraying foreign interference as this ever-
8 looming -- you know, we've all talked about this. It's this
9 giant threat requires an all-of-government response, all-of-
10 society response. It's in our politics. It's in our
11 schools. It's in our universities. It's everywhere, right,
12 the way we've been talking about it.

13 And I think the analogy I would use is CSIS
14 was kind of talking about foreign interference like it was
15 talking about climate change; right? It's everywhere. It's
16 affecting all aspects of our lives. It's very complex.
17 Requires a whole-of-society response. And the Prime
18 Minister's Office was looking for a tornado warning. They
19 were looking for actionable intelligence pieces from those
20 assessments, and that's not really what CSIS is good at.
21 They don't really do opportunity analysis. They don't do
22 options analysis. They don't really provide the guidance
23 then. They can present the threat, not necessarily what to
24 do about it. And this is where I think an empowered NSIA
25 with a secretariat, with -- better able to coordinate the
26 community as a whole, could provide a much better job of
27 taking the climate change and tweaking it and creating those
28 maybe not tornado warnings per se, but taking those very

1 specific things that could be done, and then presenting that
2 to government, because that I think is really the missing
3 piece.

4 Like, you can present -- you know, like, you
5 can be in the doom and gloom, you be in the dark and stormy,
6 but unless you're providing some kind of very specific
7 actionable things that the government can do, it's not going
8 to work. And I would like to think that that is where an
9 enhanced NSIA, whether its mandate is spelled out in law, or
10 perhaps a better just understanding -- I think I saw in one
11 of the documents someone referred to a mandate letter, could
12 actually work.

13 **DR. LEAH WEST:** Any of the former NSIAs want
14 to jump in on that?

15 **MR. DANIEL JEAN:** I spoke openly, I thought,
16 on that at the beginning of the thing. There was a tornado
17 that they saw. It was the U.S. election. That became --
18 it's not -- I prefer the word "shiny object". Politicians
19 are attracted to shiny objects.

20 So we warned them about what happened in
21 Montreal with what and how the Russians could mount this
22 information campaign. There's a so what for Canada. It
23 happened in Canada, there was some Canadians, but so what;
24 right?

25 Three months later, there's the U.S. election
26 interference. Interest? Tornado? Boom. Spike.

27 Okay. The challenge is there to say, "Yeah,
28 but we don't think --" and how many people have testified,

1 former NSIAs and things, we don't think elections is the
2 biggest threat in Canada. And so far your Phase 1 shows it's
3 probably not -- there's some local risks, political parties,
4 something that has come up.

5 So we work very hard in saying, "Yes, we need
6 to strengthen our elections, the cyber role, the CSE, the
7 creation of the Panel of Five," all of that is important, but
8 we think foreign interference is deeper than that. Like, so
9 that's how far I'm going to go into an open panel, but I
10 think the difference is not that the mandate wasn't there,
11 that the -- there was no action about that, I would agree
12 with you. Like, that's what CSIS was doing. At that time,
13 there was nothing that was most of it actionable.

14 But the issue is there was nothing shiny, and
15 then the U.S. election was shiny, and said, "Well, that must
16 be big." So they -- and we were successful in saying, "No,
17 it's not just going to be cyber. The briefing with political
18 parties should be, you know, by CSIS as well and the rest of
19 the threats."

20 But it goes back -- that's why in my remarks,
21 I say you've got to find a way to make sure that the
22 political class is engaged, it's not just attracted by the
23 shiny objects. But I've seen politics long enough to know
24 that they're not going to be attracted by things if they
25 don't feel their citizens who vote are attracted by things.

26 **DR. LEAH WEST:** I do want to -- but this ties
27 into something that you talked about before, and one of the
28 things that came up in the NSIRA report that looked at this

1 policy decision-making flow was that the policies and
2 processes developed in the wake of the 2016 election, so SITE
3 and the CEIPP, was meant to address foreign interference like
4 what we saw in the 2016 election, and it necessarily hasn't
5 adopted to foreign interference as it actually plays out in
6 Canada. And I'm wondering if you might want to speak to that
7 in response to Daniel Jean's point, but also thinking about
8 your recommendations for the Panel of Five?

9 **MR. RICHARD FADDEN:** Sure. I mean, you
10 asked, Commissioner, a few minutes ago, in response to what
11 Stephanie was saying about why Ministers aren't interested,
12 and Daniel gave an answer I don't disagree with, but in my
13 experience, they do not feel threatened. Unless they feel
14 threatened, they don't act.

15 And fundamentally, that reflects the way
16 Canadians feel. We have three oceans and the United States'
17 border. We don't feel threatened in the same way as the
18 Americans, as the Brits, and even as the Australians. And
19 yes, they will be attracted to shiny objects. I think you're
20 right. But what really captures their attention is a threat,
21 and there I go to agreeing with a number of my colleagues
22 here saying part of the responsibility for that is how that
23 threat is described and brought to their attention. And I
24 think Al is right when he says in the absence of clear
25 direction, the default is generalization. And my experience
26 anyway, Prime Ministers, in particular but Ministers,
27 generally, hate generalizations. They don't mind
28 generalizations when they're talking to the public, but when

1 they're being told about things, they want the specifics.
2 And there are instances where that's provided, there's no
3 doubt about it, but broadly speaking, most of the threat
4 assessments that have been produced certainly when I was
5 there, a couple that I've seen since then, they're too
6 general. And, you know, they've got better things to do, and
7 they just don't pay attention. And I would argue forcefully
8 that it's the issue of threats. And Daniel is right when he
9 says if the Canadian public does not feel threatened,
10 Ministers are not going to focus. And there, there is a
11 responsibility for the community to try and articulate these
12 threats, which is why initially, Commissioner, I suggested
13 that it would be helpful to you and your recommendations if
14 you can come down clearly and say there's a clear and present
15 danger. Pay attention to what I'm going to say in my
16 subsequent 600 pages or 30 pages. I don't know how long your
17 report will be.

18 **COMMISSIONER HOGUE:** Probably more than 30.

19 **MR. RICHARD FADDEN:** But less than 600? You
20 never know?

21 **COMMISSIONER HOGUE:** I don't know.

22 **MR. RICHARD FADDEN:** I've now forgotten what
23 you asked me to comment on. I'm sorry.

24 **DR. LEAH WEST:** So I will tell you, but I
25 guess I want to interject there and say, but Canadians do
26 feel threatened. They're probably just the ones that are the
27 most disconnected from the state, and I think how we bridge
28 that gap is an important thing that we've also brought up is

1 there are large subsets of Canadian population who do feel
2 threatened, but they're not the ones communicating with their
3 politicians, and how do we bridge -- fix that is also an
4 element of it. The other point I was asking you about was
5 the -- you know, the policy was designed to deal with one
6 particular threat to democratic institutions, which was what
7 we saw in 2016 election, but that's not what we're seeing as
8 the major threat to Canadian democratic institutions. So is
9 there a way of adjusting the policy, or does it need to be
10 revisioned, or you think it's sufficient as it is, given what
11 we now know is where we see foreign interference in Canadian
12 democratic processes. So I'll let you answer ---

13 **MR. RICHARD FADDEN:** I'll just ---

14 **DR. LEAH WEST:** --- and then ---

15 **MR. RICHARD FADDEN:** --- I'll do it very
16 shortly, but I think, absolutely, it has to be changed. Our
17 understanding of what's happening with foreign interference
18 is entirely different than what it was five, six, seven,
19 eight years ago. And to suggest that those initial efforts,
20 which are all in good faith and had some positive impact
21 would apply today, given the changes in the world generally
22 and what's happening in Canada, we're dreaming in
23 technicolour. So I think somebody has to take a very deep
24 breath and look at these things again, both the policies and
25 whatever structures we decide to put into place.

26 So I think -- I, in fact, as a Canadian,
27 never mind somebody who's putzed around in this area, I
28 really worry how we're going to deal with the next federal

1 election. I mean, so far, the government has talked in
2 generalities about how it's going to deal with the issue.
3 With great respect to the Commissioner's report, it may be
4 too late for them to implement any number of your
5 recommendations, even if they were inclined to.

6 But I agree with you, what was put into place
7 for the two elections that the Commissioner is particularly
8 charged with looking at, totally inadequate for today.
9 Totally inadequate.

10 **DR. LEAH WEST:** Mr. Jean?

11 **MR. DANIEL JEAN:** So I'm going to -- you
12 asked on that, I agree with some of that, I agree with your
13 question that it was created because they foresee what --
14 given what happened in the U.S., it would be kind of a
15 national approach to interfere, we'd look at what happened in
16 France and Germany, a lot of conversations with these folks.
17 But despite that, when you look at your proceedings, I've
18 been watching very carefully, some of the local level things,
19 they came up in the Task Force. So it's not like they were
20 not picked up.

21 We go back to the threshold, and then we also
22 go back on the panel position. I think that it's really
23 difficult -- we don't need to repeat what -- very difficult
24 to ask people even though they're non-partisan, we're serving
25 the executives to be making these kinds of decisions. You've
26 had Jim Judd and then Morris Rosenberg would reviewed the two
27 elections, all the material that they've had. I look at
28 Morris Rosenberg, he raised a question is the threshold too

1 high. Now the danger, of course, is the reason why the
2 threshold is high, and it relates to what you've said
3 earlier. You're going to make sure that going public is not
4 going to make it worse than not doing things; right? You
5 don't want to interfere in the election either; right?

6 So I think that definitely the Panel of Five
7 needs to be reviewed. The Task Force itself that they go and
8 have an understanding that it's bigger than what it was
9 created for. Yes, but in practice I would argue they were
10 already -- their job certainly, despite the fact this is not
11 what was expected from what I've seen in both in the
12 Rosenberg report, the Judd reports and some of your
13 proceedings. I mean, what you've found is some local things;
14 right?

15 **DR. LEAH WEST:** Last moment, I'll turn it
16 over to the Commissioner.

17 **COMMISSIONER HOGUE:** No, except for saying
18 thank you to everyone. Honestly, I think we'll be able to go
19 on for hours and hours and maybe for days and days, but even
20 what we have been able to cover this morning was very, very
21 useful. And I don't know how many pages will be the report,
22 but clearly, there's material for quite a lot. So thank you
23 very, very much for coming, for your time, for sharing your
24 experience, expertise, and I really, really appreciate it.
25 Thank you.

26 --- Upon recessing at 12:30 p.m.

27 --- Upon resuming at 1:34 p.m.

28 **COMMISSAIRE HOGUE:** [No interpretation].

1 This roundtable is entitled "Enforcing,
2 Deterring and Prosecuting FI Activities". And we have with
3 us four experts, and a fifth one is on the screen, so we have
4 five, actually, that we will hear from.

5 And it will be moderated again by Professor
6 Leah West.

7 **--- ROUNDTABLE: ENFORCING, DETERRING AND PROSECUTING FOREIGN**
8 **INTERFERENCE ACTIVITIES:**

9 **--- PANEL MODERATED BY DR. LEAH WEST:**

10 **DR. LEAH WEST:** Thank you, Commissioner.

11 [No interpretation] foreign interference can
12 have to do with these things in order to criminalize foreign
13 interference. There are few prosecution for foreign
14 interference.

15 During the Phase 1 in the spring, the
16 Commission heard testimony about some of the actors
17 responsible for investigating and prosecuting offences linked
18 to foreign interference, and some of the challenges that they
19 face. This evidence suggests that there are important
20 questions to ask about whether Canadian laws, procedures, and
21 enforcement agencies are designed and resourced to
22 effectively investigate, deter and prosecute foreign
23 interference activities.

24 This raises numerous questions raised under
25 this theme, but I'm going to begin by asking all of our
26 panellists a single question, and then I'll introduce those
27 panellists.

28 And the single question I have is, is the

1 criminal law and criminal law process a sufficient, necessary
2 and appropriate way of deterring, detecting and countering
3 foreign interference, and are there reasons why other
4 approaches should be preferable?

5 To answer this broad question, we're joined
6 first by Mr. Bob Paulson, the former Commissioner of the
7 Royal Canadian Mounted Police, Professor Robert Currie at
8 Dalhousie University, Professor Alex Wilner, an Associate
9 Professor at Carleton University, Professor Michael Nesbitt,
10 an Associate Professor at the University of Calgary, and
11 online we have Mr. Croft Michaelson, who's the former senior
12 counsel for the Public Prosecution Service of Canada.

13 So I'm going to ask my colleague, Mr. Wilner
14 -- or Professor Wilner, I should say, to start with his
15 remarks.

16 **--- PRESENTATION BY DR. ALEX WILNER:**

17 **DR. ALEX WILNER:** Thank you.

18 Dear Commissioner, distinguished guests,
19 fellow panellists and colleagues, there are three distinct
20 topics before us today, enforcement, prosecution and
21 deterrence, and I will focus my time on the last of these
22 three processes, deterring foreign interference.

23 Much of my scholarly research over the past
24 20 years has explored the ways in which classical deterrence
25 theory, as first developed by political scientists during the
26 Cold War, might be reimagined and reapplied against a range
27 of contemporary security challenges, and so I illustrate how
28 states might deter violent radicalization, transnational

1 terrorism and insurgency.

2 I also assess deterrence in cyberspace and
3 within the constructs of information warfare, and I explore
4 how artificial intelligence might both undermine and augment
5 military deterrence. And more recently, with a former PhD
6 student of mine, Dr. Marshall Palmer, I've proposed a more
7 expansive deterrence framework for application against
8 foreign election interference.

9 And so today I'd like to share my high-level
10 thoughts on two aspects of deterring foreign interference.
11 First, I will define the nature of and describe the
12 prerequisites for deterrence in countering foreign
13 interference. And second, I would like to illustrate the
14 various pathways in which deterrence by punishment, denial
15 and delegitimization might be applied against foreign
16 interference.

17 Though I am not a legal scholar, my comments,
18 I think, dovetail nicely with those of my fellow panellists
19 in that I describe the larger legal, domestic, geopolitical
20 and security contexts in which deterrence theory and practice
21 can be applied to counter foreign interference in this
22 country.

23 At its conceptual core, deterrence is
24 fundamentally about using a combination of threats to shape
25 an adversary's behaviour in a way that meets our own
26 objectives. It entails convincing another actor, who remains
27 able to behave in ways that are detrimental to us, to
28 willingly forego an action that we would rather they not

1 pursue.

2 There are two guiding principles in forming
3 my understanding of deterrence theory. First, deterrence is
4 not simply something that you say or casually lump together
5 with other related terms like defence or enforcement or
6 defeat. Rather, deterrence is a framework or a strategy, and
7 it's built on an understanding about the nature of behaviour
8 that can be applied to any context in which we seek to shape
9 or change another actor's behaviour.

10 And second, if deterrence is defined as
11 convincing an adversary to forego an unwanted action, then in
12 practice, deterrence rarely just happens on its own. Rather,
13 deterrence is something that you do and that you communicate
14 proactively.

15 Deterrence is the result of putting into
16 practice a strategy that seeks to manipulate, to shift or
17 alter an adversary's behaviour in ways that meet our own core
18 objectives.

19 So I would like to encourage, first, that
20 members of the Commission use the term diligently and
21 consistently to refer to a larger framework in which Canada
22 leverages a combination of threats and defences in a way that
23 convinces foreign actors who means us harm to pursue -- not
24 to pursue foreign interference and related activities.

25 Now, there are several prerequisites
26 informing the strength and utility of any deterrence
27 framework. The first, deterrence involves at least two
28 actors. The first actor is known as the challenger, who

1 contemplates a particular course of action. And the second
2 actor is known as the defender, who seeks to deter that
3 unwanted action. Another way to think about these relations
4 is that a challenger wants to change a status quo
5 relationship while a defender seeks to uphold it. And so in
6 our particular case, Canada is the defender and foreign
7 actors contemplating interference are the challengers.

8 Second, a deterrence framework should seek to
9 weigh on a challenger's cost-benefit analysis. Rational
10 behaviour is predicated on the costs or effort an action is
11 assumed to entail against the benefits or gains the action is
12 assumed to generate. When a rational actor believes that the
13 benefits -- sorry, that the cost of its actions outweigh the
14 perceived benefits, deterrence theory speculates that it
15 should forego a ---

16 **MS. LEILA GHAAHARY:** Excuse me ---

17 **DR. ALEX WILNER:** --- particular action ---

18 **MS. LEILA GHAAHARY:** --- Mr. Wilner, could I
19 ask you to slow down ---

20 **DR. ALEX WILNER:** I'm sorry, yes.

21 **MS. LEILA GHAAHARY:** --- for the
22 interpreters, please. Thank you.

23 **DR. ALEX WILNER:** As a prerequisite to
24 deterrence, our challengers must be sufficiently swayed by
25 rational choice.

26 A third prerequisite, defenders must clearly
27 communicate threats, readiness and expectations to
28 challengers, such that adversaries absorb relevant

1 information, they consider how to respond, and then they
2 inform or change their behaviour. Communication is critical
3 to deterrence. A threat that is unmade or a warning that
4 isn't heard or properly understood will fail to generate the
5 desired coercive effect on our adversaries.

6 A fourth prerequisite, defenders must have a
7 perceived capability to act as they have threatened and to
8 demonstrate a resolve to act as threatened if and when
9 required. Bluffing undermines deterrence. A challenger must
10 believe that a defender can and will act as it has
11 communicated.

12 And finally, deterrence works best against a
13 known adversary. Anonymity in either physical or digital
14 space complicates how deterrence is communicated and carried
15 out. Attribution is an important consideration when
16 identifying our challengers.

17 So let me turn next and conclude by putting
18 all of these definitions, concepts and prerequisites together
19 within the context of deterring foreign interference in
20 Canada.

21 Three deterrence pathways present themselves:
22 punishment, denial and delegitimization. Deterrence by
23 punishment promises some form of retaliation if a challenger
24 pursues an unwanted action. Punishment adds to an
25 adversary's costs, potentially tipping the scales of a cost-
26 benefit calculation towards inaction. Deterrence by denial,
27 conversely, functions by subtracting from or diminishing an
28 adversary's perceived benefits. Here our goal is to deny a

1 challenger what it seeks from a cost-benefit perspective.
2 Denial creates a cost by promising failure. If an adversary
3 is convinced that the unwanted action in question is unlikely
4 to get them what they desire, they may be less willing to
5 try.

6 And then finally, deterrence by
7 delegitimization. This functions by informing and shaping an
8 adversary's beliefs, attitudes, ideologies and other
9 motivating factors. Delegitimization turns on social
10 pressure and perceptions of right and wrong. In this case,
11 challengers are deterred from pursuing a certain behaviour
12 when the behaviour itself generates a belief, or a perception
13 within the actor, or among its stakeholders that pursuing the
14 unwanted action would be shameful, disgraceful, or
15 detrimental to the larger objectives.

16 A Canadian deterrence framework for
17 countering foreign interference should combine elements of
18 all three processes. The framework would provide the
19 conceptual backbone for combining the disparate approaches to
20 counter interference under one guiding conceptual rubric of
21 deterrence. And moreover, this framework would tie the
22 various approaches and solutions that Canada and other
23 democracies are proposing and applying to countering foreign
24 interference within a larger overarching strategy.

25 Now importantly, that strategy itself could
26 be broken down and applied to different actors involved in
27 foreign interference, so state and non-state sponsors of
28 foreign interference and Canadians, foreign nationals and

1 domestic organizations involved in its promotion can be
2 punished. The effect that interference is meant to have on
3 Canadians, on our society, on our democratic processes can be
4 denied. And bolstering democratic norms, values, principles,
5 expectations and institutions, both at home, but also abroad
6 might delegitimize the acceptance or use of foreign
7 interference among a variety of stakeholders, from elected
8 officials to individual voters.

9 So let me conclude then with a scenario that
10 breathes life into the proposed deterrence framework. Heavy
11 and open investments in Canada, in Canada's ability to
12 successfully investigate, enforce and criminally prosecute
13 domestic and foreign individuals, organizations and corporate
14 entities promoting foreign interference in Canada would occur
15 under public and journalistic scrutiny. Concurrently,
16 Canadian officials working lockstep with our democratic
17 allies could issue a more nuanced and credible series of
18 threats to punish state sponsors of interference, including
19 by threatening sanctions and public exposure and, possibly,
20 at the very extreme end, by threatening military or cyber
21 retaliation for interference that is deemed a threat to
22 critical national infrastructure.

23 Elsewhere, applying a whole of society
24 approach to countering interference would deny its purpose
25 and diminish its utility. In this case, different levels of
26 government would work with the federal government to limit
27 and constrict the intended effects of foreign interference by
28 diminishing the scope and perhaps the reach of

1 disinformation, by encouraging or forcing private sector
2 partners to scrub disinformation from their platforms, and by
3 improving Canadian cyber security practices in ways that
4 diminish the theft of sensitive information that might be
5 repurposed to influence our elections and elected officials.
6 And by way of public and formal education campaigns, our
7 society's ability to identify and ultimately ignore
8 disinformation meant to interfere with our democratic
9 processes might be strengthened.

10 Finally, clearly and repeatedly discrediting
11 foreign interference domestically and internationally as a
12 disgraceful form of behaviour by championing democratic norms
13 and institutions might, among and within certain societies,
14 but also including our own, create social costs to
15 participating in foreign interference. If interference is
16 widely interpreted as shameful, would-be local politicians at
17 all levels of government may become less inclined to accept,
18 invite or welcome foreign interference on their behalf. And
19 doing so would be counter to what they believe is just and is
20 expected of them.

21 So, in sum, criminal law is a necessary but
22 not sufficient means of deterring foreign interference in
23 Canada. Deterrence entails a complex interaction between
24 different actors and processes that encourages a more nuanced
25 understanding of our adversary's cost-benefit calculations in
26 deciding whether, when and how to interfere in Canada.
27 Crucially, deterrence theory helps by identifying the tools,
28 the technology, the infrastructures, the processes needed to

manipulate and shape our adversary's calculus and preferences by weighing on and utilizing punishment, denial and delegitimization together. Thank you.

COMMISSIONER HOGUE: Thank you.

DR. LEAH WEST: Thank you, Professor Wilner.

Mr. Paulson?

--- PRESENTATION BY MR. BOB PAULSON:

MR. BOB PAULSON: Well, good afternoon, everyone, Commissioner. Thanks for the opportunity to participate in the Commission's important work. I'm of the view that a properly resourced, *Charter* compliant, professionally aggressive criminal investigation leading to a timely and successful prosecution is an essential component of Canada's so-called all of society approach to foreign interference. That said, I think we need to recognize that hostile state actors are unlikely to stop their activities because we successfully arrest and prosecute their proxies or confederates. In short, we're not going to arrest our way out of this. We must, however, demonstrate competency and timeliness in bringing the criminal justice system to bear against those who would give life and participate in this criminal interference.

Arrest, charges and ultimately convictions, I believe, crystalize in the mind of Canadians the true nature of the threat that we face and it's an opportunity to demonstrate what I think Canadians expect with some accountability for what they're hearing about.

There are a number of actors in this for

1 God's sake's do something about this area, and they're all
2 armed with a host of powers and authorities and enforcement
3 options. CSE, CSIS, RCMP, Global Affairs, Elections Canada,
4 the Commissioner of Elections, other government departments.
5 And now, a Commissioner of Foreign Interference and
6 Transparency.

7 There already exists a fair number of
8 criminal offences which the police could rely upon to bring
9 enforcement against some of these activities. Some of them
10 include extortion, breach of trust, corruption, and
11 particularly relevant perhaps to transnational repression is
12 the offence of intimidation and threatening.

13 Now it's bolstered by the provisions of C-70,
14 which include some relatively complex new offences, but
15 again, some additional authorities.

16 So here we are with a complex array of
17 security and intelligence agencies and enforcement bodies, a
18 complex array of authorities, and powers, and enforcement
19 options. And so what I say is need is some coherence in
20 decision-making around what to use when. And that's easier
21 said than done, I'm sure you've started to appreciate.

22 So let me talk about the decision to initiate
23 and pursue a criminal investigation, largely understood to be
24 the prerogative of the police, and mostly that's true.

25 You know, a solid belief or a threshold
26 belief, and a specific criminal act in my view, imparts a
27 duty on the police to act, to investigate, to bring charges,
28 or recommend charges, and support a prosecution.

1 But there's also the -- and so that seems to
2 alienate the police somehow from many of the discussions
3 around grand policy options in attacking this problem. But
4 what's available to the police and to the broader community
5 that I've described is this idea of police discretion.

6 So let me take you back to the earlier 2000s
7 when terrorism was as bad as it ever was and we were having
8 difficulty bringing successful prosecutions against those
9 that were identified as posing a threat to Canadians through
10 the intelligence system.

11 CSIS and the RCMP put their heads together
12 and were able to dovetail their efforts in the form of what
13 was called and what is called One Vision. I believe it's up
14 to 3.0 now. But it's a series of principles, and it's rather
15 significant in that before then, it turned on the sort of
16 relative enlightenment of the leaders of each agency, which
17 didn't happen very often. And so this structured governance
18 system permitted decision-makers in both organizations to
19 look at specific cases and to apply some principles in
20 coordinating their efforts. Things like a criminal justice
21 response is the desired response, is the preferred response
22 when there's a threat to public safety. Things like a
23 prescribed cadence of operational deconfliction meetings.
24 Things like adopting the principle that when a criminal
25 justice response is anticipated, the earlier the information
26 is transmitted to the police, the better. A series of things
27 all contemplated and deployed to try and get ahead of this
28 seemingly insurmountable intelligence-to-evidence obstacle.

1 And it's successful. I think we can point
2 objectively to many successes of that approach.

3 And I think a similar approach, building
4 perhaps on the seed of the SITE Task Force, but broader, to
5 include many of these agencies, with some specific governance
6 around interacting, around keeping political considerations
7 out of discussions, around strategies and options, given the
8 circumstances as they're presented in each individual case,
9 with a principle of acting versus spreading information.
10 Acting versus knowing. That's fundamentally the difference
11 between the intelligence world and the enforcement world.

12 When you get all these people together, there
13 could be discussions like recognizing that perhaps a criminal
14 investigation of transnational efforts to threaten people at
15 home are legitimate and likely to occur, and therefore a
16 criminal prosecution or a criminal investigation is probably
17 not the best way to proceed and there may be other options.
18 But there's got to be a way of preserving those decisions and
19 the rationale that goes into those decision-making exercise.

20 Lastly, I'll just talk -- and no discussion
21 of criminality would be complete without a discussion of
22 resources.

23 I had the opportunity years ago to speak at a
24 forum on something called the economics of policing. And I
25 was able to do a little bit of research in terms of public
26 spending per capita on health, on education, and on policing.
27 On the first two, there was essentially an X equals Y graph
28 that demonstrates the investment, public investment, in those

1 two areas. Whereas policing kind of horizontally crept
2 across the page.

3 Park that for a second, but juxtapose it
4 against the evolution of the *Charter*, and trying to conduct
5 *Charter*-compliant investigations imposes an enormous
6 logistical task on police agencies and requires a different
7 approach to project-based attacks on -- particularly on
8 people who don't want to be caught. Particularly on people
9 who anticipate a criminal justice response.

10 Federal policing, which is the area generally
11 that has conduct of this in the RCMP, is woefully
12 underfunded. And contrary to a lot of public discussion,
13 it's not because the RCMP is involved in contract policing,
14 because the contracts pay their own freight, essentially. A
15 contracting province or municipality pays for what they get.
16 It's an actual cost contract.

17 But federal policing has been engaged in an
18 enormous remit of responsibility in terms of
19 counterterrorism, national security, in terms of drugs and
20 organized crime, border enforcement, financial crime,
21 protective policing has come under pressure lately, and
22 international policing.

23 So to think that, you know, you're going to
24 get a highly competent investigative response that is going
25 to be able to position enforcement in a way that gives life
26 to some of the things I said, would require an enormous
27 investment in a regionalized approach to deploying these
28 teams of investigators and specialized support and

1 administrative support.

2 I mean, what used to be a two-to-three
3 paragraph justification for a search and seizure instrument
4 when I was a constable is now a two-to-300-page document.
5 The -- and God help the investigator that has a failure to
6 disclose relevant information in that ITO.

7 So it's a very high-risk enterprise.
8 Disclosure costs are through the roof.

9 So I would just add that, in close, on the
10 need to take this seriously, the need to recognize that
11 enforcement is a component of our response, but the need to
12 make sure that we have the capacity to deliver *Charter-*
13 compliant investigations.

14 Thank you.

15 **COMMISSIONER HOGUE:** Thank you.

16 **DR. LEAH WEST:** Thank you.

17 Mr. Michaelson?

18 **MR. CROFT MICHAELSON:** Thank you. Good
19 afternoon. Can you hear me?

20 **DR. LEAH WEST:** Yes, we can.

21 **--- PRESENTATION BY MR. CROFT MICHAELSON:**

22 **MR. CROFT MICHAELSON:** Okay. That's great.
23 Thank you very much for the invitation to participate on this
24 roundtable.

25 I was a federal prosecutor for almost 30
26 years, and senior general counsel with the Public Prosecution
27 Service of Canada and my remarks are rooted in my experience
28 as a prosecutor, in particular my experiences conducting

1 prosecutions raising sensitive national security issues.

2 In my view, the criminal law has an important
3 role to play in signalling to foreign states and their agents
4 the types of conduct that we consider unacceptable, but I
5 would caution against relying on the criminal law to do much
6 of the heavy lifting in combating foreign interference.

7 Other measures outside of the criminal law,
8 such as administrative proceedings under the *Foreign*
9 *Influence, Transparency, and Accountability Act*, sanctions,
10 enhanced governance and oversight of vulnerable processes may
11 well be more effective than criminal proceedings in deterring
12 foreign interference.

13 I see three challenges with using criminal
14 law to combat foreign interference.

15 The first is the challenge of defining
16 foreign interference offences with sufficient precision to
17 survive scrutiny under the *Charter*. The second is the high
18 bar required to obtain a conviction at a criminal trial. And
19 the third is what is commonly referred to as the
20 intelligence-to-evidence problem, the difficulties that arise
21 when one seeks to use intelligence information in the context
22 of criminal investigations and prosecutions.

23 Turning to the first challenge, the challenge
24 in defining criminal conduct with sufficient precision. Both
25 you, the Commissioner, and the National Security and
26 Intelligence Committee of Parliamentarians have noted the
27 difficulty in drawing a line between foreign influence that
28 is considered legitimate and foreign interference that is

1 unacceptable, and you both observed that there is a
2 considerable grey zone.

3 The point I wish to make here is that the
4 criminal law itself is not a particularly good tool to try to
5 address ambiguity or conduct that may fall into a grey zone.
6 Criminal offence provisions are subject to scrutiny under the
7 *Charter of Rights and Freedoms* for overbreadth, and the
8 Supreme Court of Canada has stated that if a criminal offence
9 provision is so broad in scope that it includes conduct
10 bearing no relation to the law's purpose, that provision will
11 be overbroad and violates section 7. This places a restraint
12 on the use of the criminal law. Laws that are broadly drawn
13 to make enforcement more practical will run afoul of section
14 7 if they deprive even one person of their liberty in a way
15 that does not serve the law's purpose.

16 Now, the new foreign interference offences in
17 the *Foreign Interference and Security of Information Act*
18 appears to have been crafted with this principle in mind, and
19 they seem to capture much conduct that is considered foreign
20 interference, but could one go further and craft a broader
21 offence or offences that would capture all of the potential
22 permutations of foreign interference? I'm not sure that one
23 could do so without running into serious concerns of
24 overbreadth.

25 Turning to the second challenge associated
26 with using the criminal law, the legal standard to prove a
27 criminal case is high. The Crown is required to prove all of
28 the elements of the offence beyond a reasonable doubt, a

1 standard considerably higher than the civil standard of proof
2 on the balance of probabilities.

3 I note that the new foreign interference
4 offences all require that the Crown prove a link between the
5 offender and a foreign entity. The Crown must typically
6 prove beyond a reasonable doubt that the offender engaged in
7 certain conduct at the direction of, in association with, or
8 for the benefit of a foreign offender.

9 Practically speaking, I think that this
10 particular element will be the most challenging for the
11 police to investigate and for the Crown to prove in a
12 criminal trial proceeding. Given that we are talking about
13 conduct by foreign entities and their agents that is designed
14 to be concealed and obscured, you can anticipate that it will
15 be quite difficult for the police to gather sufficient
16 evidence to prove the link with the foreign entity beyond a
17 reasonable doubt. The high bar to prove a criminal
18 conviction lessens the utility of the criminal law as a tool
19 in deterring foreign interference.

20 I'll turn now to the third challenge, often
21 referred to as the intelligence-to-evidence problem, which
22 relates that the difficulties one encounters when one seeks
23 to bring intelligence information obtained through covert
24 means into a criminal trial process that is open and
25 transparent.

26 I think it likely that future investigations
27 of the new foreign interference offences will have their
28 genesis in intelligence information that is shared by CSIS

1 with the police. This is because one of the essential
2 elements of the offence, that necessary link between the
3 offender and the foreign entity, will probably first surface
4 in the context of an intelligence investigation. In my
5 experience, the intelligence investigation gathered by CSIS
6 that is likely to have particular value to a police
7 investigation is likely to consist of information from either
8 confidential human sources or intercepted communications, and
9 there are difficulties associated with relying on both types
10 of intelligence.

11 If the intelligence information is from a
12 confidential human source, that will pose a difficulty
13 because both the human source and the Service would need to
14 agree to waive the confidentiality that ordinarily protects
15 the identity of the human source under the *CSIS Act*. That is
16 a not to say a waiver of confidentiality is out of the
17 question. In the Toronto 18 terrorism case, two confidential
18 CSIS sources agreed to become police agents and testify at
19 trial. But human sources in this particular context may be
20 reluctant to disclose their identities if they have concerns
21 about possible retaliation by the foreign entity against
22 themselves or their loved ones.

23 If the intelligence information provided to
24 the police is a communication intercepted under a CSIS
25 warrant, and the police then rely on that communication as
26 part of the reasonable grounds to obtain their own warrant or
27 authorization to intercept communications, the CSIS warrant
28 and underlying affidavit may well become the subject of

1 scrutiny at trial.

2 The trial court may well need to review the
3 CSIS warrant and affidavit to determine whether the seizure
4 of the communication by the Service was lawful. That's an
5 important consideration any time the product of a CSIS
6 warrant issued by the police is whether that warrant and
7 affidavit could be disclosed to the defence in a manner
8 sufficient to allow for effective review and challenge at
9 trial without compromising national security.

10 In some cases it will be possible to balance
11 these two competing interests. A good example of this is a
12 terrorism case that I prosecuted, *Regina versus Jaser*, where
13 we were able to provide the defence with redacted copies of
14 the CSIS warrant and underlying affidavit, as well as
15 summaries of redacted information in a manner that was
16 sufficient to allow for effective review and challenge at
17 trial. And in that case, the trial judge was able to
18 conclude that the CSIS warrant was lawful, but there may well
19 be other cases where it will not be possible to disclose the
20 warrant and affidavit in an redacted form that is sufficient.
21 And if that is the case, the information gathered under the
22 warrant could not be used by the police.

23 I should add that in *Regina versus Jaser*, the
24 Service provided redacted copies of the warrant and
25 affidavit, and some summaries of redacted information in
26 consultation with both the prosecutor, myself, and the trial
27 judge, but without the involvement of the Federal Court. In
28 that case, the defence was content with what the Service

1 produced. But in other cases, the defence might well resort
2 to the section 38 disclosure regime in the *Canada Evidence*
3 *Act*, and pursue an application in the Federal Court for
4 disclosure.

5 In my view, the section 38 disclosure regime
6 is both cumbersome and time-consuming. If the defence had
7 resorted to that process in *Regina versus Jaser*, it would
8 have resulted in the bifurcation of the proceedings and
9 likely contributed to considerable delay of the trial.

10 In summary, Commissioner, the foregoing
11 challenges associated with the criminal law, in my view,
12 limit its utility in combatting foreign interference, and
13 other measures that don't have these same challenges may well
14 be more effective.

15 Thank you.

16 COMMISSIONER HOGUE: Thank you.

17 DR. LEAH WEST: Professor Nesbitt.

18 **--- PRESENTATION BY DR. MICHAEL NESBITT:**

19 DR. MICHAEL NESBITT: Thank you, and thank
20 you for the opportunity to be here, to the Commissioner and
21 everyone involved.

22 In some ways I'm going to skip the beginning
23 of what I had to say and echo the comments of Mr. Paulson,
24 Mr. Michaelson, and Mr. Wilner, and just say that criminal
25 law is an absolutely necessary but clearly insufficient tool
26 in the toolkit to combat foreign interference. Obviously,
27 it's important that Canada is not seen as a safe haven where
28 this sort of activity can take place. On the other hand,

1 criminal law, when applied, will only be applied to a small
2 handful of cases at any given time, and within that, a small
3 handful of the types of activities and the manifestations
4 that might result from foreign interference. So in other
5 words, a small subset of a small subset of the larger foreign
6 interference pie.

7 So what I'd like to focus on, instead of the
8 criminal law as we often think about it, which is the
9 offences, I'd like to talk about criminal process, procedure,
10 and structures. I think that is -- and haven't come up with
11 a better word for it, but this is a little unfair, but I'm
12 going to say where Canada has tended to fall down, when it
13 has fallen down, tends to be on the enforcement side of
14 existing laws, not the absence of laws in this area, and
15 particularly after Bill C-70 and some of the recent new laws
16 we have in this area, I think we have more than enough in
17 general on the criminal law side on the books in our *Criminal*
18 *Code* and security so, yeah.

19 What I think then is Canada needs to focus on
20 the effect of investigation of criminal laws, as you've
21 heard, and that is to say bringing them to charge and then to
22 a successful, fair and, as Mr. Paulson said, *Charter*
23 compliant result. But I also think this means thinking a
24 whole lot bigger than tinkering. That doesn't mean tinkering
25 with offences. It doesn't mean tinkering with bureaucratic
26 processes that are already in place. It doesn't mean
27 tinkering to get us to a One Vision 4.0. All of that may be
28 necessary, but again, it is insufficient, and at this point,

it probably amounts to tinkering around the margins.

So I'm going to focus on two institutions in particular and one subject area that require a good deal of work and a good deal of big thinking, the first being the RCMP, the second being CSIS, and the third, this is subject matter area and I'll call it money crimes, broadly speaking. In each case, I'm going to focus not on the offences or the particular mandate that they have, but rather, on the big picture, so the institutions, the processes and the resourcing that will drive the investigations.

Okay. First the RCMP. As I know this Commission has now heard, Canada's RCMP is bifurcated, a term, by the way, that very much defines this area of law. It is bifurcated between national security policing and contract policing. That bifurcation happens the moment someone walks in the door to be trained, continues through promotion, and then on to the skills that are developed and maintained when the investigations take place.

I'm happy to answer questions here. I'm not going to get into it in detail, so for now, I'll simply add my name to what I think is a chorus of academics who have studied this and perhaps what the Commission has already heard, and that being that much of the RCMP's contrasting [sic] policing agreements expire on or around 2032. And it is time to start planning for the expiration of those contracts now and what it will mean to proceed thereafter with a true national police force.

The focus needs to be on structure and

1 resourcing here, where the money goes, why and what the
2 implications are. That includes how do you attract, train
3 and retain experts needed to do national security policing
4 correctly. So to put that in lay terms, how do you get a
5 forensic accountant away from KPMG that stays away from KPMG
6 when KPMG pays a whole lot more money. It is at this point
7 time to plan for something different with the RCMP.

8 Second CSIS. As you've already heard,
9 Canada's system of investigating national security matters
10 was bifurcated in 1984. It was bifurcated again between
11 those that collected intelligence but also some evidence,
12 that being CSIS, and those that collect evidence, of course,
13 but also, by the way, some intelligence, and that being the
14 RCMP. Before then, like perhaps the FBI, the RCMP collected
15 both. Now there were good reasons in 1984 to suggest a
16 separate intelligence agency, and I won't get into that
17 history. Nor am I saying there isn't good reason to have
18 both CSIS and the RCMP. What I am saying is that while the
19 day-to-day relationship between those two organizations has
20 been discussed time and time again and put into practice
21 through One Vision 1.0, and then 2.0, and that was imperfect,
22 and then 3.0 and that was imperfect, and within the next 5
23 years 4.0 and that's imperfect. What hasn't been discussed
24 is the broader structural relationship between these two
25 organizations and what exactly they're doing in this space.

26 So again, to give one example, we have CSIS
27 and the RCMP investigating a terrorism matter. At some
28 point, the RCMP will take over and start investigating to

1 charge. The question then becomes at court one about sharing
2 information, about whether they have stepped on each other's
3 toes in the process, the question that isn't being asked is,
4 why is CSIS still there? And there's good reasons for them
5 to still there; right? It's hard to pass this back and
6 forth; right? Maybe they want to keep an eye on things
7 beyond the police investigation. Maybe they're looking at
8 other factors in the investigation. There's also good
9 reasons for them not to be there. We're already paying
10 another organization to do this work, to lead to what the
11 goal is, which is prosecution, and that other organization
12 may be actually hampered by the disclosure regime that will
13 invariably result when you have multiple national security
14 organizations involved in that process. So it's time to
15 think about some of those broader structural relationships
16 between these organizations.

17 And I'm going to quote something which I
18 think is -- which I think has been improved but I think it's
19 important and this comes from a Toronto 18 or so-called
20 Toronto 18 terrorism trial from 2009 and that's *Ahmad*, and
21 this is a quote.

22 "CSIS was aware of the location of
23 the terrorist training camp. This
24 information was not provided to the
25 RCMP who had an undercover -- who had
26 to uncover that information by their
27 own means. Sometimes CSIS was aware
28 that the RCMP were following the

1 wrong person, or that they had
2 surveillance on a house when the
3 target of the surveillance was not
4 inside, but CSIS did not intervene."
5 (As read)

6 It's time to start looking about -- looking
7 at why that happens, how that information is shared at a
8 broader level.

9 Another area to consider is one you've again
10 heard about, which is the intelligence-to-evidence conundrum,
11 and Canada, again, with our bifurcated court system between
12 the Federal Court and terrorism, or these sort of cases, the
13 Superior Courts.

14 This was first addressed in 2010 in the Air
15 India Inquiry, which essentially recommended an end to the
16 bifurcated system. As far as I know, every consultation we
17 have on this, which recently is every few years, have come
18 back with another suggestions which -- a number of
19 suggestions which are often taken up. And the one suggestion
20 that isn't taken up, for whatever reason, continues to be the
21 study of the bifurcated system. And I will say it's my own
22 sense that the recommendation with respect to the bifurcated
23 system from virtually anyone who studies it outside of the
24 institutions, right, so those who see the processes, those
25 who are not in Ottawa -- let Mr. Michaelson speak to
26 prosecutors who may be in the region and see this in a
27 particular way, but it's that it doesn't make any sense.

28 If -- to be clear about this, if Kafka were

1 writing today, Canada's bifurcated system in national
2 security matters would fit very well into the trial. He just
3 didn't manage to think of it. It's a hinderance, as Mr.
4 Michael said to speedy trials. It takes away from the
5 criminal process for what seems to me a largely uncertain
6 result.

7 One other thing I'll mention with respect to
8 CSIS, is there are some simple reforms, but again, they're
9 broader; right? So not a new criminal offence, but we should
10 be thinking about legislating O'Connor rules, so for third-
11 party disclosure with respect to national security
12 institutions or government institutions. So *O'Connor* was a
13 case that dealt with health information from the '90s, but
14 now it's being applied most often to information held by CSIS
15 as a third-party collector of intelligence with some overlap
16 to the RCMP. There are ways to legislate that could clarify
17 what those rules are and make it easier rather than fiddle
18 with processes of those trying to abide by current rules.

19 And I will just say, we have a couple of at
20 least academic papers on this which make a whole lot of
21 sense. One is by Craig Forcese and another is by Leah West,
22 and it's called "The Problem of 'Relevance': Intelligence to
23 Evidence Lessons from UK Terrorism Prosecutions" in the
24 Manitoba Law Journal 41(4) from 2018.

25 The final one I'll mention here is money.
26 And the money problem relates to CSIS and the RCMP, but we
27 also have to think about how it relates to the Public
28 Prosecution Service of Canada, Global Affairs, and others.

1 So in essence, do we have the right people with the right
2 skills and incentive hired in the right ways doing the right
3 work in the right places? And we have all sorts of evidence
4 to suggest we might have a problem here.

5 We have four sanctions prosecutions since
6 1991 in the history of Canadian sanctions law, and yet every
7 year we see Canadians prosecuted in the U.S. for violations
8 that look like they may violations in Canada, and we see
9 agencies from abroad saying Canada is a safe haven for this
10 sort of activity.

11 That's the same with terrorist financing. We
12 get criticized fairly regularly as Canada being a safe haven
13 for terrorism financing from a number of groups.

14 I'll give you one example. We've never had a
15 terrorist financing case with respect to money being sent to
16 Hezbollah. That's shocking if you know the Canadian system.

17 We have, I think, four charges out of the now
18 70 individuals charged, and we have multiple studies again
19 here, at least one I can think of, indicating that a number
20 of these cases could have gone ahead with terrorist financing
21 charges as well as what was charged, and it wasn't.

22 So again, the issue here comes back to the
23 broader question about resourcing of CSIS, of the RCMP, of
24 the right prosecutors. It comes back to questions as to why
25 the U.S. runs its sanctions, for example, out of the Treasury
26 Department and OFAC in particular, who are experts in
27 financing, and money, and spreadsheets, and all that sort of
28 stuff, and yet Canada continues to run it out of Foreign

1 Affairs, where diplomats move in their job every couple of
2 years and are not trained for any of this work.

3 But what comes from all of this to my mind is
4 a need to think big at this stage and make big
5 recommendations, not small tinkering. We need to think about
6 how the criminal law works. We need to think about the
7 structure of our national security organizations in relation
8 to existing laws. We need to think about how investigations
9 to prosecutions run through the system and how it's all
10 functioning together. We need to think about the resourcing,
11 but again that's not just the resourcing in terms of money,
12 that's also resourcing in terms of human resourcing, how you
13 do that, what the structure looks like of an organization so
14 that when money goes in, it doesn't get diverted two years
15 later to whatever the hot issue is that day.

16 Thank you.

17 **COMMISSIONER HOGUE:** Thank you.

18 **DR. LEAH WEST:** Small problems.

19 Professor Currie?

20 **--- PRESENTATION BY MR. ROB CURRIE:**

21 **MR. ROB CURRIE:** Thank you, Dr. West.

22 Commissioner, Colleagues, I'm honoured to be
23 asked to appear today.

24 You've heard a lot of wisdom from my
25 colleagues. I'm going to drill down on the foreign part of
26 foreign interference and confine my remarks to one basic
27 theme, which is this: if the criminal law is to be used to
28 fight foreign interference, and I agree with the general

1 tenor of my colleagues' remarks, that it is a tool in the
2 toolbox, then it should be done with an explicit textured
3 focus on the international aspects of this situation that we
4 find ourselves in.

5 That is to say, our criminal law should be
6 used with the international context in mind. It should be
7 used in a way that's fully infused by relevant international
8 law norms, and specifically Canada's rights and obligations
9 under international law.

10 The nature of the threat here means that
11 criminal law, as a tool, needs to be employed in such a way
12 that it is fully protective of Canada's national interests in
13 an international setting where they are increasingly
14 threatened. And I will use my few minutes to explain what I
15 mean by all of that.

16 My starting point is that international law
17 is relevant to criminal law and it's more relevant today than
18 ever. And I start there because after more than two decades
19 of trying to teach this material to various players in the
20 justice system, I can assure you that most police officers,
21 criminal lawyers, and judges in Canada have little to no
22 working knowledge of the concepts I'm about to explain,
23 present company excluded, of course.

24 Encouragingly, the Prime Minister recently
25 invoked Canada's sovereignty. Sovereignty is one of the
26 bedrock principles of international law. It captures the
27 idea that states like Canada are fully independent entities.
28 Even in a state like Canada which is enriched and influenced

1 by other cultures and diaspora communities, our government
2 and our legal system make the decisions.

3 Right alongside the principle of state
4 sovereignty is the principle of non-interference. Foreign
5 states are not permitted to interfere with Canada's domestic
6 interests, nor can Canada do likewise to them.

7 To do so is to breach a fundamental norm that
8 is designed to allow countries to live in a state of
9 relatively peaceful coexistence. This international law rule
10 in part is why this proceeding is called the Foreign
11 Interference Inquiry.

12 The Prime Minister also recently mentioned
13 Canada's territorial integrity. In international law, a
14 sovereign state has a defined territory with borders and
15 despite the verbiage one hears about the increasing
16 meaninglessness of territory and the so-called borderless
17 world, territory is not obsolete, and borders are not
18 obsolete; both matter.

19 On a country's territory, only the state can
20 act like the state. On Canada's territory, only the
21 government of Canada can make and invoke the force of the
22 law. This is particularly relevant to criminal law.
23 Criminal law has always been seen to be one of the areas of a
24 country's law that is closest to the heart of its
25 sovereignty, not just in Canada, but in all countries. And
26 it's often described as an expression of a country's
27 collective morality, but it has four other functions that I
28 want to briefly touch on. And I'll go lightly because my

1 colleagues have covered off some of it well. But they are
2 these four: a deterrent function; a protective function;
3 third, a communicative function; and fourth, an
4 accountability function.

5 On deterrence, a number of my colleagues have
6 spoken to this and I agree that the deterrent aspect of
7 criminal law is something we know about. And in this
8 setting, it should be engineered, and applied, and policed in
9 a way that it deters foreign actors from engaging in criminal
10 conduct on our soil. I agree with what I've heard here
11 today.

12 But the second function is the protective
13 one. Criminal law is a direct expression of the
14 international law of jurisdiction, specifically jurisdiction
15 to enforce the law. And the way that manifests as a power of
16 the state on the international plane, quite apart from what
17 it does related to what it does domestically.

18 Again, the basics. Only the Government of
19 Canada and delegate institutions can lawfully enforce
20 criminal law, which involves the use of coercive powers
21 against individuals. The state has a monopoly on the use of
22 coercive power and it has an obligation to protect everyone
23 on its territory. Not just citizens, but everybody, and
24 protect them from any attempt by a foreign sovereign to use
25 coercive power. A sovereign state that cannot do this is not
26 worthy of the name.

27 The third function is this. Canada's
28 criminal law should have a communicative function as well.

1 Specifically, a criminal law should be part of the
2 implementation of foreign policy, and I mean something
3 specific by foreign policy. I mean a harder-edged statecraft
4 that signals Canada's commitment to what is sometimes called
5 the rules-based international order. The way we use and
6 enforce our criminal law on our territory before our courts
7 communicates Canada's demand that international law be
8 respected, that an international system of sovereign equals
9 who refrain from interfering with each other is sound policy
10 to which Canada is committed.

11 The final way in which Canada should use
12 criminal law is as an accountability mechanism. And I mean
13 something a little different than what Mr. Paulson meant,
14 though I agree with his remarks.

15 Contrary to popular belief, international law
16 is enforceable by various means that exist along the spectrum
17 from informal to formal.

18 States do take each other to court, to
19 international courts even. Canada itself is currently party
20 to proceedings against several foreign states at the
21 International Court of Justice.

22 To be sure, criminal law is not directly part
23 of those kinds of proceedings, which operate at the state-to-
24 state level, but my point is that the way in which we create,
25 administer, and enforce our criminal law should be done with
26 an awareness that it might eventually end up as part of an
27 international case. It should communicate that there's not
28 only the prospect of local criminal accountability for

1 individual actors, but also the prospect of international
2 accountability for foreign states that emerge as bad actors.

3 The prosecutorial charging decisions that are
4 made, the selection of evidence that is gathered, the
5 decisions to go to trial, the sentences that are imposed, all
6 of this should operate in appropriate cases with the
7 international context in mind, and the justice system and its
8 players need to have the knowledge and the toolboxes
9 necessary to factor this in in the right cases.

10 On that point, I'll conclude with a few
11 practical observations and proposals.

12 Because the context of the criminal acts
13 we're discussing here is so internationalized, it's important
14 that Canada maximise the use of the powers and the tools that
15 are at its disposal, and these tools can involve
16 international law, and in fact international law can make
17 them even more effective.

18 Here is one way. Police and Crown
19 prosecutors must become comfortable with the use of extended
20 territorial jurisdiction, which means charging and
21 prosecuting people for criminal acts that don't take place
22 entirely within Canada, or even maybe at their heart outside
23 of it, but which have impacts on Canadian territory, and
24 specifically that impact the lives of people in Canada.

25 We need more comfort with extraterritorial
26 jurisdiction, which is where we would be willing to prosecute
27 offences that take place wholly outside Canada, but are
28 linked to Canadian interests, very internationalized

1 interests.

2 Now, I say this not because you couldn't pick
3 up a text book and find it, because you can, but historically
4 there has been a reticence by Parliament in its lawmaking,
5 and the Crown in its law enforcing to fully engage on cases
6 that have international aspects. It's cultural and it's
7 unnecessary because international law is actually quite
8 permissive on these points. States are very free to take
9 jurisdiction over cases that affect their national interests,
10 even when those cases have transnational features.

11 Now, I do want to offer there's good news in
12 Bill C-70 and the changes that have been made. There is some
13 use of extraterritorial jurisdiction in there. Not as much
14 as is available, I think, but there is some. In any event,
15 everyone needs to understand it, both how it works and the
16 potential that it might cause upset that there are
17 international implications to how we manage this as well.

18 Of course, this is best done in active
19 collaboration with other states, which brings me to a second
20 point. Our Departments of Justice and Global Affairs, as
21 well as the RCMP's international cooperation bureaus, are the
22 contact points for our law enforcement partners in other
23 countries. They do good work. They facilitate Canada's
24 collaboration with a wide variety of foreign partners well
25 outside the Five Eyes. Canada has an extensive network of
26 criminal cooperation. But this network of cooperation
27 between countries needs to trickle down more into the local
28 law enforcement context more than it does currently.

1 Anecdotally, police and prosecutors the
2 country over will often quickly abandon cases that have
3 transnational aspects because they are viewed as being too
4 time consuming and administratively unwieldy.

5 In my home province of Nova Scotia, we've --
6 over 15 years, we've had a series of cases of foreign states
7 interfering in our criminal justice system, and what attempts
8 were made to deal with it were so far not successful, either
9 because of local unwillingness to engage with the
10 international aspects, or federal unwillingness to help when
11 they did.

12 Moreover, a lot of law enforcement personnel
13 are not necessarily aware of what international cooperation
14 networks are or how they can access them.

15 Cooperation even with our partner countries
16 can be bumpy and not all of that is easily fixed, but what we
17 can do is ensure that there is more effective circulation and
18 communication of information that makes policing and
19 prosecuting of transnational cases more informed and more
20 effective.

21 And on the policing side, it's important that
22 this does not begin and end with the RCMP. Policing of
23 matters with transnational aspects will often ultimately fall
24 into federal policing, but it's the front-line provincial and
25 municipal police who will frequently encounter these cases
26 first.

27 Particularly when interacting with diaspora
28 communities, especially those known to be targeted by foreign

1 states, police need to be able to be equipped to go into the
2 situation with an expectation that any criminal cases that
3 emerge will have transnational aspects, and therefore that
4 they will need to have knowledge, and skills, and access to
5 networks that are unconventional to their normal day-to-day,
6 but that will enable more success.

7 It's worth noting that there are encouraging
8 success stories in this regard, even just lately in the
9 media, like the RCMP's recent investigation revealed into
10 alleged activities by personnel and agents of a foreign
11 government.

12 What is needed, Commissioner, to conclude, is
13 a country-wide effort to enable police and prosecutors,
14 particularly in communities targeted by foreign interference,
15 to have the knowledge base and operational toolboxes to
16 ensure that Canada's criminal law can serve important
17 international objectives and more robustly protect Canadian
18 sovereignty.

19 Thank you.

20 **COMMISSIONER HOGUE:** Thank you.

21 **--- OPEN DISCUSSION:**

22 **DR. LEAH WEST:** So now I'm going to ask some
23 thematic questions of the panellists until we take the break.

24 I'll start by directing my questions to
25 individuals, and then ask for people to jump in as they see
26 fit.

27 And Professor Wilner, I'm going to put you a
28 bit on the spot, because we hadn't talked about this one, but

1 I'm going to ask you to assess your theory of deterrence and
2 your three criteria, and based on what you've heard, whether
3 or not you think our adversaries are deterred by Canada, and
4 why or why not?

5 DR. ALEX WILNER: They are not. And perhaps
6 not yet. What I'm fascinated by is the aspect of using
7 criminal law filtered through international law to signal
8 capabilities, intent, relationships. That's fascinating. I
9 think that's a useful way of putting the F back into foreign
10 interference. And so this is weaving the domestic space into
11 the international space.

12 I also would suggest that criminal law, or
13 law broadly, does signal normative red lines that we've
14 established, that we agreed upon that we will protect. That
15 sends a message again that we have our eyes open, at the very
16 least.

17 I appreciate Michael's point about a lack of
18 seeing through this; right? Seeing the end of it. Criminal
19 prosecutions. And this goes back to the terrorism issues
20 that we're faced with.

21 I think that sends the wrong message as well;
22 right? We have the laws, but we don't have the means to
23 pursue to the end, and so that may signal weakness.

24 And so I -- you know, I'm grappling with all
25 these issues. But I do think -- I think that we're perhaps
26 on the right trajectory towards adding new tools to the
27 toolkit that provides a fulsome approach to deterring and
28 countering foreign interference.

1 **DR. LEAH WEST:** Thank you. One of those new
2 tools in the toolkit is the Foreign Transparency Registry
3 that has not yet been put into full effect or practice.

4 But I'm wondering if, Mr. Michaelson, you can
5 think to its capacity to deter, in terms of do you think it's
6 going to be a good tool and are there ways of actually
7 enforcing it? Do you see it actually being enforceable?

8 And then I would just ask, Alex, if you think
9 that this kind of transparency mechanism does actually add to
10 its deterrent effect?

11 **MR. CROFT MICHAELSON:** Well thank you. So
12 with respect to the Foreign Transparency Register, it sheds a
13 light on activity, right, that currently is hidden. And when
14 we look at the experience in other countries, I mean, the
15 United States has had a Foreign Influence Registry for many,
16 many years. I think it goes back to the 1930s. You know,
17 their experience with it, until recent years, was that they
18 tended to sort of pursue voluntary compliance efforts, rather
19 than prosecutions.

20 I think part of the issue they had was that
21 they didn't have the power to compel documents and our
22 Foreign Transparency Register, the Commissioner will have the
23 ability to compel productions and documents.

24 Certainly our partners in the U.K. and
25 Australia have thought that this is a useful approach as
26 well.

27 So, you know, at the end of the day, we'll
28 see where it goes, but I think in terms of when you talk

1 about conduct, like, parliamentarians in particular, you
2 know, engaging in activity with foreign actors maybe they
3 shouldn't be engaged with. That will come to light. And I
4 think if those kinds of connections come to light, it will
5 have a deterrent effect, because people, I think, will be
6 less likely to engage in that kind of behaviour if it's going
7 to be public notice and quite open, published on a public
8 registry. So that's -- we'll have to wait and see how it
9 goes at the end of the day, but the ability of the
10 Commissioner to compel the production of documents, the
11 ability of the Commissioner to rely on information that is
12 not admissible as evidence in court proceedings, you know, it
13 seems like a good approach and a good first step, for sure.

14 **DR. ALEX WILNER:** I'm in general agreement.
15 I think the transparency registry does illustrate capability,
16 intent, resolve. I think the proof of use and the concept
17 itself would be to cross point a good marker for whether or
18 not it deters, but I think one issue, perhaps, that it -- or
19 one additional element is that it denies an easy route for
20 those willing to pursue foreign interference, an avenue to do
21 so.

22 And so going back to the concept of
23 deterrence by denial, we're not just looking to punish.
24 We're looking to deny easy access to do the bad things that
25 they want to do.

26 And so it's possible that this will do that.
27 Time will tell.

28 **DR. LEAH WEST:** One thing we heard in a panel

1 earlier this morning was the suggestion that even where
2 prosecutions may never happen because the individual is no
3 longer in the country, right, or we're talking about a
4 foreign agent that is abroad, there's a useful signalling
5 mechanism and a useful public education mechanism of bringing
6 charges for foreign interference even if there's no
7 reasonable prospect of conviction, which is generally the
8 threshold prosecutors use for bringing charges.

9 I'm just wondering if anyone has thoughts
10 about that, and I'll start with Mr. Paulson.

11 **MR. BOB PAULSON:** So I was fascinated by my
12 colleague's presentation on extra-territoriality, which is
13 something that we've availed ourselves of in the past. And
14 to your question, we charged a fellow by the name of Mokhtar
15 Belmokhtar in relation the kidnapping of Louis Guay and Rob
16 Fowler knowing fairly well and confident that we weren't
17 going to go and collect him from the Sahel and bring him back
18 to prosecution. And ultimately, I'm told -- I think we
19 learned that he's dead.

20 But to that very point, there is some benefit
21 in demonstrating the competency of the investigative
22 enforcement arm by bringing charges, and we've done it in
23 other cases successfully, bringing back one of the kidnappers
24 through an undercover ruse in the Lindo case, kidnapping
25 case.

26 So there is ample opportunity to bring -- and
27 Americans do it frequently, announcing charges against
28 Russian cyber attacks. Unlikely that they'll ever show up,

1 but if they do -- and I think that builds the confidence in
2 Canadians seeing that, actually, something is coming from it.
3 Maybe there will be no prosecution, but there's a record.

4 **DR. LEAH WEST:** Anyone else want to speak to
5 that?

6 Professor Currie?

7 **MR. ROB CURRIE:** Yeah, I agree entirely with
8 what Mr. Paulson said. There's a great deal of utility
9 there.

10 It's an activity for the police that requires
11 resources, it requires specialized knowledge, and that's
12 going to be a theme emerging here. Everything needs to be
13 well resourced and better resourced than it is, but that
14 signalling, communicative aspect is important. For Canada to
15 be out there in this way, it certainly underscores our
16 commitment to dealing with foreign interference, among other
17 kinds of criminal activities, and the -- you know, the simple
18 fact is Mokhtar Belmokhtar, people like that, we might never
19 get them or we -- I'm going to talk about Nova Scotia again.

20 We just had a case out of Nova Scotia
21 recently where a guy had jumped bail. We thought we'd never
22 see him again. He went to Italy for some reason. There was
23 an INTERPOL Red Notice issued, and they were waiting for him.
24 So that -- there's utility beyond the symbolic, I guess is
25 what I would emphasize there.

26 **COMMISSIONER HOGUE:** That will be a departure
27 from the -- I will say the common view or the way the various
28 agencies are operating these days. How would you suggest to

1 proceed for making such a shift in the way we are looking at
2 extra-territorial jurisdiction?

3 **MR. ROB CURRIE:** I'm more attuned to what's
4 going on with the Crowns and the courts, and so right there
5 I've long been an advocate for just more continuing legal
6 education on the international law aspects of domestic
7 criminal cases.

8 You know, the resources are available, but
9 when it's not part of the day to day very much, other things
10 rise to the top where it's more important that we look at,
11 you know, this other thing that we see more of and then, when
12 a relevant case comes up, there's a scramble for the toolbox.

13 And it's one thing if you're working in a
14 really well-resourced prosecution department in Toronto, but
15 entirely another thing if you're in Kamloops or Come By
16 Chance, Newfoundland, where you need to be able to get that.

17 So just making it part of the framework to
18 have resources available and ongoing training and familiarity
19 even if we're making people grit their teeth and bear it as
20 we introduce yet another thing for them to learn. And as --
21 and I don't mean to sound sceptical, but the fact of the
22 matter is, as I tell my students, there will never be less of
23 this, there will only be more. The world is getting smaller.

24 It's finally hitting Canada in a way that it
25 hit other countries long ago, and it's time that we increased
26 that capacity, I think.

27 **MR. BOB PAULSON:** I think if I can -- Bob
28 Paulson here, for the record.

1 If I can build on what Mike was saying
2 earlier, it turns on the professionalizing of the
3 investigative capacity, building, training, resourcing,
4 allowing that capacity to be deployed in those cases. In the
5 case of the Fowler-Guay kidnap, there was an enormous
6 government response because there was enormous public aspect
7 to the whole thing. And it seemed that, you know, having
8 those resources available already deployed and all sorts of
9 international activity, you know, warranted some sort of
10 outcome, some sort of result from this. The consequence of
11 kidnapping Canadians abroad was reinforced by quality
12 evidence given to the Attorney General to ultimately approve
13 charges.

14 But it turns on capacity and it turns on a
15 professional almost accredited approach to putting people in
16 charge of these investigations.

17 **DR. LEAH WEST:** So I want to turn now to
18 something that you recommended, which was this policy process
19 for thinking through options when it comes to activity that
20 might rise to the level of criminality and foreign
21 interference, but maybe criminal prosecution is not the
22 choice that we want to have.

23 And we heard from Professor Wilner that we
24 need a toolkit, and I think we've heard over the course of
25 the week that there is a big toolkit. We heard from our
26 diplomats about all of the different tools that they have in
27 their toolbox. There are sanctions. There's the
28 international legal forum, international fora. There's, you

1 know, pursuing intelligence threat disruption, cyber active
2 and defensive measures. Like there is a wide toolkit here,
3 but we need people around a table deciding which avenues to
4 pursue.

5 And I wanted to ask you to think through that
6 a bit more. You mentioned the lack -- or you need to have
7 those discussions without politics being at play, but for
8 most of the tools, other than choosing criminal prosecution,
9 there is Ministerial oversight required for any of them.

10 So I'm just wondering where you would sit
11 that body. Do you see multiple levels of some sort of
12 process, if you could think through that? And if anyone else
13 has anything they wanted to add on that as well.

14 **MR. BOB PAULSON:** So in my experience,
15 there's been clumsy efforts at trying to coordinate the
16 community. And this morning, you talked to two former very
17 well-respected National Security Advisors who talked about
18 the challenges of trying to coordinate the community.

19 It can't exist there because the political
20 considerations, although not, you know, sort of manifest in a
21 sense that Ministers aren't sitting around a table -- Deputy
22 Ministers are sitting around a table. And ultimately, this
23 becomes a political consideration.

24 So the success, if, indeed, we've had success
25 with the CSIS/RCMP evolution, has been to have practitioners,
26 operational practitioners, also agency leads, but operational
27 practitioners forced together to have discussions. I can
28 only imagine the kind of discussions that could be had given

1 the wide array of options that exist now. And in order to
2 arrive at the best course of action, I think they've all got
3 to be free to be able to discuss the possible consequences
4 outside of political considerations as to what may come of
5 PNGing a person rather than putting the handcuffs on them.
6 Or having CSIS do a threat reduction, if it's applicable.
7 The circumstances have to be, frankly, laid out for everyone
8 to be able to make those important decisions.

9 And there needs to be a record of those
10 discussions. Because I think some of the criticism that
11 we're hearing today is an absence of information about who is
12 making that decision? Who made that decision? And how did
13 that get reconciled, given the other responsibilities that
14 exist around government? So, I think it requires some heavy
15 thinking, but some clear, structured governance around those
16 assemblies of decision-makers within each of the agencies.

17 **DR. LEAH WEST:** Just a follow-up on that, to
18 think through practically, would you see foresee that coming
19 up with an options, you know, a list of options to pursue
20 that they would then be determined at the political level, if
21 it -- if those options required ministerial approval?

22 **MR. BOB PAULSON:** Well, ultimately, those
23 would be considerations in the discussion. If it was indeed
24 to rely sort of solely on a CSIS threat reduction activity,
25 then that requires ministerial engagement, and you would
26 recognize that. And what would be the consequence longer
27 term of engaging Ministers in that activity?

28 And, you know, a good example might be, I

1 heard colleagues talking about the registry. And I was
2 enormously excited to see the powers that this new
3 Commissioner would have to compel the so-called coercive
4 powers. Now, what -- as they're making decisions around
5 whether they'll proceed in an administrative fashion to
6 punish someone or refer it to the RCMP, what of the
7 information that's gathered and compelled, can that be
8 formed? Can that be relied upon by the investigation? And
9 how does that inform other agencies? They're very, very
10 complex issues that need those people in decision-making
11 roles to be able to do that, to make those decisions and
12 account for them.

13 But now, there's an absolute paucity of
14 accountability at any of these existing, you know, Assistant
15 Deputy Minister meetings and Deputy Minister meetings.
16 There's lots of discussion, lots of, "Okay, well, I'm going
17 to take that back." And there's no -- you heard me speak in
18 my opening comments about the need, a culture of doing things
19 as opposed to informing people about things. That's the
20 culture that exists within the bureaucracy and large parts of
21 the government, is that it's just about knowing things. And
22 when it comes to who's going to do something, those
23 conversations don't really happen there. And, at least,
24 that's been my experience.

25 **MR. CROFT MICHAELSON:** If I can just
26 interject, it's Croft Michaelson. You know, going forward,
27 there will be a lot of different players potentially
28 involved. There will be the Foreign Influence Transparency

1 Commissioner, CSIS, the RCMP, potentially the Commissioner of
2 Elections in certain types of scenarios.

3 And, you know, just to echo Mr. Paulson's
4 point, you know, when we've -- there needs to be -- there
5 will need to be some form of coordinating function, but at
6 the operational level, to sort out who's going to take the
7 lead on -- and what avenue is going to be pursued and what
8 makes sense.

9 You know, and in the national security -- in
10 the context of the counterterrorism space, I mean, the -- at
11 the operational level, the RCMP and CSIS sort of had those
12 type of mechanisms at the local level.

13 **DR. LEAH WEST:** So, currently, the SITE Task
14 Force exists, and it now exists throughout; it's not only
15 during the writ period. But do you see this overtaking the
16 SITE Task Force or being something that would be -- the SITE
17 Task Force would feed from it or complementary?

18 **MR. BOB PAULSON:** Well, I think building upon
19 that. I mean, the -- the seeming intent of the SITE Task
20 Force is to provide some mechanism for coordination of these
21 important issues, make sure that the police are in the room
22 and can -- but, to Croft's point, you know, there needs to be
23 that, okay, we understand, we understand what we know now,
24 what are we going to do about it, and what is the best way to
25 go about mitigating that or deterring it or stopping it? And
26 what are the consequences for everybody that's involved in
27 there?

28 I'm making it sound quite simple. It's a

1 very complex landscape. But absent the participation of all
2 the affected stakeholders, I don't think you can come to a
3 coordinated, you know, action.

4 And then, once things are underway, there's
5 nothing worse than having, you know, an ongoing criminal
6 investigation reported on into the government. Not because
7 of any other reason, other than those are very interesting
8 things to politicians, and they get out. So, it's not about,
9 you know, keeping our masters in the dark. It's about the
10 integrity of this investigative process that hopefully is
11 going to have an outcome. So, I think it would build on the
12 SITE Task Force. It would require the same sort of even more
13 elaborate governance that is provided for the SITE Task
14 Force.

15 **DR. LEAH WEST:** So, another element of
16 coordination -- we have about five minutes before the break,
17 three now, but I'll just -- we'll plant the seed -- is this
18 coordination amongst allies. And we are talking about
19 transnational activity that is affecting not just Canada, but
20 our allies, and we've seen that very recently in terms of the
21 charges against India or the allegations against India.

22 So, I'm just wondering if, Professor Currie
23 and Professor Wilner, if you had some quick remarks you
24 wanted to talk about, about how we leverage allies or how we
25 can improve upon the relationships with allies in this space.

26 **DR. ALEX WILNER:** I can be very quick.
27 Canada has yet to ever create a deterrence posture in any
28 domain. We function militarily within an allied setting.

1 And we're realizing quickly the limitations of acting in an
2 allied setting in cyberspace, where only at a certain
3 threshold, a very high threshold, where an allied response
4 might be expected. And so, we actually need our own cyber
5 deterrent posture. And I would suggest further, our own
6 specific posture related to foreign interference.

7 But those postures themselves would feed into
8 what we see internationally amongst allies, best practices,
9 and so forth. And so, it's a bit of a mesh, right? It's a
10 bit of an ecosystem of postures feeding into the end game of
11 deterring what we don't want to happen to us. Only then do
12 we prosecute and enforce. But deterrence is really the
13 bedrock, I would suggest.

14 **MR. ROB CURRIE:** Rob Currie, I'd only add, I
15 think, that I would get in line with the long line of
16 commentators who said it's time for new, rigorous, deep-
17 textured attention to foreign policy and formulating what it
18 looks like in the near term, in the medium term, in the long
19 term. In the way we've done in years past.

20 Again, that's a massive exercise, also, but
21 making sure that our foreign policy is geared to the current
22 threat environment. And I think that's, you know, that's
23 where we're living, the current threat environment. And the
24 perceptions of our allies along those lines, and specific
25 thought and attention to whether we are properly building
26 relationships, properly maintaining existing relationships,
27 whether it's NATO, whether it's Five Eyes, whether it's, you
28 know, any number of collective networks Canada is a part of.

1 With regard to what we re talking about on
2 this panel, we bring a very aware, border-porous kind of
3 posture around criminal law enforcement as part of the tool
4 bag to that table, as has been done in the past. There's
5 much to build on historically, both in our relationships and
6 the way we've administered them domestically. But a clear-
7 eyed and far-sighted attention to those relationships and how
8 they -- how they're going to support our own domestic
9 integrity as well.

10 **DR. LEAH WEST:** Commissioner, I think we'll
11 take a break?

12 **COMMISSIONER HOGUE:** Yes, we'll take the
13 break. Thirty (30) minutes. So we should be back at around
14 3:30.

15 --- Upon recessing at 3:00 p.m.

16 --- Upon resuming at 3:45 p.m.

17 **COMMISSIONER HOGUE:** You can begin.

18 **DR. LEAH WEST:** Thank you.

19 So we received a lot of questions. Some of
20 them more specific, some of them more general. We're going
21 to start -- I'm going to ask Professor Currie to give us an
22 international law lesson.

23 In the last couple of days, we've heard a lot
24 about the diplomatic tools, and including PNGing diplomats
25 for example. There's been some questions about why we can't
26 prosecute or what would be required to prosecute a diplomat
27 who is engaged in foreign interference in Canada. I'm just
28 wondering if you could explain the legal barriers or

1 impediments in that regard?

2 **MR. ROB CURRIE:** Sure. This is Rob Currie.
3 This is -- rests on a network of law that helps states get
4 the day-to-day business done, because they have to interact,
5 governments have to have their personnel interacting, they
6 have to have people on the ground in foreign countries, and
7 for that work to get done, the work of diplomats and other
8 kinds of officials can't be interfered with by local law
9 enforcement.

10 Now, there are trade offs. And this
11 represents very much a trade off that countries make and
12 agree to. They say that, "We will send out diplomats to your
13 foreign capital, our ambassador or ambassadorial staff,
14 people who are accredited as diplomats, and you will accept
15 that, because of the importance of the job and the importance
16 of international discourse, that you won't allow your police,
17 your law enforcement mechanisms to interfere with them,"
18 meaning they are immune from the process of the courts, they
19 are immune from arrest, they are immune from the exercise of
20 jurisdiction locally.

21 Now, that's not to say that they're immune
22 and they can do anything. They are meant to actually follow
23 the local law, abide by it quite assiduously. Where this
24 becomes a harder-edged inquiry is when they don't. When a
25 person who enjoys that level of immunity commits a crime or
26 otherwise gets themselves in trouble in the foreign country.

27 The immunity keeps them from being
28 immediately arrested or otherwise detained or interfered with

1 by the state, but there is a diplomatic process on top of
2 that. So in a situation where a foreign accredited diplomat
3 commits a crime or is implicated in a crime, the host
4 government is not only empowered, but entitled under
5 international law to ask the sending government, "We want to
6 prosecute this individual. Please waive their immunity."

7 Now, that practice differs entirely based on
8 the nature of the crime, the countries involved. The U.S.
9 makes those requests fairly frequently. They are fairly
10 frequently granted. They are infrequent here in Canada,
11 though there is recent history with them.

12 The foreign states have the choice, and the
13 choice is waive the immunity, which means the individual can
14 be prosecuted, or refuse to waive the immunity, which means
15 they can't be, but then the final step of that process is
16 that the host government is free to, and usually does expel
17 that person. That's where the phrase *persona non grata* comes
18 from. They are ruled to be a person of no legal status.
19 They must immediately leave the country.

20 That's at the level of diplomacy. There's a
21 similar layer of protections with consular staff. It's more
22 limited. There are geographical limitations. There's a lot
23 of technical material there, but the basics are the same.

24 **COMMISSIONER HOGUE:** And can you just tell
25 me, do they sometimes waive the immunity? Or it's something
26 that is rarely seen?

27 **MR. ROB CURRIE:** In Canada, I can't think of
28 a case where the foreign state agreed to waive immunity.

1 Expulsion is normally how these things happen. I know in --
2 the only other country I'm aware of much of their practice is
3 the U.S., where they do manage to convince sending
4 governments to waive, very often in narcotics cases and
5 things like that. But in Canada, it's very, very unusual.

6 **DR. LEAH WEST:** Could you just speak to the
7 likelihood of it being waived in a case that involves foreign
8 interference?

9 **MR. ROB CURRIE:** If we do things the way
10 Professor Wilner has explained them, and we articulate these
11 demands, then in a way it won't create any worries, because
12 the state will be so ashamed of having engaged in foreign
13 interference that they will either immediately recall their
14 diplomats, or potentially allow for prosecution. But again,
15 the likelihood is not large. The states that are inclined to
16 interfere with us if their immune personnel are caught doing
17 it, they are most likely going to be recalled and immunity --
18 so they will continue to enjoy the immunity, but the
19 Government of Canada is fully empowered to push them out of
20 the country.

21 **DR. LEAH WEST:** Thank you. I want to return
22 to a discussion we had earlier, and as well this morning,
23 about this concept of laying charges as a signalling and as a
24 revelation of -- or at least a modicum of accountability for
25 people who aren't necessarily in Canada or who have left the
26 country after engaging in foreign interference.

27 And I just want to clarify the example of the
28 United States, and they're frequently doing this was raised

1 as an example, and I'm just wondering if, Mr. Michaelson, you
2 can speak to the differences and/or any similarities in how
3 that process occurs in the United States versus in Canada?

4 **MR. CROFT MICHAELSON:** Are you speaking to
5 the -- it's Croft Michaelson. You're speaking to ---

6 **DR. LEAH WEST:** Yes.

7 **MR. CROFT MICHAELSON:** --- the charging?

8 **DR. LEAH WEST:** The charging where you --
9 where someone is outside of the country and -- versus the
10 laying of an indictment in the United States.

11 **MR. CROFT MICHAELSON:** Well, so in the United
12 States, they have a practice of, in their indictments, they
13 draft their indictments, they are really a narrative of the -
14 - and fairly extensive narratives of the conduct that
15 underlies and leads to the ultimate charge. So it's a
16 charging document, but it has a very, very long narrative.
17 And they can run into the tens, I've seen indictments that
18 are, you know, 50 or 60 pages long in the United States, and
19 those documents -- anyone reading that document will really
20 understand, to a large extent, the nature of the allegations
21 and the conduct that is being alleged against the individual
22 named in the indictment.

23 In Canada, charging documents are very
24 different. Whether it's an Information or an indictment,
25 those just specify the charge or charges that are alleged
26 against the accused. We don't go into large-scale narratives
27 of all the allegations. We prefer to argue our cases in
28 court and furnish the evidence in the context of the trial

1 proceeding.

2 So they're very different.

3 You know, investigations in the U.S. are also
4 quite different. They tend to be directed by a prosecutor.

5 So either -- at a superficial level, you have
6 everybody, sort of the District Attorney. You know, District
7 Attorneys they will often be involved in directing an
8 investigation. Same with at the federal level, Assistant US
9 Attorneys working together with the FBI, they are very much
10 involved in the investigation.

11 In Canada, we have separate independent
12 functions. We have the investigative function, which is the
13 policing function, and we have the prosecution function,
14 which is an independent function. So there are those
15 differences as well as between Canada and the United States.

16 **DR. LEAH WEST:** But Mr. Paulson, forgive me
17 if I'm wrong, but I seem to recall in my past, large-scale
18 announcements where there's Mounties standing in front of
19 seized, I don't know, drugs or guns or whatever; you know,
20 these are prior to prosecution. So there is some element of
21 information or narrative that could accompany a charge, could
22 it not?

23 **MR. BOB PAULSON:** Oh sure, yeah. And I think
24 that, you know, we do that with, you know, varying degrees of
25 competency in terms of making those announcements. In the
26 case of Belmokhtar, where we charged, I think we -- you know,
27 first of all, we had to secure the Attorney General's consent
28 to bring that charge. They do an analysis of the public

1 interest in bringing that charge, and we were fairly vocal in
2 terms of announcing the charge.

3 I think everybody understood that it was
4 unlikely that we would get him back, but there's an
5 opportunity there to communicate the effort and the work, and
6 short of a conviction at least demonstrate the competency of
7 the criminal justice system to address those things.

8 More broadly, you know, now that I'm retired
9 several years I find myself yelling at my television as
10 police officers get up to make an announcement only to say,
11 "It's an ongoing investigation, it's before the courts, we
12 can't say anything." So you wonder why they're there in the
13 first place. I think there's opportunities to be a little
14 bit more strategic, in terms of giving information that will
15 not compromise the ongoing investigation or the prosecution,
16 with a view to sensitizing Canadians to what's going on.

17 **MR. CROFT MICHAELSON:** And if I can just
18 interject? It's Croft Michaelson.

19 I can tell you prosecutors hate press
20 releases by police because of the potential for compromising
21 a fair trial down the road. And so there -- to Mr. Paulson's
22 point, there's a balance. The police can say some things but
23 if they too far, then we have concerns about impacting on the
24 fair trial rights of the accused.

25 **DR. LEAH WEST:** Okay. So on the topic of
26 strategic disclosures -- there's a segue for you -- there's
27 strategic disclosure around charges, informing people of the
28 alleged offences, but also in the context of intelligence.

1 And I'm just wondering if you can speak to the deterrent
2 effect, or how that plays into deterrence, and if you could
3 provide some examples?

4 **DR. ALEX WILNER:** Sure. It's Alex Wilner
5 speaking.

6 In the leadup to the Ukraine -- I'm sorry; in
7 the leadup to the Russian invasion of Ukraine, there was a
8 very dramatic series of strategic public disclosures by high
9 officials in Washington, the UK, Canada to a degree, some of
10 these were disclosed -- some of these events took place out
11 of the White House, sometimes it was the State Department, if
12 I'm correct, sometimes they were within an Allied setting.
13 And the idea there was to illustrate to the Russians, and to
14 their leadership particularly, that their intent was known,
15 that their means were known, and that there was momentum to
16 counter it by a variety of means. And I think part of the
17 deterrent messaging around that was to get into Russian
18 leader's head; "Where are the leaks? How do they know this?
19 What kind of threats do I face? What are the costs that I
20 can't see at the moment?" And so it's to try to change and I
21 would say cloudy their perspectives of the use and utility of
22 that form of aggression in Ukraine.

23 It's possible that in -- you know, taking it
24 back to today's discussion, it's possible that in this world
25 of foreign interference, that you can imagine well-placed,
26 timely public disclosures by officials -- I won't say
27 military officials but officials, could perhaps get under the
28 skin of a foreign operator who's attempting to interfere in

1 Canadian elections or, more broadly, in other matters.

2 How that would work? I mean, I think it
3 needs to be studied. I think I would be curious -- as a
4 scholar would be curious to see if there's evidence in other
5 jurisdictions, but I think name and -- naming and shaming has
6 perhaps a public -- sorry; a deterrent effect. Doing so
7 within the Allied setting, once again, would establish kind
8 of a lockstep approach to countering interference. And it's
9 again, perhaps one more toolkit in the box, right, to kind of
10 nudge an adversary away from these types of engagements with
11 us.

12 **DR. LEAH WEST:** So I'm formulating this
13 question on the fly, so I apologize. But the -- I guess what
14 is the difference -- and maybe anyone can speak to this --
15 between strategic disclosures and warning? You know, because
16 in effect in the Russian example they were the same thing.
17 And one of the big concerns we hear so often in the
18 discussion around foreign interference in democratic
19 processes is that warning itself could affect the democratic
20 process, or it could diminish trust in democratic
21 institutions.

22 So is it different in this space? Should it
23 be different, or do you see it as having a similar effect?

24 **DR. ALEX WILNER:** Alex Wilner speaking.

25 I think the focus is here is not just
26 warning, right? It's the strategic disclosure of
27 intelligence, secret information. So handpicked information
28 that we will associate to an understanding of our adversary's

1 calculus. So it's not just a public warning, we think this
2 is happening. It's very tailored, I would say niche, and
3 it's meant to insert ourselves and our capabilities into an
4 adversary's calculus, and to sow confusion, disorientation,
5 and uncertainty in their ability to do what they want to do;
6 deny, deny their ability to do so, or to the costs that they
7 can't yet see. And I think that's the point. And you do it
8 in advance.

9 There's a concept of deterrence, there's
10 general deterrence; I'm powerful, you know it, don't mess
11 with me. And then there's very technical deterrence, at the
12 level of an event, we see you doing this, we think you're
13 doing this, we know how to respond, we're getting ready to do
14 so. And I think, you know, I'm not exactly sure where, which
15 type of deterrence we're talking about at the moment, but
16 it's not general deterrence; it's specific deterrence around
17 specific events, and I would imagine that goes beyond just
18 warning, it's more detailed and calculated.

19 **DR. LEAH WEST:** So that is potentially an
20 element of threat disruption, in a sense; you're identifying
21 the potential threat and saying, "we see you coming, and
22 we're prepared to stop it," to get people to change course.

23 There are other elements of threat disruption
24 or threat reduction, and we've heard through the evidence
25 about potentially law enforcement choosing not to pursue
26 criminal prosecutions, but rather choosing to disrupt or
27 reduce the threat through other means. And I'm wondering if,
28 Mr. Paulson, you can speak to how that might play out; if you

1 have any thoughts on the validity or the usefulness of threat
2 reduction activity by criminal law enforcement, and where --
3 and who might be best placed to engage in that kind of
4 activity?

5 **MR. BOB PAULSON:** Yeah, well, I would say
6 this; you know, the police have, as their primary function,
7 the investigation of crimes. But they also have a duty to
8 prevent crimes. And when investigating, if you come to an
9 assessment that there's unlikely, or having regard for
10 partner activity, better ways of going about it, then often
11 you can just confront.

12 You know, there's a term in surveillance
13 called overt surveillance. I'm not suggesting that's a good
14 technique, but it is one technique of allowing the target to
15 know he or she is under surveillance. And that changes their
16 approach to what they're doing. Often a confrontation of the
17 target or associates to the target can be useful at deterring
18 their activities. But that has to be very carefully weighed
19 against the likelihood of evidence collection or activities
20 of other partner agencies.

21 I'd also say this, getting back to
22 disclosure. There's a tactical advantage to sometimes having
23 these disclosures of evidence, or of intelligence, in terms
24 of, you know, the vernacular is kicking the anthill once
25 you're positioned to collect evidence. And that has a very
26 positive impact in terms of generating evidence, wiretap or
27 surveillance evidence, or witnesses, or sources, or
28 undercover operators that are close. So that is also a

1 useful tool.

2 **DR. LEAH WEST:** Can you speak a bit about
3 engagement at the -- sorry, I'm trying to formulate. It's
4 been a long day.

5 **MR. BOB PAULSON:** Local law enforcement?

6 **DR. LEAH WEST:** Yeah, crime prevention at the
7 local level.

8 **MR. BOB PAULSON:** So the *RCMP Act* requires
9 that the RCMP prevent crime. Most police agencies, municipal
10 police agencies, the two provincial police agencies that
11 exist, three, I guess, have as their duty to prevent crime.

12 And so I was going to observe earlier in our
13 discussions that there is a vast network and infrastructure
14 of avenues into communities, diasporas, and just ground-level
15 access to individuals in order to socialize, inform folks,
16 community policing officers. You know, the philosophy of
17 community policing is alive and well and applied in varying
18 degrees to even federal policing, in terms of engagement with
19 communities. And we rely -- one of the benefits to having
20 the RCMP engaged in contract policing is that access to local
21 information.

22 I'll point out that recent headlines relating
23 to India, you know, had a murder investigation being
24 conducted by a contract division giving rise to an
25 understanding of what was going on, and then coordinating
26 through federal policing and on to government to get the
27 outcome that we're seeing.

28 So that can't be undersold, that network of

1 police officer contact at local level, and the ability to
2 access that and to leverage that, in whatever the agenda'd
3 item is, is invaluable, frankly. And we've used that
4 extensively with -- in counterterrorism in the day. So it's
5 a powerful, powerful tool that sometimes gets overlooked.

6 **DR. LEAH WEST:** Professor Nesbitt, you've
7 written in the past on threat reduction, and I'm just
8 wondering your thoughts on threat reduction or disruption by
9 law enforcement and anything to consider in terms of that?

10 **DR. MICHAEL NESBITT:** Yeah, I guess my
11 addition would be to sort of reinforce a number of things
12 that Mr. Paulson has just said, and then just to offer a
13 slight warning.

14 And so to reinforce it, I mean, law
15 enforcement does all sorts of things to reduce threats;
16 right? So if there's an immediate threat, you're going to
17 take action to stop a bomb from going off, rather than say,
18 "Hold on, we're going to let it go off because we've got to
19 build a case." Right? Clearly that is going to happen.

20 Over the longer term, we do anything from
21 visiting schools to inform kids to community policing, which
22 can be really effective in terms of talking to communities
23 about what's going on and figuring out sort of things.

24 In the national security space, on the
25 terrorism side of things, we have all sorts of things across
26 the country where we do this sort of work. So where I'm from
27 in Alberta, we have the Organization for the Prevention of
28 Violence, the OPV, that does work with young individuals

1 usually, or historically, on counter-radicalization or
2 deradicalization in that space, right, as sort of an
3 alternative to charging.

4 So clearly lots of space for this work.

5 You do have to be careful. And I say that
6 primarily because we have CSIS for this very reason, which is
7 that in the 1970s, after the FLQ crisis and the invocation of
8 the *War Measures Act*, it was -- with the Macdonald Commission
9 then in 1984 and then the creation of CSIS, it was thought
10 that when you give a police agency intelligence powers with
11 disruption powers, that there might be incentive to use the
12 disruption powers, rather than the policing. It's easier. I
13 don't have to go do all the work to get a 300-page warrant
14 and spend a year gathering that evidence.

15 And so rather extreme example obviously, but
16 we did see a series of abuses over a number of years; right?
17 So from opening hundreds or thousands of pieces of mail to
18 burning down a barn in one case, where they thought an
19 individual had -- where individuals were meeting.

20 So I think the lesson from that just can't be
21 lost, which is that we've gone through it once where we said
22 the gold standard maybe isn't the prosecution, just as a
23 general sense, without guardrails, and we, in Canada, have
24 seen that once go off the rails as a result.

25 The final thing that I'll just say here, just
26 to add to what's been said is in 2015, CSIS was given
27 disruptive powers and that was reinforced and made what I
28 would argue to be more constitutional in sort of, I think it

1 came in 2019, but through 2017, Bill C-59 Act. And one of
2 the purposes of that was this very thing, was to say, "Look,
3 this is the intelligence agency. They sometimes need
4 disruption capacity, and so -- and we feel they require it."
5 And so it was CSIS then that was given the powers, but in
6 being given the powers, they were given guardrails, and those
7 guardrails were warranted. And I mean that in the legal
8 sense; they have to go get a warrant. And that just ensures
9 further disruptive activities under section 12.1 of the *CSIS*
10 Act.

11 **DR. LEAH WEST:** Speaking of Bills that got a
12 lot of attention, C-51 and C-59, they were subject to a lot
13 of debate, study, review, there was a lot of input at the
14 committee process by civil liberties groups on the most
15 recent, other than the last one, big national security Bill
16 C-70, because of the imperative, presumably, around having
17 things in place for future elections did not go through that
18 same level of scrutiny, and civil liberties groups decried
19 that because of the lack of study about potential *Charter*
20 impacts.

21 I'm wondering if any of you sitting around
22 this table have concerns about either the fact that there was
23 a lack of study of potential impacts and hearing of those
24 voices in the Bill moving forward, or any specific provisions
25 or elements of the Bill that you think are particularly
26 problematic?

27 And I'll start with Professor Nesbitt,
28 because -- because.

1 **DR. MICHAEL NESBITT:** So we're talking about
2 a bill that's very new. So I say that because while having
3 read the Bill, I have not had time to formulate my thoughts
4 on the details.

5 Now, I suppose that goes to the point, which
6 is that there aren't very many of us in this space and sort
7 of *post hoc* we're trying to figure out our view on the Bill.

8 I will add, you know, the other question
9 there is not just the *Charter* compliance, although that's
10 obviously always a good question. The other is whether
11 there's something missing, right, that maybe more could have
12 been done through consultations. And I refer back to my
13 earlier conversation about sort of taking a broader approach
14 to thinking about the mandate and structure of the
15 organization and how it engages with other organizations. So
16 I don't know, but at some point it would be nice to have that
17 opportunity, I suppose, for Canada.

18 **DR. LEAH WEST:** Mr. Michaelson, do you have
19 any thoughts.

20 **MR. CROFT MICHAELSON:** Well, the Department
21 of Justice, on their website, they have their *Charter*
22 statement, as they're required to do, and, you know, they've
23 indicated that in their view, the legislation is
24 constitutional, the Attorney General is required to turn
25 their mind to the legislation and whether it's
26 constitutional.

27 And I frankly think that they take those
28 functions very, very -- those responsibilities very

1 seriously, so I think that they are primarily of the view
2 that the legislation is constitutional.

3 You know, nothing leapt out at me as I was
4 looking at it, but again, as Professor Nesbitt said, it's
5 early days and one never knows, you know, what arguments a
6 smart and creative defence lawyer can come up in a reasonable
7 hypothetical argument at trial.

8 You know, we've had other legislation that's
9 gone forward and no doubt everybody thought it was
10 constitutional, and it was found to be unconstitutional
11 because of reasonable hypotheticals that no one had thought
12 about.

13 So again, it's early days and we'll see.

14 **DR. LEAH WEST:** Thank you. Now I want to
15 turn back to potentially some of the provisions that have
16 been added to the *Criminal Code*.

17 But Professor Currie, if you could expand on
18 your discussion of seizing opportunities to use
19 extraterritorial jurisdiction in the foreign interference
20 space?

21 **MR. ROB CURRIE:** Sure. Rob Currie. And let
22 me bounce off the last one as well, because here is an aspect
23 of C-70 that won't be a problem under the *Charter*, which is
24 the expansion of the territorial reach of some of the
25 offences.

26 And I say that because there have been legal
27 challenges to extraterritorial criminal law provisions in the
28 past under a theory that it was somehow offensive to

1 individual rights, and that is -- it's incorrect -- it's an
2 incorrect argument and because it's a matter of
3 constitutional power, the federal government is fully
4 competent to legislate in a manner that makes -- extends our
5 criminal law beyond our shores if they choose to do so.
6 There are limits, but they are limits imposed by
7 international law, not by domestic constitutional law.

8 So I think that's -- you know, that's just a
9 point worth making. Extending the geographical reach of law
10 enforcement doesn't impinge on *Charter* rights by itself.

11 But to get into the weeds of what that means,
12 I think the best way to explain it is to take a hypothetical
13 FI case, which is one person who is, you know, an agent of a
14 bad actor state making threats, intimidating remarks maybe,
15 or bribes, or that kind of activity.

16 There are three levels, jurisdictionally, at
17 which it might be done.

18 It might be done entirely on Canadian soil,
19 then we don't have a problem. That crime happened entirely
20 in Canada, Canada is fully jurisdictionally competent.

21 But what if the bad actor is telephoning the
22 individual from another country or sending them email --
23 threatening email threatening their family? Does Canada have
24 jurisdiction to do anything? Can the police even look at
25 that?

26 And again, anecdotally, that can be a
27 problem. Somebody walks into a police station and says, "I'm
28 getting these threatening emails. I think I know where

1 they're coming from." And the poor under-resourced cop says,
2 "They're coming from outside of Canada. We can't do anything
3 about that." And legally, that's not true, but resource-
4 wise, to an extent, it is true.

5 But that's an example of what's referred to
6 technically as qualified territorial or extended territorial
7 jurisdiction. If a crime begins outside Canada but finishes
8 here, we have jurisdiction over it. If it begins here and
9 finishes outside Canada, we have jurisdiction over it. And
10 there's an extensive body of case law around that.

11 But in C-70, there are also fully
12 extraterritorial provisions, which is to say the entire
13 offence takes place outside Canada. And those are situations
14 where Canada can completely lawfully, under international
15 law, take jurisdiction over the offence, even though it's
16 entirely outside our borders, based on some other link to our
17 national interests, to our nationals, sometimes. And the
18 examples we see in C-70 are situations where either the
19 perpetrator, or the victim, or both are Canadian nationals,
20 they're outside Canada, which is -- which extends it right
21 out, or that other Canadian national interests are
22 implicated, because there's a slightly murky but still well-
23 worn principle of international law that says states can
24 criminally prosecute crimes that take place outside their
25 borders if they are -- if those crimes are directed at their
26 fundamental national interests. And this is everything from
27 espionage to counterfeiting of passports and currency.

28 But foreign interference activities, I would

1 offer, fall right in neatly into that pocket of things Canada
2 is absolutely competent to do.

3 So all three of those levels of jurisdiction
4 are available to Canada. The ones that touch outside our
5 borders are the ones that historically we've been
6 uncomfortable with. And I say historically because it comes
7 from the U.K., where for centuries they didn't care what
8 happened off the island. It didn't matter what happened in
9 France. It matters more than ever now what happens outside
10 Canada that potentially impacts us.

11 So there is a really good set of
12 jurisdictional tools, and C-70 really is beginning to crack
13 that open, and I just say we should break it even further
14 open.

15 **DR. LEAH WEST:** One of the parties asked a
16 question about a tool that is fully extraterritorial in
17 scope, which is the *Crimes Against Humanity and War Crimes*
18 *Act*. Do you see that as a potential tool in the context of
19 foreign interference?

20 **MR. ROB CURRIE:** I think the short answer is
21 no. And you're right, that's -- that part of our criminal
22 law provides a set of offences that do apply entirely
23 extraterritorially, as well as within Canada, but it is on
24 the subject of a really narrow range of crimes, literally
25 three: genocide; crimes against humanity; and war crimes.
26 And I think we can expect that those three kinds of conduct
27 won't play a large role, if any, in foreign interference
28 efforts.

1 DR. LEAH WEST: Commissioner?

2 COMMISSIONER HOGUE: I'm okay. You can go
3 on.

4 DR. LEAH WEST: I'm just going to invite the
5 panellists to offer any last remarks that they might have or
6 that they want to convey to the Commission, or things that
7 they want to, you know, double stamp on.

8 Professor Wilner?

9 DR. ALEX WILNER: Thank you. Alex Wilner
10 speaking.

11 I want you to imagine a world where
12 deterrence doesn't work. It's not pretty; right? It means
13 that we're responding repeatedly with no understanding of the
14 larger things that we could do. And so deterrence is, again,
15 -- my takeaway is deterrence is something you actively do.
16 You think about it, and you apply it, and you tie all of
17 those loose strings that we have going now, and you tie it to
18 this core, which is don't mess with us. Don't mess with us.
19 We have the means to deny the success. We have the means to
20 prosecute. We have the means to attack you if needed.

21 Until we link all of these pieces together,
22 it's the early days of counterterrorism, whack-a-mole. One
23 there, one there, one there, one there. We keep responding.

24 So deterrence again is just simply a
25 framework that feeds into this entire soup of activity. And
26 I think it ties neatly into what we can do domestically and
27 internationally because we're not doing it alone.

28 So I think we need a bit of a shift.

1 And finally, one last piece is that from a
2 deterrence scholarship, we're still stuck in the Cold War
3 logic of deterrence, which was success or failure. If the
4 nuclear bomb goes off, deterrence failed. But we're not --
5 that's not the kind of deterrence we're into. We're kind of
6 leaning into criminal deterrence, which is we put up with a
7 certain threshold of pain, but to a certain degree beyond
8 that, we bring the hammer down.

9 And so I think when we speak of deterrence,
10 we should take it out of the Cold War context, we need to
11 internationalize it, and update it, and expand it, but it
12 needs to be within the context of what we're facing today,
13 which is a mess, which is an absolute mess. But I think it
14 is the bedrock upon which all of the other pillars can rest.

15 **DR. LEAH WEST:** Could you just briefly speak
16 to how you see denial working in terms of building trust in
17 democratic institutions, public education? How does that
18 feed into your framework?

19 **DR. ALEX WILNER:** The logic of denial is to
20 strip an adversary the ability to acquire what it hopes to
21 acquire with the unwanted act.

22 And so denial here in this case is to, I hate
23 to use this word, but to inoculate Canadian society against
24 responding in the ways that our adversaries would like for us
25 to respond when they engage with disinformation, which is to
26 ultimately change my vote, or to undermine the credibility of
27 our legal system, or our democratic system, et cetera.

28 And so we saw this again going back to the

1 early days of counter-radicalization, the idea was to
2 inoculate people, societies, communities, against falling
3 into this trap, radicalization in one case. In this case,
4 acting upon disinformation or foreign interference.

5 And so I think denial is sending the message
6 that we are able to absorb and ignore the things that you
7 send our way. This is not exclusively or even solely about
8 what the Federal Government can do. I think public education
9 is part of this. I think it's about engaging with scholars
10 and setting up communities of practice, and all the rest;
11 right? But I think denial is part and parcel, because we can
12 only punish so much, but denial is about how we protect
13 ourselves and link that to manipulating behaviour.

14 **DR. LEAH WEST:** Thank you. Anyone else? Mr.
15 Paulson.

16 **MR. BOB PAULSON:** I think we need to consider
17 why it is that we are being victimized the way we are
18 recently. And what weakness that demonstrates or is being
19 exploited by those hostile state actors. I think it's
20 absolutely vital that we get our act together, because it's a
21 harbinger of what's going to come. Weakness breeds an
22 invitation to do more.

23 And I think the perception, and this is very
24 anecdotal, but I think the international perception,
25 particularly among our adversaries, is that we are vulnerable
26 to exploitation. And so, that should just maybe underscore
27 the importance of your work.

28 **MR. CROFT MICHAELSON:** If I could just make

1 an interjection briefly. It's Croft Michaelson. There's
2 been some discussion about strategies such as laying charges
3 against individuals outside of the country where there may be
4 little prospect of prosecution actually going forward.

5 And I think the practical reality is that for
6 police that are under-resourced, that's not going to be a
7 strategy that they're going to be interested in pursuing.
8 And prosecutors probably won't be particularly interested in
9 it either. It really calls for, if this is a priority, it
10 really calls for proper resourcing of both the police and
11 investigative function -- the police and prosecutorial
12 functions.

13 You know, if I think back, you know, and Bob
14 will remember this too, but when you think back to the early
15 days of the *Proceeds of Crime* legislation, when that first
16 came out in the 1980s, we didn't really get -- make a lot of
17 headway initially, and then we set up specialized units. And
18 the specialized units then had, you know, identified it as a
19 priority activity, and then we started to make a lot of
20 headway in investigations and successful prosecutions.

21 So, no doubt the Commissioner's heard about
22 resourcing in other -- in other roundtables, but I think
23 that, you know, it's central to actually having an effective
24 prosecution function.

25 **DR. LEAH WEST:** And this will turn into an
26 excellent segue to my question for Professor Nesbitt, which
27 is you spoke a bit about money and sanctions. I'm just
28 wondering about your thoughts as sanctions and their

1 deterrent effect in this space, and if you could speak to
2 that.

3 **DR. MICHAEL NESBITT:** I think -- so if I may
4 give you the technical answer, I think the academic
5 literature over time is largely split on the actual
6 deterrence effect of sanctions. Having said that, the more
7 recent work I have seen would seem to suggest that sanctions
8 do have a deterrent effect. I also have serious questions
9 about whether we're measuring the right thing in a number of
10 those studies.

11 So, just anecdotally speaking, when we
12 sanction Russia, very quickly there's a Russian response to
13 sanction a bunch of high-profile Canadians. So, what does
14 that tell you? They're paying attention, they care, and they
15 feel like they need to respond. So, I guess that gets me to
16 my feeling about this, which is that it is hard to study this
17 space or just watch this space and not think that sanctions
18 have a meaningful deterrent effect.

19 Having said that, we have to be honest about
20 where Canada sits in the sanctions space, and that is as an
21 economically smaller player, beside and supportive of the
22 United States, and I suppose the last thing I'll say in that
23 regard is that when we're talking about sanctions, there's
24 only so much we will do. A lot of it is for supporting the
25 U.S., and if the U.S. is doing something, then sanctions will
26 have a deterrent effect.

27 But I will say our lack of -- it's perhaps,
28 once again, an opportunity to bring up our lack of

1 enforcement, right? So in 1992, we have the *Special Economic*
2 *Measures Act*; we have two prosecutions to date under the
3 *Special Economic Measures Act*. One of which fell apart at
4 pre-trial, and the other, which was a guilty plea for what
5 was literally sending stuff to Iran in contravention of our
6 Iran regulations, and the border catches it and says, "You
7 can't send this stuff to Iran." So, pretty easy capture.

8 And so, in the absence of that enforcement,
9 which we have been working, and there has been good headway
10 in the last four or five years at Foreign Affairs with
11 funding for the RCMP, and then RCMP setting up sort of
12 sanction resourcing within the broader sort of national
13 security and money areas, we're getting there, but we haven't
14 seen those results yet. And until we start seeing those
15 results, Canada's ability to deter or contribute to the
16 broader deterrence goals of our allies, particularly the EU,
17 the U.K., Australia, and the U. S. on the sanctions side, is
18 pretty limited.

19 **DR. LEAH WEST:** And my last question is for
20 Professor Currie, before I turn it over to the Commissioner.

21 Are there any other international fora
22 besides international courts where you could see Canada
23 taking its concerns over FI that might be useful, or other
24 convention bodies, et cetera, or do you really see pursuing
25 international legal measures at say the ICJ as the only tool
26 internationally?

27 **MR. ROB CURRIE:** The ICJ, it's not even a
28 great tool. You know, those proceedings are time-consuming,

1 they're contentious and expensive, and you always run the
2 risk that the foreign state on the other side will withdraw
3 their agreement to consent to the Court's jurisdiction. So -
4 - and it's been stunning in cases where they didn't, in fact.
5 So, there are layers of politics there.

6 But this is more on the informal end of
7 enforcement. It's more about relationships with allies,
8 presenting united fronts and really appearing to have a
9 robust domestic framework that is outward-looking and that
10 will counter the authoritarian and meddling forces that are
11 coming at us. That's no less enforcement of international
12 rights and obligations than going to court is. It's just a
13 different and, frankly, more historically grounded way of
14 doing it.

15 **DR. LEAH WEST:** Thank you.

16 Commissioner?

17 **COMMISSIONER HOGUE:** I have one question for,
18 I think it will be for Mr. Michaelson. You have a lot of
19 experience in prosecuting various crimes. And I'm interested
20 in knowing whether you have any ideas as to how to minimize
21 the impact of the intelligence-to-evidence problem. In the
22 context of if, for any reason, the decision will be made to
23 prosecute foreign interference, can you think of any means of
24 minimizing this problem?

25 **MR. CROFT MICHAELSON:** Well, the best way to
26 minimize the problem is to rely on as little intelligence
27 information as possible, obviously.

28 I do think there may be room for some

1 statutory reform of the section 38 disclosure regime. I
2 think that, you know, my prosecution in the *Regina v. Jaser*
3 case, you know, we navigated the national security issues in
4 that case, I thought, quite successfully. I thought that
5 what Justice Code came up with in *Regina v. Jaser*, you know,
6 might be a useful template on how to, you know, how one could
7 actually reform the section 38 disclosure regime and invest
8 jurisdiction in a Superior Court trial judge to address the
9 issues.

10 You know, absent that, you know, now, we have
11 -- the disclosure regime we have has been one that's been
12 crafted, you know, by the Supreme Court of Canada. They've
13 always said there may be more than one disclosure regime
14 that's constitutional. And so, whether one looks at some
15 outside-of-the-box thinking and really thinks about, you
16 know, having an alternative approach from the one we're
17 thinking about, something like intelligence information, I've
18 thought about this a lot and I really haven't cracked the nut
19 yet, Commissioner, so there's not much more I can add on.

20 **COMMISSIONER HOGUE:** It's not an easy one.

21 **MR. CROFT MICHAELSON:** Yeah, it's not an easy
22 one. I had some ideas in a paper that I wrote that was
23 published in the *Manitoba Law Journal*, you know. Some of it
24 was blue-sky thinking, and I'm not sure that it would
25 actually ultimately make things much better. But I don't
26 really have any easy answer for you.

27 **COMMISSIONER HOGUE:** Thank you.

28 So thank you very much. It was interesting,

1 challenging, and what is fascinating is you have many
2 different experience; many different field where you have an
3 expertise, so I will have to put all that all together and
4 try to find our way in that context.

5 But I really, really appreciate all the
6 information you have provided me with today. And again, I
7 have said that on a few occasion, but it's really food for
8 thought for us, and we realize how much work we have ahead of
9 us.

10 So thank you, and have a good day, all.

11 **MR. CROFT MICHAELSON:** Thank you.

12 --- Upon adjourning at 4:34 p.m.

13
14 **C E R T I F I C A T I O N**

15
16 I, Sandrine Marineau-Lupien, a certified court reporter,
17 hereby certify the foregoing pages to be an accurate
18 transcription of my notes/records to the best of my skill and
19 ability, and I so swear.

20
21 Je, Sandrine Marineau-Lupien, une sténographe officielle,
22 certifie que les pages ci-hautes sont une transcription
23 conforme de mes notes/enregistrements au meilleur de mes
24 capacités, et je le jure.

25 
26 _____

27 Sandrine Marineau-Lupien
28