HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

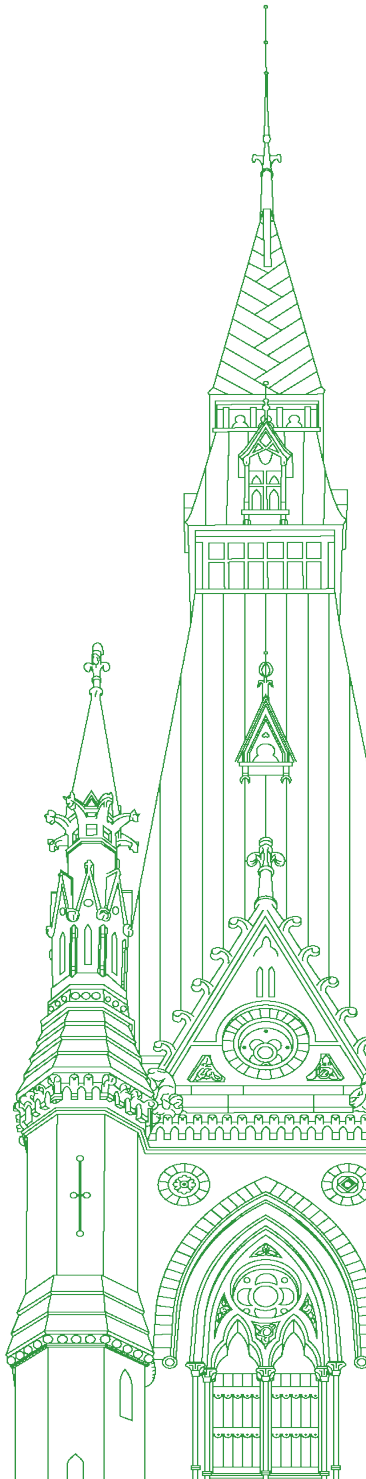
44th PARLIAMENT, 1st SESSION

Standing Committee on Public Safety and National Security

EVIDENCE

NUMBER 112

Wednesday, June 5, 2024



Chair: Mr. Ron McKinnon

Standing Committee on Public Safety and National Security

Wednesday, June 5, 2024

● (1710)

[*English*]

The Chair (Mr. Ron McKinnon (Coquitlam—Port Coquitlam, Lib.)): I call this meeting to order.

Welcome to meeting number 112 of the House of Commons Standing Committee on Public Safety and National Security.

Pursuant to the order of reference referred to the committee on Wednesday, May 29, 2024, and the motion adopted by the committee on Monday, May 27, 2024, the committee resumes its study of Bill C-70, an act respecting countering foreign interference.

Before we begin, I would like to ask all members and other in-person participants to consult the cards on the table for guidelines to prevent audio feedback incidents.

Please take note of the following preventative measures in place to protect the health and safety of all participants, including the interpreters in particular. Only use a black, approved earpiece. The former grey earpieces must no longer be used. Keep your earpiece away from all microphones at all times. When you're not using your earpiece, place it face down on the sticker placed on the table for this purpose. Thank you all for your co-operation.

Today's meeting is taking place in a hybrid format. I would like to make a few comments for the benefit of members and witnesses.

Please wait until I recognize you by name before speaking. I will remind you that all comments should be addressed through the chair.

I have specific comments to make on Bill C-70. I would like to remind members that amendments to Bill C-70 must be submitted to the clerk of the committee by 4 p.m., eastern standard time, on Friday, June 7, 2024. It is important for members to note that, pursuant to the order adopted by the House on May 30, the 4 p.m. deadline to submit amendments is firm. This means that any amendments submitted to the clerk after the deadline and any amendments moved from the floor during clause-by-clause consideration of the bill will not be considered by the committee.

I will also note, for all members of the committee, that the charter statement on Bill C-70 has been distributed, and you should find it in your inboxes.

I'd like to now welcome our witnesses for today.

[*Translation*]

Mr. René Villemure (Trois-Rivières, BQ): I have a point of order, Mr. Chair.

I'd like to make sure that the sound checks have been completed for the interpreters and those participating in the meeting by video conference.

[*English*]

The Chair: Yes, all tests are done.

[*Translation*]

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Thank you.

I'd now like to welcome our witnesses for today.

With us, as an individual, we have Mr. Richard B. Fadden.

Welcome back. I remember having you here before.

From Canada-Hong Kong Link, we have Gloria Fung, immediate past-president. By video conference, for Hong Kong Watch, we have Katherine Leung, policy adviser.

I'd like to thank you all for your participation in our meeting today and for your flexibility in appearing so quickly.

I now invite Mr. Fadden to make an opening statement of up to five minutes.

Please go ahead, sir.

Mr. Richard Fadden (As an Individual): Thank you, Mr. Chair.

Thank you for the opportunity to speak to you on Bill C-70. I am especially grateful for this opportunity because it addresses a number of issues that I and many others have advocated on for some time.

Bill C-70 is a relatively complex and, in some cases, quite technical piece of legislation. However, its overarching thrust goes a considerable distance towards dealing with the threat of foreign interference—again, a threat that has been with us for some time. In particular, the creation of offences relating to foreign interference and the creation of the foreign influence transparency commissioner and of the registry he or she will be required to maintain will provide tools that Canada is lacking. These measures will not make foreign interference go away, but they will help deal with the threat.

As well, the provisions amending the CSIS Act, permitting the service to disclose information much more broadly than is currently the case, will assist government institutions, as well as the private sector and civil society, in understanding and dealing with threats to our national security. In this respect, these amendments will help deal not only with foreign interference but also with other threats to national security.

I have two last comments. The first deals with concerns that I have seen reported in the media to the effect that some provisions in the bill risk charter compliance issues. I am not a charter lawyer. Indeed, I am a lapsed lawyer. However, I do not see this risk in the actual words of the bill. Is there a possibility that its implementation might increase the risk? Possibly.

Having said this, it seems to me that this is frequently the case with any law that creates offences. However, I do not believe—and I hope you will agree with me—that such concerns should prevent you from approving Bill C-70. I think that there are four reasons for this. First is the certificate of the Minister of Justice, which the chair just referenced. I also think that Parliament is entitled to believe in the good-faith implementation of the law by ministers and officials. If there is a real problem, there is always recourse to the courts. Finally, if there are really serious problems, you can change the law.

My last comment relates to what I understand is the view of some: that Bill C-70 should not be dealt with on a fast track. I would suggest to the contrary that the expeditious review and passage of Bill C-70 is in the national interest. I can see no possibility that our geopolitical adversaries will in any way in the foreseeable future modify their behaviour so as to lessen threats to our national security. These threats are real and affect virtually every part of our country: the private sector, civil society, individuals and governments at all levels. NSICOP, NSIRA and the Hogue inquiry all clearly support the view that the threats you are considering are real and require action. To not deal with Bill C-70 in the days and weeks ahead and—if you'll forgive me for saying so—in an environment increasingly affected by the possibility of an election could mean the demise of Bill C-70.

My last thought is that, even if Bill C-70 were to receive royal assent next week, implementation will take some time, and I hope you will take this into account as you consider time frames relating to the bill.

Thank you for your attention, and in due course, I'd be more than happy to try to answer your questions.

Thank you, Mr. Chair.

● (1715)

The Chair: Thank you, sir.

I now invite Ms. Fung to make an opening statement of up to five minutes.

Please go ahead.

Ms. Gloria Fung (Immediate Past President, Canada-Hong Kong Link): Mr. Chair and distinguished members of the committee, I thank you for this opportunity to comment on Bill C-70, the countering foreign interference act.

I'm the immediate past-president of Canada-Hong Kong Link and convener of the Canadian coalition for a foreign influence transparency registry. The coalition established in 2021 consists of 33 multicultural community organizations, think tanks and human rights groups across Canada. Our mission is to advocate for a foreign influence registry to be enacted in Canada to enhance transparency in the democratic process.

Over the past two decades, both CSIS and Canadian civil society have repeatedly warned our government about foreign interference and transnational repression in Canada, but they have remained complacent. The transnational repression faced by diaspora communities includes telephone threats, cyberbullying and smearing of Canadians through disinformation campaigns, surveillance, coercion and harassment through counterprotests and physical attacks.

The Chinese Communist Party is by far the most active state player in this interference operation through its sophisticated network involving hundreds of proxies, posing a major threat to our national security, sovereignty and democracy. Canada is at the back door to the U.S., China's adversary. By infiltrating Canada, China can access sensitive intelligence information of the U.S., the Five Eyes allies and NATO.

CCP agents capitalize on the openness of our democratic system to infiltrate community, media, academic and business sectors. They are active in undermining our democratic institutions at all levels of government.

As we recently brought together eight MPs from all five federal parties to call for the immediate introduction of legislation to counter foreign interference, our coalition welcomes the bill and strongly supports the emerging non-partisan consensus to get the registry passed and to get it up and running before the 2025 election call. We hope the House can send it to the Senate before it rises for the summer.

I would like to make the following recommendations.

Number one, the government should set up an independent commission to coordinate and monitor the implementation and future periodic reviews of the act.

Number two, the act and corresponding regulations should be reviewed and updated within one to two years after the 2025 federal election. After this, they can be reviewed once every five years in accordance with the rapidly evolving foreign threats.

Number three, for the purpose of the registry, "political activity" defined in the act needs to be expanded to include elections to internal political offices; political party leadership contests; appointments of individuals to public offices; government hiring decisions; third party political advertising; decision-making within parliamentary and legislative caucuses, such as the selection of officers, expulsion of members and removal of leaders; law enforcement decisions; and decisions of tribunals and regulators.

Number four, legislation should allow authorities to be proactive in implementing the registry. In Australia, for instance, authorities can send a request for information to determine whether or not individuals or entities need to register.

● (1720)

Thank you.

The Chair: You're right on the dot. Thank you very much.

We go now to Ms. Leung to make an opening statement of up to five minutes.

Please go ahead.

Ms. Katherine Leung (Policy Adviser, Hong Kong Watch): Thank you, Mr. Chair.

I'm the policy adviser for Hong Kong Watch in Canada, and I am before the committee today to speak to Bill C-70.

Hong Kong Watch supports the speedy passage of the countering foreign interference act such that it will be in place before the next election. We support the bill as a whole, but I will use my time to speak with emphasis on suggested amendments that would ensure that the scope of the bill would thoroughly address foreign interference.

We support the proposed amendments to the Canadian Security Intelligence Service Act, especially amendments related to equipping national security partners to build resiliency to threats by enabling broader disclosure of CSIS information to key partners beyond the Government of Canada. Foreign interference is not limited to governmental targets but rather affects individuals and organizations across various sectors.

We know, from media reports and previous committee testimony, that there are considerable foreign interference activities targeting Canadian universities, businesses and technology. This is why broadened information disclosure will allow institutions to better understand and anticipate potential threats and to take proactive measures to safeguard their operations and intellectual property.

We're also supportive of the proposed measures to counter foreign interference under part 2 of the bill. The creation of new offences for foreign interference, including deceptive acts that undermine democratic processes and harm Canadian interests, is much needed. These amendments address the reality that foreign interference often targets individuals at the grassroots level, thereby indirectly influencing democratic processes and Canadian interests.

While intimidation, threats and violence are tactics used by foreign entities to silence dissent within diaspora communities, discrimination is another method employed to suppress opposition. We have seen cases in which individuals in Canada have faced job loss or eviction from their homes due to their political opinions.

We would be supportive of proposed amendments that acknowledge the tactic of discrimination and provide mechanisms to counter it effectively. We also support the creation of the foreign influence transparency registry. By imposing obligations on individuals and entities to register arrangements and disclose foreign influence activities, the Government of Canada can increase transparency and accountability.

However, it is important to expand the scope of the act beyond political processes. Much of foreign interference occurs at the community level, where it can suppress public discourse and indirectly influence democratic processes.

Let me illustrate how transnational repression as a form of foreign interference can have an impact on political processes. This is from a case study of a Hong Konger in Canada, which I heard about through my work at Hong Kong Watch. A pro-democracy activist from Hong Kong fled to Canada in 2020, after participating in the 2019 protests and encountering police altercations that led to the detention of her friends. She claimed asylum, settled in Calgary and continued her advocacy for democracy in Hong Kong. She is one of the founding members of a group of volunteers who assist persecuted Hong Kongers seeking asylum in Canada.

Since publicly criticizing the Chinese government, she has received anonymous threats on Telegram, including harassing messages about her appearances and advocacy, and graphic videos, including a bloody video of a woman suffering severe blunt force trauma to the head and a video of a beheading, with captions referencing her involvement in pro-democracy organizations. The sender also disclosed personal details about her life, including her boyfriend's name, her employer and her workplace address. She has reported these threats to CSIS and the RCMP.

As Bill C-70 is written, the anonymous sender in this case would not trigger a requirement to register as a foreign agent. This is not an activity directly related to parliamentary or legislative proceedings, development of a legislative proposal, development or amendment of a policy or program, decision-making by a public office holder or government body, elections, referendums or nomination contests. Rather, this is something that has silenced this individual. Due to fears for her safety, she no longer participates in pro-democracy advocacy for Hong Kong, despite permanently living in Canada.

Foreign states use transnational repression to discourage dissent by diaspora communities, thereby undermining democratic participation and the ability of elected officials to represent their constituents fully. Expanding the act to encompass all levels of foreign interference activities, including transnational repression and intimidation, will provide a more comprehensive safeguard against these threats.

With that, I conclude my remarks here.

● (1725)

The Chair: Thank you for your remarks.

Thank you, all. We will start our questioning at this point, beginning with Mr. Caputo.

Mr. Caputo, go ahead for six minutes.

Mr. Frank Caputo (Kamloops—Thompson—Cariboo, CPC): That's great. Thank you very much, Chair.

I thank all of the witnesses. We have had some wonderful witnesses here today. We've had excellent witnesses throughout, but this panel in particular really stands out to me.

Ms. Leung, Ms. Fung and Mr. Fadden, thank you for being here. I have only six minutes, but there's really so much to ask.

Mr. Fadden, I'm going to key in on the first note that I took from what you said. You said that this threat has been with us for some time. Now, we've heard from different people, but you have a fairly distinguished background in this regard.

How long has this issue been with us, and is it intensifying or are we just more likely to discover it right now?

Mr. Richard Fadden: I think it's difficult to pick a particular day or week or month, but I would say that it has been with us in a noticeable way since easily the last couple of years of Mr. Harper's government. It existed before then, but I think, with the passage of time, it has intensified and it continues to intensify.

The most noticeable increase in intensity occurred after President Xi became the leader of China. His activity is much more aggressive and proactive, and that's been manifested in all of the policies of the People's Republic, both with respect to foreign interference and more generally.

Mr. Frank Caputo: All right. Obviously, this act is country-agnostic so far, but have you noticed this intensity from any other foreign state actors?

Mr. Richard Fadden: I think, Mr. Chairman, that China stands out, but I also think, as has been reported in the media, that Iran is becoming slightly more active. I think India is as well, not just with respect to the killing of Mr. Nijjar but throughout the community.

Russia operates, I think, in a slightly different way. If China covers the waterfront as much as they can, Russia tends to be more specific. They're more like a surgeon. They do intervene. I don't think that has necessarily increased in intensity a great deal, but they're there and they continue to intervene, although not necessarily through their diaspora. That's the one big difference between them and China.

Mr. Frank Caputo: I see what you're saying.

You commented that there's been a fairly recent difference in intensity when it comes to foreign interference. Is that solely in terms of foreign state actors having a greater desire to interfere, or is there something happening here in Canada—a lack of enforcement, perhaps—that is playing into that?

Mr. Richard Fadden: I think it's a bit of both. As I said a minute ago, China in particular but also others have become much more aggressive and assertive, but I also think that, compared to our close allies, Canada has been a little bit slower in providing the state with tools to deal with this.

I'm not suggesting that it's been ignored, but I am suggesting that it's taken us a while to get there. The United States, the United Kingdom and Australia have dealt with this issue, I think, more quickly than we have. Your colleagues in Australia, for example, have enacted a variety of pieces of legislation to directly address both foreign interference and espionage.

I think the main difference is that, when an adversary goes through a list of countries it wants to attack, it will do something in each of them, but if there's one that is slightly less organized, slightly less structured to push back, the adversary will make a bit of an effort there.

Mr. Frank Caputo: Okay. Thank you.

Now, Ms. Leung, you said that interference "targets individuals at the grassroots level", and you even talked about job losses and evictions, things that people in this room might not be used to hearing about. When I think of interference, certainly I think of different things than those. Can you expand a little bit on that? You talked about the silencing of individuals as opposed to the impacts on governments.

We have about a minute and a half. Are you prepared to expand on that for that time?

● (1730)

Ms. Katherine Leung: I can give a case study for both of these cases.

The job loss one involved a community member from the Hong Kong diaspora here in Canada who told me that he was employed by someone of Chinese descent here in Canada, and that person had very strong feelings about the Hong Kong pro-democracy movement.

Now, it's notable that he came to Canada under the Hong Kong pathway after having participated in the pro-democracy movement. His employer told him that it was not because of his political opinions that he was treating the community member in this way, but shortly after that, the man was mistreated to the point where he left his position.

The other case is that of a young woman who was renting a shared house in Toronto. She participated in a pro-democracy protest in 2019 in Canada, brought home posters, flyers from the protest and put them up in her room, which was her space. Her landlord then evicted her. It was shortly after that she found out that this landlord was a core member of the United Front in Canada.

That is a bit of context as to what that means.

Mr. Frank Caputo: Thank you.

I see that I only have 15 seconds, so I will pass the baton, at this point, Mr. Chair.

The Chair: Thank you, Mr. Caputo.

We'll go now to Mr. Bittle for six minutes.

Please go ahead, sir.

Mr. Chris Bittle (St. Catharines, Lib.): Thank you very much, Mr. Chair.

I'll start my questions with Mr. Fadden. I appreciate a fellow lapsed lawyer. There are a few of them around the table on both sides.

I was wondering if you could talk a bit about how this legislation balances providing CSIS with modernized authorities while still ensuring transparency, oversight and independent review.

Mr. Richard Fadden: I think, principally, that the bill maintains quite heavy involvement of the Federal Court in anything being proposed. This is not to be trite, but a friend of mine was reading the bill and said it seemed like an employment opportunity for the Federal Court. I mean, the Federal Court is mentioned a lot in this bill.

If any of you were to ask me if I thought anything could be done to the bill to improve it, I would say to simplify it a bit. However, I understand there are a whole bunch of checks and balances written into it.

Fundamentally, the requirement for CSIS to obtain ministerial authority for the use of datasets and a whole variety of other things, both from the minister and as it goes to the court, will ensure they stay squarely within the law. The authority being given to CSIS to speak more broadly with civil society and the private sector will simply make these issues more understandable to everybody.

One thing that struck me since I've left government is how little people understand about these issues. Therefore, CSIS going out there and talking to the private sector and civil society, and getting feedback in the other direction, broadly speaking, will simply contribute to an environment where greater transparency and accountability will be easier.

I'm not suggesting by this that, all of a sudden, everybody will be cleared to the top-secret level and it will all go away. However, to my mind, there's a pretty careful balancing in the act. Again, if I had my druthers, I'd simplify it a bit, but I understand the checks and balances built into it.

Mr. Chris Bittle: I appreciate simplicity. Despite being a lawyer and the excitement of a make-work project for lawyers, simplicity is generally the best way to go.

With the changes proposed in Bill C-70, how, in your mind, does this compare us with our Five Eyes allies, especially the U.S.?

Mr. Richard Fadden: It brings us very close to where they are.

We have to be careful not to compare directly. Our societies are different and whatnot. Most of our allies have had a registry for some time. Some are country-specific. Some are neutral, as Mr. Caputo suggested. The creation of foreign interference as a crime goes a long way to bringing us in line with our close allies. If it doesn't put us at the forefront, it goes a considerable distance.

To be honest, I think it will lessen the concerns of some of our allies about the caution with which we've approached some of these measures.

● (1735)

Mr. Chris Bittle: Do you see this legislation as having borrowed from other allies of ours?

Mr. Richard Fadden: Yes, I think so. Australia is often drawn upon, because it's very similar, as well as the United Kingdom. The U.S. is a bit harder, because their system of government—as you know—is different.

However, with respect to the United States, the main thing this will accomplish is that it will suggest to them, quite forcefully, that Parliament is taking this very seriously. Simply the creation of crimes and potential penalties of up to life imprisonment sends a pretty powerful message that the country is annoyed.

I think it's mostly the U.K. and Australia, but the United States will likely be pleased we're going down this path.

Mr. Chris Bittle: Thank you so much.

I will turn to Ms. Fung for a moment.

You've been a strong advocate for the creation of a foreign influence transparency and accountability act. Can you inform the committee of your advocacy work, consultations you may have had with the Department of Public Safety and your views on the bill we have in front of us with respect to that?

Ms. Gloria Fung: I was involved in Hong Kong and then ever since I immigrated to Canada. I have been observing, monitoring and collecting data on foreign interference and transnational repression for the last three decades. I have served different NGOs and coalitions, helping all civil society organizations come to a common understanding about the magnitude and depth of foreign interference, especially transnational repression, which significantly impacts the safety and freedom of expression of Canadians on Canadian soil.

Mr. Chris Bittle: How much time do I have, Mr. Chair?

The Chair: You have 30 seconds.

Mr. Chris Bittle: I will say thank you to our witnesses, and I'll pass it along.

Thank you.

[*Translation*]

The Chair: Thank you.

Mr. Villemure, you have the floor for six minutes.

Mr. René Villemure: Thank you very much, Mr. Chair.

I'd like to thank all the witnesses, Ms. Leung, Ms. Fung and Mr. Fadden, for being with us tonight.

Mr. Fadden, I'll start with you, if I may.

Earlier, you mentioned a number of aspects of the bill. Tell us in a few words how we could improve it.

Mr. Richard Fadden: That's a good question, and one that I've been thinking a lot about. I believe that at the end of the day, given where we are today, there's not a lot to do. As I suggested to your colleague, the Federal Court's involvement should be somewhat reduced. I think that would help a little bit.

Fundamentally, I think this is a good bill. It's not a perfect bill, and you will no doubt want to change things in five years, but, compared to the laws of our allies, it's not all that bad.

Mr. René Villemure: Okay.

I had some questions about the commissioner's independence. We understand from reading the bill that the individual will be able to act independently. However, I still have reservations about their accountability to the Department of Public Safety and Emergency Preparedness. Personally, I'd prefer that there be real independence and that, in other words, the individual be appointed after consultation with parliamentarians and the other chamber, and not only after a briefing.

So what's your opinion on the independence of that individual?

Mr. Richard Fadden: I think the commissioner's independence is very important. I'd say that, at the end of the day, there would be some benefit in making the commissioner's position an officer of Parliament, similar to the Auditor General. I don't think the world will end if we do that sort of thing, but, if we continue to maintain the independence of the commissioner as prescribed in the bill, it would really be worth asking them whether it's working properly after 18 months to two years. The easy solution would be to make the commissioner an officer of Parliament.

Mr. René Villemure: When we look at the bill as a whole, it seems that we're looking for transparency, trust and leadership. Without prejudice to an individual, I think it would be easier and independence would be perceived better if there were real independence rather than a facade.

With regard to the registry, we note that foreign principals, as they are called in the bill, will have to register if they engage in influence activities to change public policy. What do you think of the idea of having two-party registration? By that I mean registration of both the foreign principal and the public office holder who is the target, if I can put it that way.

Let's establish that this is not considered an immense burden. It could be as simple as a notification. The idea behind this is that if one person registers and the other does not, an alarm bell will sound somewhere. We're talking about making the registry more effective.

What do you think of that approach?

● (1740)

Mr. Richard Fadden: Honestly, I hadn't thought about it before, but it seems to me that there would certainly be advantages to doing that, since it would encourage even more transparency.

On the other hand, I think unintended consequences should be carefully considered. I'd have to think about that a little bit. I would encourage you to ask your analysts to reflect on potential consequences that we can't think of at the moment.

Mr. René Villemure: We definitely need to think about unintended consequences as well as the red tape we want to try to avoid. The goal is not to make the machine work harder. We're seeking greater transparency.

I had another question for you.

What do you think about imposing some kind of a pause after a political term before joining a foreign entity, that is to say accepting a mandate for a foreign government?

Mr. Richard Fadden: I agree. In my case, when I retired, I couldn't talk to anybody for 12 months. So I think a pause on potential activities with a foreign entity isn't a bad thing at all. In fact, I think it would be a good thing.

Mr. René Villemure: Okay.

Ms. Fung, you were quite an advocate—

[*English*]

Ms. Gloria Fung: Could you ask the question in English?

[*Translation*]

Mr. René Villemure: No, I can't. You have to listen to the interpretation.

I hope you stopped my time, Mr. Chair.

[*English*]

The Chair: We'll add a little time, absolutely.

Mr. René Villemure: It will be an extra five minutes...right?

Some hon. members: Oh, oh!

Mr. René Villemure: You can't blame me for trying.

[*Translation*]

Ms. Fung, you are a known advocate for the creation of a foreign agent registry. Are you satisfied with the proposed registry as it stands?

[*English*]

Ms. Gloria Fung: First of all, I am not a lawyer. However, we have been working with a lot of lawyers with respect to the act. All of our coalition member organizations consider Bill C-70 to be a good and strong bill.

[*Translation*]

Mr. René Villemure: Okay, thank you.

Ms. Leung, I have the same question for you.

[*English*]

Ms. Katherine Leung: I am also not a lawyer, but I am happy with the bill as it stands, currently.

There are amendments I would suggest, but the bill, currently, as it stands, is better than what we have in our Canadian framework. It is a good first step for this government to take to counter foreign interference.

[*Translation*]

Mr. René Villemure: Thank you very much.

Mr. Fadden, I'll go back to you.

You mentioned Australia earlier. Unless I'm mistaken, Australia was one of the first countries to create a registry. However, there haven't been many prosecutions as a result of the registry. It seems to me that the registry has experienced some minor technical difficulties. Is that true?

Mr. Richard Fadden: Yes, I think it is. I don't know the details, but, if I understand correctly, the Australian authorities' intention was simply to provide an additional tool that could help. They didn't intend to create the potential for a large number of lawsuits or things like that. If I remember correctly, the Australian government tabled two or three other acts or bills that created new criminal offences. However, the intent was mainly to give the Australian authorities greater knowledge of the actors, and not necessarily to assign active police powers.

Mr. René Villemure: Ultimately, it was more to register the actors.

Is the registry proposed here better than the Australian one?

Mr. Richard Fadden: I think that at the end of the day, it will largely depend on how it comes into force. As you know, Parliament often prescribes something, and then the coming into force can go one way or the other. I think if the government chooses an active commissioner who really wants to make a big difference, it will be better than what Australia is doing. That could go a long way in addressing this issue.

Mr. René Villemure: Thank you very much.

Ms. Fung, what do you think?

● (1745)

[*English*]

Ms. Gloria Fung: I think the present bill is a strong and good bill. However, because of rapidly evolving foreign influence patterns, it is of utmost importance that our government or the future commission conduct periodic reviews of the act and all corresponding regulations on a regular basis.

We are really competing with time, so we would like to see the bill passed and enacted before the next election is called, in order to protect our national security and democracy.

What I suggest is that you consider reviewing and updating the act and corresponding regulations one to two years after the 2025 election. After that, review the act and regulations once every five years. The rationale for this is that usually, during federal elections, there are very good examples of the patterns, strategies and tactics of foreign interference. What we observe in the next election will give us more data to consider when it comes to improving the act.

[*Translation*]

Mr. René Villemure: Thank you very much.

[*English*]

The Chair: Thank you, sir.

We go now to Mr. MacGregor for six minutes.

Mr. Alistair MacGregor (Cowichan—Malahat—Langford, NDP): Thank you very much, Mr. Chair.

I'd like to echo my colleagues in thanking all the witnesses for being here today to help us through this study.

I don't think you're going to find anyone around this committee table who doesn't understand the importance of the issue before us. That's why, with respect to Bill C-70.... You know, it is quite rare to see a moment of unanimous consent to get a bill through committee this quickly. That being said, it puts a lot of pressure on us committee members because it is a fairly large and consequential bill. We need to do our thorough review of it because it still has to go through the Senate. Of course, if the Senate finds that we didn't do our job properly, they'll amend it and send it back to us, adding to further delay, so we want to make sure we're doing our job properly here.

Mr. Fadden, I'd like to start with you.

I took note of your comment that putting in a registry is not going to stop the clandestine nature of so much foreign interference. Of course, we have various consequential amendments to the Security of Information Act, otherwise known as SOIA. However, putting a law in place is one thing. Making sure we use that law to prosecute and convict is another. I know there's often quite a wide gulf between what is considered intelligence and what is considered evidence—what would stand up in a court of law.

What we haven't talked about a lot is how there are some pretty consequential amendments to the Canada Evidence Act to set up a framework to safeguard sensitive information. I know CSIS has to, by the very nature of its raison d'être, be quite careful with the intelligence it has, because you don't want to get rid of an intelligence source. At the same time, in addition to its detection and disruption activities, we also want to see some prosecutions and convictions happen.

As you look through this bill, are you satisfied that we have the legislative changes in place that can lead us down that path?

Mr. Richard Fadden: I have two related answers.

I think, on the authority of the commissioner to fine people, the standard of proof there will be less than that of the criminal law. It will make it easier for the commissioner to impose fines than it would be if you're accusing somebody under the Criminal Code or the Evidence Act. On that side, it's a good call. There's still the possibility of judicial review, but the commissioner can simply impose the fines at a reasonable level of proof.

There are other crimes, some of which provide for life imprisonment—which is, to be honest, one of the things that surprised me about the bill. You still have the criminal law level of proof, but I don't know if there's a great deal that can be done without dealing with the old intelligence-to-evidence issue. It's an issue we've tried to resolve for the last 20 years.

Having said that, the appointment of a special counsel and all of these other measures will help. Part of the difficulty is that the rules of discovery in this country are among the broadest in the Commonwealth. When we have issues before the criminal or civil courts, everything becomes available. I'm not sure this is the statute to fix that, but I would urge upon you the view that it is a significant issue and a lot of people have tried to resolve it.

As long as you have the criminal level of proof, I think you've done what you can. Again, I would urge you to look at this more generally in the future.

● (1750)

Mr. Alistair MacGregor: Thank you for that.

Ms. Fung, I'd like to turn to you.

I want to go back to your opening statement, where you had some recommendations for amendments. I took note of how you were looking at the existing definition in part 4 of "political or governmental process". You note that it covers, I think, six items, but you want it expanded to include leadership processes, nomination contests and third party advertising.

Could you walk me through that request in a bit more detail to help us understand?

Ms. Gloria Fung: The reason we would like to advocate for an expansion of the definition is that, based on our observations on the ground, foreign interference occurs at every single level of the decision-making process, whether it's within the party or outside the party. For instance, in terms of political party contests, we have witnessed a lot of interference behind the scenes. Of course, many of the proxies are advocates representing foreign countries. They disguise themselves as being a Canadian politician or a Canadian community representative. Even in terms of some of the other appointments, we have seen a lot of unlawful lobbying behind the scenes that involves monetary benefits. Sometimes it can be intangible or in kind.

I would like to provide a broader understanding of where foreign interference could occur. It's really beyond the imagination of most Canadians. However, for people like us who have been observing it on the ground, we have seen a lot more than what is being reported by Canadian media.

The Chair: Thank you, Mr. MacGregor.

That brings our first round to a close. We'll start our second round. We will end this round with Mr. MacGregor, once again.

We go now to Mr. Motz for five minutes.

Mr. Glen Motz (Medicine Hat—Cardston—Warner, CPC): Thank you very much, Chair.

As indicated, thank you to the witnesses for being here today.

I want to start with you, Mr. Fadden.

Does June 2010 ring a bell for you? That's when you first started ringing the alarm bells for this country on foreign interference and how we needed to start taking notice. Do you feel somewhat vindicated?

Mr. Richard Fadden: I guess so, although my intention wasn't to generate quite the excitement that it did. Part of the complication, at the time, was that we were very restricted in what we could say publicly.

I just want to say that I was very careful to say that foreign influence provided some measure of influence. I wasn't arguing that everybody was controlled. However, yes—

Mr. Glen Motz: You're making a statement that you were somewhat confined in what you could say.

Do you think the provisions in this act now give CSIS the powers they need?

Mr. Richard Fadden: I think so, and—

Mr. Glen Motz: Is there something more that should be added?

Mr. Richard Fadden: The challenge here is going to be for CSIS or whoever to set up a process.

To pick an example, one of your next witnesses is from the Business Council of Canada. CSIS is going to want to have a relationship with the Business Council where they can share classified information. What does that mean in practice? Are they going to have to security clear them? Are they going to have a parallel system?

A lot of it will be in the implementation, but the act itself provides a legislative framework that is pretty good.

Mr. Glen Motz: Concerns have been raised about the new commissioner. They're appointed by order in council without any parliamentary approval, according to the act. We've heard from witnesses who have some concerns about that. They figure the commissioner should be independent and have a similar role to the Auditor General, for example.

What are your thoughts on that?

Mr. Richard Fadden: I'll repeat what I said to Mr. Villemure.

The proof will be in the pudding. You could have the current appointment process go forward, and there'll be no problems at all. I think the real issue is perception. We have a tradition in this country of having institutions like commissioners being agents of Parliament regarding privacy and access to information. I could go on.

To my mind, since we're dealing with an act that wants to promote accountability, transparency and independence, there would be an advantage to making this individual an agent of Parliament in much the same mode as the Auditor General.

● (1755)

Mr. Glen Motz: Thank you for that.

Mr. Caputo mentioned something about the country-agnostic approach to the foreign registry. Can you discuss whether you agree or disagree with that approach?

Mr. Richard Fadden: I agree. If you don't have the country-neutral approach, you're going to have to either list the countries in the statute or provide the Governor in Council with the capability of doing that.

Also, if you list them, you're going to—without a shadow of a doubt—significantly affect our relations with those countries. I have a lot of problems with China, but China is there. We have to find a way of dealing with it. Therefore, the neutral approach is much better. It doesn't prevent anybody anywhere from dealing with an issue. On listing specific countries, I'm not the foreign minister, but I think they would tell you that it's not necessary to obtain the objectives of the statute, so don't do it.

Mr. Glen Motz: Ms. Leung, I have a question about the foreign registry for you.

You indicated previously that the foreign agents registry must encompass activities outside of political or governmental processes. Do you think that, as it stands, it's good enough the way it is? Do you have some recommendations for us that can be added, in order to improve this aspect you're concerned about?

Ms. Katherine Leung: Thank you for the question.

My view is that this bill is good as it stands, but amendments can be made to make it better. It is better than what we currently have in our Canadian framework.

Much of foreign interference happens at the grassroots level, as I indicated in my opening remarks. For example, if somebody advocating for pro-democracy movements in Hong Kong is intimidated to the point where they don't feel safe doing that anymore—they no longer write to their MP or go to meetings in Parliament—it stops that individual from participating in Canadian democracy with their charter-protected rights. This is something that has—

Mr. Glen Motz: Let me ask you a question related to that, to some degree.

I asked Mr. Fadden about CSIS's powers to share information. We agree, I think, that it's necessary. Do you think the act goes far enough for the diaspora community in Canada to receive the information it needs to protect itself against foreign influence?

Ms. Katherine Leung: I think that will depend on how the act is executed. I still have a lot of questions regarding the kind of information that will be shared and with whom, and whether it will be sufficient for community groups to counter foreign interference.

I think a lot of the problem with foreign interference at the community level is.... It's not that we don't know it's happening. We're very aware of it. A lot of our community members experience it, people at my organization included. I think the information sharing is great. We should know what we're facing and become proactive against it. However, at the end of the day, it is our safety that we hope this act can protect.

Mr. Glen Motz: Thank you.

The Chair: Thank you, Mr. Motz.

We go now to Ms. O'Connell for five minutes.

Ms. Jennifer O'Connell (Pickering—Uxbridge, Lib.): Thank you, Chair.

Thank you to all the witnesses for being here.

I'll start with you, Ms. Fung.

You mentioned areas where the bill should be expanded to include things like election financing and issues around nominations in leadership races. It's my understanding that this legislation includes the nomination of a political candidate, the holding of an election or referendum, decision-making by public office holders and the proceedings of a legislative body. Certainly, my interpretation of some of the areas we're hearing about is that they would be inclusive of this.

If there's language you think is not making this clear, I'm curious about how we could improve it. When it comes to the financing of campaigns—you mentioned an example of in-kind—that would currently be illegal under the Elections Act if it's not reported. We wouldn't duplicate all of the Election Act financing rules within this law. How can we ensure the language is clear?

I assume that, for example, a leadership race would be included. Where is the language missing that's causing this disconnect?

● (1800)

Ms. Gloria Fung: In order for the act and regulations to be successfully implemented and achieve their original purpose, it is of utmost importance that they contain a good definition of "foreign interference" in various aspects, so that the general public, as well as the enforcement department, can hold foreign agents accountable based upon this.

At the same time, I think public education is also very important. I can look at the reason why Canada has become one of the most badly infiltrated countries by the CCP. There's hardly any meaningful sharing of information from CSIS or the RCMP regarding how Canadians in the general public can protect themselves when certain circumstances happen to them, or how they can report this effectively in a timely manner to the concerned department so that the enforcement department can follow up on it.

It really takes two-way communication to get this act and the regulations effectively implemented.

Ms. Jennifer O'Connell: Thank you. I'm sorry. I have limited time and I'm trying to get questions out to all of the witnesses.

Mr. Fadden, you spoke earlier about the speed at which you hope we move on this, the improvements, and how no piece of legislation is perfect. I acknowledge that. There is also the suggestion about the independence of the commission and having it as a standalone, separate body. In your experience, that in itself would take additional time—having that body set up. Frankly, the space and infrastructure that would be needed in such a sensitive role.... That's not to say that, in the future, this might not be the route of Parliament.

Do you see a concern around speed and how setting up an independent body or commissioner could create challenges versus using some of the infrastructure Public Safety might already be able to build on and support?

Mr. Richard Fadden: I think it will complicate things slightly.

Having said that, if you treat the new commissioner as an agent of Parliament.... What I think the Privy Council Office usually does is treat them like a commission of inquiry initially and develop a structure around them. As I said to your colleagues, I think it would be desirable, but I don't think it's necessary.

If the commissioner finds that, after 18 months or two years, it's not working, I would very much hope you would be willing to consider changes.

Ms. Jennifer O'Connell: Ms. Leung, if I have a bit of time, I want to speak to you about the horrific example you provided to the committee about the individual who was targeted—her place of business, her address and her boyfriend being communicated with. I can see how, up to this point, there is no criminal offence to deal with that type of intimidation. However, through part of this legislation—although it wouldn't require registration if it wasn't specifically deemed political activity—there would be new criminal offences that might possibly be able to deal with that situation. I recognize you've acknowledged that more can be done.

Does the fact that this isn't simply a registry—that there are also criminal offences—help alleviate some of these issues?

Ms. Katherine Leung: Thank you for the question.

Yes, I agree that it is alleviating for the community to know there are now criminal provisions for some of these acts of foreign interference that occur to them.

I would like to point out, however, that discrimination is not part of what is in the bill. As with the examples I raised earlier, it is a tactic used by the Chinese Communist Party and its proxies to target Canadians who are speaking out against human rights violations. That would be an important amendment to add.

● (1805)

The Chair: Thank you, Ms. O'Connell.

[*Translation*]

Mr. Villemure, you have the floor for two and a half minutes.

Mr. René Villemure: Thank you very much, Mr. Chair.

Mr. Fadden, I'm going to come back to you.

The amendment to the Canadian Security Intelligence Service Act will allow CSIS to share information with universities, municipalities, and so on. However, these entities are not in the registry.

Do you believe that entities receiving federal funding, such as universities, researchers, municipalities, and even Crown corporations, should be subject to the registry?

Mr. Richard Fadden: In a word, yes.

Mr. René Villemure: That's as clear as it gets.

Ms. Leung, I'll ask you the same question. You mentioned universities in your opening remarks. Do you think that universities, municipalities and Crown corporations, for example, should also be subject to the registry?

[*English*]

Ms. Katherine Leung: Yes, they should.

[*Translation*]

Mr. René Villemure: Okay. It seems all answers are clear right now.

Mr. Fadden, this entire bill on foreign interference contains no definition of what foreign interference is. How would you define it?

Mr. Richard Fadden: There's probably a good reason for that: It's very hard to define.

I would simply say that it's a foreign entity using non-public methods to force someone in Canada to do or not do something against their will. To some extent, it's simply a form of diplomacy done covertly and through intimidation.

Mr. René Villemure: So we're talking about veiled diplomacy and intimidation. That's interesting.

As we know, something that's not defined doesn't exist. So I find it unfortunate or annoying that an attempt is being made to set parameters that are not defined.

Mr. Richard Fadden: I'd like to add something. After listening to everyone, I note that we've all mentioned the coming into force issues. I may have missed this information when I was reading the bill, but it seems to me that it wouldn't be unreasonable for the bill to include a provision requiring the Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs to report annually on the general operation of this act. Otherwise, information specific to the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, the commissioner, the Chief Electoral Officer and so on will be scattered all over. The minister should be asked to gather the information once a year, for the benefit of the public and Parliament. That would be helpful.

Mr. René Villemure: That's interesting. You're right, CSIS and the RCMP are creatures that do not tend to talk to each other.

There is also talk of a review every five years. Personally, I think that's a good thing. However, we need only think of the Privacy Act, which came into force in 1983 and has not been reviewed, or the Canadian Security Intelligence Service Act, which came into force in 1984 and was reviewed in 1990. Regardless of their political stripes, governments don't really make a habit of reviewing legislation every five years.

What could be done to ensure that the review is done?

Mr. Richard Fadden: It would simply be a matter of saying that the act will no longer be valid if no review is done. This method is sometimes used by the Americans. It's like an atomic bomb, but something like this could be done. We could say that if the review doesn't take place, that would mean a few provisions of the act are no longer valid, or we could provide for a penalty, so to speak.

Mr. René Villemure: I've never heard of that idea. That's fascinating.

Thank you very much.

[*English*]

The Chair: We will now go to Mr. MacGregor.

You have two and a half minutes.

Mr. Alistair MacGregor: Thanks, Mr. Chair.

Ms. Fung, I'd like to continue with you.

There have been a lot of comments made about the urgency of getting this act in place quickly, given the seriousness of the issue. The consequential amendments to both the Security of Information Act and the Canada Evidence Act say they come into force on the 60th day after this act receives royal assent, so that's a pretty tight timeline. In part 4, though, regarding the new registry, it is up to the Governor in Council to fix a day. We have the parts that deal with the more clandestine nature of foreign interference coming into place relatively quickly, and we'll see how well federal agencies can make use of those new tools. However, the new registry is very much up in the air.

You made mentioned in your opening comments having some kind of commission to oversee how this act comes into force. Do you want that set up as a parallel to cabinet? I want to understand the mechanics of how you would like to see this work.

● (1810)

Ms. Gloria Fung: Actually, this suggestion is based on the Australian model. They set up an independent commission to oversee and monitor the implementation of all the foreign interference-related measures. I think, in Canada, we require such an independent commission to be set up. It should be totally independent of the government so as to maintain that neutrality and fairness in managing all the foreign interference cases.

Mr. Alistair MacGregor: Thank you.

You also talked about having a review fairly soon after the next federal election—in order to see how these new legislative provisions act in practice—and then the formal review five years thereafter.

Is that what you want to see us focus on?

Ms. Gloria Fung: Exactly, yes.

Mr. Alistair MacGregor: Okay.

I'd like to end by thanking you all. I really appreciate your testimony today.

Thank you.

The Chair: Thank you, Mr. MacGregor.

Thank you, witnesses, for joining us today. Your testimony is most helpful to our work. Thank you also for making yourselves available on such short notice. As you know, we're under very short timelines to pass this bill. Of course, you understand the importance of doing so, so thank you.

We will now suspend and bring in the next panel.

Thank you, all.

● (1810)

_____(Pause)_____

● (1817)

The Chair: I call this meeting back to order.

I'd like to welcome our witnesses for the second hour. We have appearing today as individuals, Mr. Christian Leuprecht, professor, Royal Military College of Canada; and Ms. Emmanuelle Rheault, attorney. From the Business Council of Canada, we have Trevor Neiman, vice-president, policy and legal counsel.

I would like to thank you all for your participation today in our meeting and your flexibility in being able to appear so quickly.

I will now invite Mr. Leuprecht to make an opening statement of up to five minutes.

Please go ahead, sir.

[*Translation*]

Prof. Christian Leuprecht (Professor, Royal Military College of Canada, As an Individual): Thank you, Mr. Chair.

Good evening, ladies and gentlemen.

[*English*]

I bring extensive comparative expertise on matters of national security and intelligence across allied and partner democracies, including my book, *Intelligence as Democratic Statecraft: Accountability and Governance of Civil-Intelligence Relations Across the Five Eyes Security Community*.

[*Translation*]

The Gathering Storm is the title of volume 1 of Winston Churchill's five-volume history of World War II. That title is apt to recall once again. The fall and dissolution of the Soviet Union introduced a sense that liberal democracy was ascendent and spreading.

More than thirty years later, around the globe, democracy and democracies have been in retreat. They are coming under growing duress from confident authoritarian regimes and other enemies of democracy who use hybrid warfare activities that leverage grey-zone tactics to undermine democratic institutions, political processes, economic prosperity and social harmony.

[*English*]

Here in Canada, recent reports by NSIRA and the NSICOP expose vast and significant vulnerabilities across a broad scale, including the systematic infiltration of Canada's political, economic and social institutions by adversarial actors who are prepared to go as far as alleged treasonous behaviour. These reportedly include some of your own colleagues.

It could hardly be more ironic that two review entities created by this government to improve the accountability of agencies effectively end up holding the government to account for having been naive and negligent on intelligence and national security.

Make no mistake. The now well and widely documented activities by hostile actors pose an existential threat to Canada's security, prosperity and democratic way of life. For too long, this government and its predecessors have taken democracy for granted. Instead, democracy needs to be defended.

The fragility of Canadian democracy is on full display, yet the bill shows neither courage nor ambition. It amounts to a minimalist approach. It represents the absolute minimum the government would have to do anyway, but only once its hand was forced.

The bill does not update the national security threats to Canada in section 2 of the CSIS Act, which dates from 1984. It fails to remove section 16, which is proving a growing impediment to CSIS to fulfill its mandate. It introduces a minimalist five-year review of the CSIS Act only, instead of the entire security and intelligence framework and posture, as Australia does.

Although it amends the Security of Information Act, notably removing the threshold of harm to Canadian interests, it forgoes other important updates such as the harms provision in section 3.

Why the bill would not grant the minister the ability to designate a list of states and actors of concern as part of the foreign influence transparency registry, as the U.K. does, is beyond me, unless the aim is to avoid ensnaring any one political party's sycophants, lawyers and accountants that make a pretty good living off their hostile state patrons.

This bill does not give FINTRAC explicit enforcement powers to track and seize assets and transactions that are being used to enable foreign interference. There are no amendments to the CBSA Act to deem inadmissible persons suspected of engaging in foreign interference in Canada or another allied country. Also, the bill fails to reform the RCMP with the aim of making it more targeted and effective at meeting its federal mandates.

● (1820)

[*Translation*]

Just this week during question period the Prime Minister claimed that his government would do whatever it takes to keep Canadians safe.

[*English*]

The Chair: Excuse me, sir, but could you stay back from the microphone a bit? It's a problem for the interpreters.

[*Translation*]

Prof. Christian Leuprecht: Okay. I'm on my last sentence, Mr. Chair.

Yet, this bill barely sets minimum thresholds to protect Canadian democracy and make its defence more proactive, robust and resilient against highly persistent adversaries.

Thank you.

[*English*]

The Chair: Thank you, sir.

I will now invite Ms. Rheault to make an opening statement of up to five minutes.

Please go ahead.

[*Translation*]

Ms. Emmanuelle Rheault (Attorney, As an Individual): Thank you, Mr. Chair.

Members of the committee, I want to begin by thanking you for the opportunity to speak to you.

I have been a lawyer for 10 years and I exclusively practise criminal law, on the defence side. The Criminal Code and certain sections of the Canada Evidence Act are therefore part of my daily life. Therefore, I will focus most of my remarks on these two acts, but I will make a brief incursion into the Security of Information Act to talk about some of the provisions you wish to add to the Criminal Code.

First, I have several observations to make with respect to the proposed amendments to the sabotage offence, which is currently dealt with in section 52 of the Criminal Code. Some efforts are commendable, but many others are alarming.

First of all, as far as I know, the offence of sabotage does not exist in Great Britain. In the United States, federal laws restrict the scope of the offence. In New Zealand, sabotage is also a much more limited offence than what is intended by Bill C-70.

Subsection 52(1) of the current Criminal Code defines the offence of sabotage as "a prohibited act for a purpose prejudicial to …". In all transparency, I say to the committee that I think the way this paragraph is formulated right now is incomprehensible. The proposed amendment is therefore very commendable and welcomed by the law clerks, because the proposed wording is much clearer. In addition, proposed subsection 52(5), which provides an exception for certain groups, is an advantage compared to the current version of the Criminal Code. However, I feel the clarification is too restrictive.

The proposed new subsections 52(1) and 52(2) are much more problematic.

Subsection 52(1) that the bill proposes to add to the Criminal Code creates a new sabotage offence in relation to essential infrastructure. First of all, I want to say that this is far too broad. Under proposed subsection 52.1(1)(c), the offence applies to anyone who intends to "cause a serious risk to the health or safety of the public or any segment of the public". However, the concept of "segment of the public" could be interpreted as meaning two individuals. So it wouldn't have to be the majority of the population. In addition, the bill is far too broad when it talks about a serious risk to safety. I say this because the broader the provisions are, the less they will stand up to the test of the courts as far as constitutionality and Canadian criminal law are concerned.

Next, proposed subsection 52.1(2) defines essential infrastructure. However, I'd like to point out that this definition includes facilities or systems belonging to private companies. If we push the interpretation of this proposed subsection, the facilities or systems of a private video game company like Ubisoft could be considered essential infrastructure, since they are information and communication technology infrastructure. So you're not only targeting public entities, and even companies owned by the federal government or a provincial government, but also private companies, which is very problematic.

Furthermore, the concept of economic well-being, which is added in proposed subsection 52.1(2), is also problematic because it's very broad. It's not restrictive enough and, to my knowledge, it's not defined anywhere in the Criminal Code.

In addition, the safeguard that's added by proposed subsection 52.1(5), which excludes from the definition of the offence acts committed in the course of advocacy, protest or dissent, is not sufficiently restrictive, because it's conditional on the lack of intent to cause any of the harms referred to in proposed paragraphs 52.1(1)(a) to (c). In New Zealand, for example, the exception applies purely and simply to acts committed as part of a protest or as part of a claim, with no conditions attached. Proposed subsection 52.1(5) could lead the courts to interpret it very broadly, even speculatively, in certain situations.

● (1825)

Another thing I note in the proposed provisions is the concept of mischief. The offence of mischief already exists in section 430 of the Criminal Code. However, you want to include in these new provisions almost any type of mischief committed for one of the purposes intended. As a result, mischief will become an even more serious offence, with a maximum sentence of 10 years' imprisonment, rather than two years, or five or 10 years in some cases. You want to make that offence much more serious.

As for proposed section 52.2, there are some issues. I'm thinking in particular of the definition of "device" in proposed subsection 52.2(3). The term "device" is not limited to computer programs. This term is defined in a number of places in the Criminal Code, and the definition includes many more things than computer devices. Devices can be explosives or weapons, for example. That could be a problem in court.

[*English*]

The Chair: Could you wrap it up, please?

[*Translation*]

Ms. Emmanuelle Rheault: Yes. I'll wrap up very quickly.

With respect to proposed section 52.3, which deals with the consent of the Attorney General, if you want the Government of Canada to retain some jurisdiction over those provisions, you would have to add some missing words.

● (1830)

[*English*]

The Chair: Thank you.

I now invite Mr. Neiman to make an opening statement of up to five minutes.

Mr. Trevor Neiman (Vice-President, Policy, and Legal Counsel, Business Council of Canada): Mr. Chair and committee members, thank you for the invitation to take part in your study of Bill C-70.

We're an organization representing Canada's most innovative and successful businesses, so I will restrict my comments today to the portion of the bill that has the most direct relevance to the Canadian private sector. That is subclause 34(3), which seeks to amend the Canadian Security Intelligence Service Act to enable CSIS to disclose threat intelligence to stakeholders outside the Government of Canada for the express purpose of increasing their awareness and resiliency against foreign interference.

However, before commenting on this clause, I want to make clear that Canada's business community is broadly supportive of Bill C-70. From the establishment of a foreign influence transparency regime to the creation of updated offences for attacks directed against essential infrastructure, this urgently needed bill will help protect Canadians' lives and livelihoods by providing our government with the tools it needs to better protect our economy and society.

I'll start my substantive remarks by noting that, while the current discussion in Canada surrounding foreign interference has been rightly focused on the integrity of our democratic processes and the safety and security of targeted ethnic and cultural groups, it is important for us all to acknowledge that state actors actively target all aspects of Canadian society to advance their strategic interests. This includes the Canadian economy.

Indeed, in an era of growing geopolitical rivalry, in which supply chains, infrastructure networks and technological innovation increasingly determine strategic advantage, Canadian businesses are often the primary target of our adversaries. This should concern all Canadians. Economic security threats are not abstract, nor do they exist in a vacuum. These threats target the critical infrastructure needed to heat and power our homes. They target the supply chains that provide our families with low-cost medicine and food. They target the intellectual property that creates good jobs and pays our bills. In short, these threats put Canadians' very safety, security and prosperity at risk.

To be sure, Canadian businesses and governments invest billions each year to keep Canadians safe from these and related economic attacks. However, if we want to be truly effective in protecting our way of life, we must replace our independent efforts with collective action. Key to building this partnership is the sharing of threat intelligence. Unlike the domestic security agencies of Canada's Five Eyes partners, such as the United States' FBI or the United Kingdom's MI5—which possess modern authorities that allow them to share detailed threat intelligence with their respective business communities—CSIS is presently prohibited from sharing all but the most generalized information with the Canadian private sector. This represents a significant gap in Canada's defences.

Despite CSIS having both the knowledge and expertise to help companies withstand growing threats, its outdated legislation means Canadian businesses are left fending for themselves. It is for this reason that the Business Council strongly supports subclause 34(3).

With new threat-sharing authorities, CSIS could communicate more specific and tangible information with Canadian companies. This would give business leaders a clear understanding of the growing threat and the protective measures that could be taken to better safeguard their employees and customers, as well as the communities in which they operate.

The use of these new authorities could also benefit the Government of Canada by helping CSIS build greater trust with the Canadian private sector. This would encourage Canadian business leaders to share more with Ottawa about the threats they're seeing on the ground, which would better inform government policy as well as improve CSIS's ability to respond to emerging threats.

Of course, the granting of any new authorities must be consistent with the values we share in our democratic society, including respect for individuals' rights and freedoms. On this front, we are very pleased to see that the Government of Canada has incorporated rigorous standards and safeguards into subclause 34(3), such as those ensuring that individual disclosures protect Canadians' privacy interests.

Before concluding, I want to stress the need for urgency. The Business Council of Canada agrees with many lawmakers that the protections contained within Bill C-70 must be put in place before the next general election. The preservation of our democratic system is of utmost importance.

However, I will add that, when it comes to strengthening the resiliency of our economy, Canada is falling well behind our allies. This exposes everyday Canadians to unnecessary risks. By failing to move in lockstep with our closest allies, we risk being perceived as a weak link. This could jeopardize our country's relationship with our closest allies, especially the United States, at a pivotal moment when the global order is being reshaped and partnerships matter most.

I'll conclude by noting that Bill C-70 is just one of many economic security reforms that must be undertaken urgently to protect Canadians. As a priority, the Business Council urges the Government of Canada to complement subclause 34(3) with a formalized threat exchange to securely receive and disseminate Bill C-70's threat intelligence broadly across the Canadian economy. This and nearly 40 other much-needed reforms are included in the Business Council's recent report, “Economic Security is National Security”. That report is available on our website.

Thank you for the opportunity to speak. I look forward to your questions.

The Chair: Thank you, sir.

We'll now start our questions off with Mr. Shipley.

Go ahead for six minutes, please.

Mr. Doug Shipley (Barrie—Springwater—Oro-Medonte, CPC): Thank you, Chair.

Thank you to all the witnesses for being here this evening. I was going to say “today”, but it really is evening now.

I'd like to start with Mr. Leuprecht, if I could.

Mr. Leuprecht, you were very passionate in your opening remarks. I was listening quite intently. You mentioned systemic infiltration at the very beginning, and the words “treasonous behaviour”.

Could you expand on where you think this systemic infiltration is?

● (1835)

Prof. Christian Leuprecht: It's not what I think in terms of systemic infiltration. We have plenty of evidence at the municipal level in terms of infiltration. We have ample evidence in terms of research security within our universities. We have evidence at the provincial level of government, and we have evidence that includes charges laid within private and public sector institutions in this country, including of course the government, just this past week, forcing two entities in Vancouver...that engaged effectively in what it appears to be the illicit transfer of dual-use, anti-drone technology to a hostile actor.

I can send you a long list, but the public record on this is extensive.

Mr. Doug Shipley: I appreciate that. That's a good start. It's a little disheartening to hear, but at least we're doing something now to try to correct it a bit.

I'd like to stick with you, sir, if I could, because we've heard different perspectives in favour and opposed to Bill C-70's country-agnostic approach to the foreign registry list. I think in the beginning you mentioned that you definitely see a benefit to listing countries. Expand on why you see that being a benefit, and you mentioned persons too.

Prof. Christian Leuprecht: Yes, I figure that this is probably going to be one of the more critical decisions and one of the more controversial decisions, and I can see both sides, including Director Fadden's case for not, I think, giving the minister the option.

Much of what this legislation will ultimately do, rather than sort of prosecuting people, is about drawing red lines and establishing clearly what sort of behaviour is and is not acceptable in this country. This is what much of the Criminal Code, for instance, also does. It lays out the rules of the road.

The problem that, for instance, universities have when it comes to research security—where the government made a similar choice of listing only public sector entities but not private sector entities, all of whom have Communist Party structures within them that pose the exact same threat that public sector entities engaged in intelligence and defence do—is that, for universities, for private sector actors, it doesn't provide a reference point based on which they can then engage in higher scrutiny. Without government providing that reference point, it will become relatively easy to accuse universities of randomly, for instance, scapegoating or whatnot.

I think more direction from government is required for those players who do not have the classified access that federal government entities do, including on the research security side, for instance, where I chair the Ontario research fund advisory board and where we know there are significant challenges around what is being funded.

Mr. Doug Shipley: I would like to move to Mr. Neiman.

Mr. Neiman, in a letter to the previous minister of public safety, the Business Council of Canada stated that you wanted to see, and I'll quote this, amendments to the Canadian Security Intelligence Service Act to allow CSIS to proactively share threat intelligence with employers where it is in the public interest and subject to all necessary safeguards and oversights.

Can you speak to these new information-sharing powers in C-70, and if they meet your requirements?

Mr. Trevor Neiman: Thank you for the question.

As I mentioned in my opening remarks, CSIS is presently prohibited by its governing statute from sharing all but the most generalized information with the business community. This is because, for lack of a better word, the federal government is CSIS's exclusive client. Therefore, the private sector can't get access to information. Academic institutions can't get access to information, and neither can municipalities or indigenous governments.

The only exception to this general rule is once a national security threat materializes into an imminent national security event. At that point, if CSIS can satisfy some very stringent legal requirements, it can use its threat reduction mandate to alert a specific company about a specific threat.

This means of sharing information is very much a legislative workaround. These threat reduction powers were not designed for information sharing, so this process is deeply flawed. The main reason it's flawed is that, as I mentioned, there's a very strict legal requirement that must be met before information can be shared. That means these powers are rarely used.

Second of all, the regime is reactive in nature. Threat information can only be disclosed after a material and immediate threat has emerged. At that point, that information provides very little utility for a business, as its options to mediate or mitigate the threat are very few. Moreover, as I mentioned, the disclosure can only be made to a specific business that has been targeted.

If the goal is to strengthen the overall resiliency of the Canadian economy, the current set of tools is inadequate. That's why the Business Council has been very supportive of the adoption of subclause 34(3), which allows CSIS to proactively share threat intelligence with a broader set of stakeholders, including the business community.

You mentioned that the Business Council, as a part of advocating for these changes, has been very clear from the start that any new amendments must be reflective of the values that we share in our society, including the protection of individuals' rights and freedoms. Therefore, we were very pleased to see—and I can get into this more in another question—that there are a number of checks and balances to protect individuals' and corporations' privacy, as well as accountability mechanisms.

For instance, if there's a disclosure of personal information or corporate information that is otherwise prohibited, that information needs to be shared with NSIRA. There also needs to be ministerial authority granted, and the minister, in that case, must be of the view that the disclosure is essential to the public interest and that the benefit of the disclosure to Canada's national security clearly outweighs the privacy implications.

● (1840)

The Chair: Thank you, Mr. Shipley.

We'll go now to Mr. MacDonald for six minutes, please.

Mr. Heath MacDonald (Malpeque, Lib.): Thank you.

Thank you to the witnesses for being here.

Mr. Neiman, I'm going to continue by following up on Mr. Shipley's questions. You're with the Business Council of Canada. About two weeks ago, I had the Insurance Bureau of Canada in, and we discussed the increasing risk that small and medium-sized enterprises are facing, possibly through cyber-attacks, which can lead to foreign interference based on whatever content they're in possession of.

It was interesting, because they were asking us how they deal with it. How are companies dealing with something like this now?

Are they buying insurance policies on cyber-attacks, which will likely lead to foreign interference if, for example, they hold certain information that could be very essential to them, to an individual, to a community or to a community group or something?

Mr. Trevor Neiman: Thank you for the question.

The Business Council represents approximately 170 of Canada's largest, most successful businesses, so I can't speak to the specifics of the challenges facing small and medium-sized businesses, but what I can say is that small and medium-sized businesses are very much a part of the supply chains of large businesses. Large businesses are quite concerned about the security posture of small businesses, because they can often be an indirect route to attack large businesses.

There needs to be much more done in this space in terms of government support, and Bill C-26 is one way to help in that regard. The private sector itself is also willing to step up and do more. For instance, our members are very much committed to working with their supply chains to build up their baseline resiliency, including through education, capacity building and relationship brokering, including working jointly with Canada's security and intelligence community, with agencies like CSIS, the CSE and the RCMP.

Mr. Heath MacDonald: This committee just did a review of Bill C-26. During that testimony, we heard that there were about 5.2 million cyber-attacks in four months in 2023, from September to December. I think that's correct. Of those, 62% targeted critical infrastructure.

In our testimony during our last meeting, Michel Juneau stated that “86% of our national infrastructure is either owned or operated by the private sector”. It's going to become a very serious issue, or it already is a very serious issue. We may not even be aware of what's transpiring underneath. What's the best way to go about delivering that message and ensuring that there are safeguards in place within this bill?

You talked a bit about 40 items that you guys did a report on. Can you talk a bit about them, and give us a couple of examples and their relevance?

Mr. Trevor Neiman: The Business Council did put out a recent report, last September, that set out a pretty comprehensive set of reforms that we believe the Government of Canada should adopt to address the most glaring gaps in Canada's economic security posture. We were very happy to see that a number of them were incorporated into this bill, particularly clause 34, which allows for increased information sharing.

As I mentioned at the beginning of my remarks, we've also supported the foreign influence transparency registry, as well as the new sabotage offences as they relate to the protection of essential infrastructure.

At the same time, as I mentioned in my opening remarks, we think this bill should move forward on an expedited basis, so we wouldn't want to make significant changes to the bill that would slow down that process. However, we would hope that the government would try to bring in some of the additional changes that we suggested.

You mentioned critical infrastructure and I just want to provide a short commentary on that. The Business Council is very supportive of the amendments to the sabotage provisions. We note that the current provisions in the Criminal Code date from 1951. They have not been updated since then.

Obviously, the threat environment has changed drastically since then. We see more and more that our adversaries have an increased intent and willingness to target and undermine our critical infrastructure. Those are the systems that allow Canadians to heat and power their homes, communicate with their loved ones across this vast nation and get their goods to and from international markets. Disruption to those systems would be absolutely devastating to Canadian society. I don't think I exaggerate much when I say that a substantial disruption to our central infrastructure could put millions of Canadians' lives, security and prosperity at risk. We think that the amendments are a good step forward.

We're also very happy to see that the government has included some safeguards in there, including making exceptions for work stoppages related to labour disputes, as well as exceptions for individuals who are legitimately engaged in advocacy, dissent and protest, as well as the requirement for a proceeding to be brought before the Attorney General to provide consent.

We think that those protections there provide the right balance between protecting Canada's economic and national security and, at the same time, making sure that these provisions are respectful to individual Canadians' rights and freedoms.

● (1845)

Mr. Heath MacDonald: Mr. Leuprecht, if I didn't ask you a question, our good friend, Mr. Desserud, would be upset with me when I return to Prince Edward Island, so I'm going to ask a quick question.

You didn't use this word, but you talked a little bit about contextualization of the agnostic list. You were somewhat against that in your preamble.

Before the chair cuts us off, can you quickly give me your main reason for that?

Prof. Christian Leuprecht: I think entities need a clear signal.

If you're a university or a private sector company, to be fair, you now need to.... Australia ran into this problem, where all foreign actors need to be treated equally. If you're a foreign visitor to a university from Germany or you're a foreign visitor from some hostile state, the university cannot treat the risk assessment differently. It means that you cannot deploy the very scarce resources you have in a targeted fashion, so it's just giving the minister the option.

The other advantage is that it allows the government to negotiate. If it gets indirect threats from a hostile state actor, the government can now indirectly signal that, if they're going to treat us like that, we might end up listing their particular country and maybe two can play at this game.

The Chair: Thank you.

[*Translation*]

Mr. Villemure, you have the floor for six minutes.

Mr. René Villemure: Thank you very much, Mr. Chair.

Thank you to the witnesses, Mr. Neiman, Professor Leuprecht and Ms. Rheault.

Ms. Rheault, as George Orwell said, the fewer the words, the less people are tempted to think. Earlier, you told us that it was too restrictive, that words were missing or that there were too many words. I would like to give you an opportunity to further explain that.

Ms. Emmanuelle Rheault: Let's simply look at section 52.3, which the bill proposes to add to the Criminal Code and which deals with the consent of the Attorney General. It says that "No proceeding for an offence under subsection 52(1), 52.1(1) or 52.2(1)", that is, sabotage offences, "shall be instituted without the Attorney General's consent". The Criminal Code defines the Attorney General as the provinces, the Director of Criminal and Penal Prosecutions in Quebec and the Attorney General. If Ottawa wishes to retain its discretion, it should say "Attorney General of Canada". There is language like that in section 773 of the Criminal Code to allow the federal government to retain its discretion with respect to certain sections of the Criminal Code that are more sensitive internationally, whether against other countries or against other individuals.

There is also the exception set out in proposed subsection 52(5). According to the bill, an act of sabotage is permitted when a person participates in advocacy, protest or dissent, but does not intend to cause any of the harms referred to in paragraphs 52(1)(a) to (c). It's extremely broad. We're still referring to the first paragraph of this clause, which is a problem in the first place. With respect to the latter part of the exception, as I mentioned, I haven't seen that in New Zealand, for example. I've only seen it in the current bill. In my opinion, this wording would create problems, because its scope is much too broad.

● (1850)

Mr. René Villemure: Do you have any comments on the proposed amendments to the CSIS Act?

Ms. Emmanuelle Rheault: You're probably referring to the Security of Information Act. I'm sorry, I may not know all the terms as well as some of your guests.

I have limited myself to the sections of this act that are incorporated into the Criminal Code. For example, I took a closer look at proposed subsection 20.4(1) that the bill proposes to add to this act. It talks about influencing a political or governmental process. It reads: "Every person commits an indictable offence who, at the direction of … a foreign entity …" Once again, this section is very general. Yes, the term "foreign entity" is defined in section 2 of the Security of Information Act, but there are other definitions. I can quickly see examples that probably correspond to what you have in mind. I hear what the other guests are saying and I hear some of the concerns being expressed. Given the way this provision is worded, influence groups could be covered by proposed section 20.4 without necessarily being tied to the government.

Once again, the scope of this section is very broad and, since we're talking about a criminal offence here, the constitutionality of this section could quickly be called into question.

Mr. René Villemure: Thank you very much.

Professor Leuprecht, you gave impassioned testimony. You said that it was the minimum required to live together, no less.

You've listed a lot of things, but if you had to prioritize them, what do you think are the main missing or faulty things?

Prof. Christian Leuprecht: I'd say that, in general, the federal government has faced challenges in sharing information with stakeholders effectively and efficiently, as well as in a timely manner. We've seen this in the recent reports of committees dealing with accounting.

[*English*]

We know this from FINTRAC. FINTRAC has trouble sharing the right information. We know this from CSIS. We've noticed that we have it within agencies and among agencies.

The way the bill enables the ability to share information within government and with external stakeholders.... We have some very good models—the Canadian Cyber Threat Exchange, for instance, and the Canadian centre for cybersecurity, where I think there are probably significant synergies with CSIS in terms of sharing threat actor information. Some entities have cracked it precisely because the government has enabled information-sharing provisions.

I think we are just too restrictive.

[*Translation*]

Mr. René Villemure: At the outset, you mentioned a lack of courage and ambition. That's quite striking.

The bill states that there will be a review every five years. I can name you a series of laws that must be reviewed every five years, but they aren't reviewed. We're trying to create an incentive, as it were.

A little earlier, a witness suggested including a provision that says if there's no review after five years, the act is no longer valid. That would be akin to a nuclear bomb.

Would you have a suggestion for us to ensure that the act is reviewed every five years?

Prof. Christian Leuprecht: For example, the Australians require that a report be produced every five years providing an overview of the intelligence and national security architecture. The individual who is tasked with that has quite a bit of latitude. The report is quite long, but it generally focuses on a particular area where they are trying to suggest improvements.

We're talking about laws that are not very visible to the public or to members of Parliament, and they are also very complex. As the witness indicated, it has very significant consequences on the protection of civil life and human rights. Given that the global security environment is changing so quickly and we have laws with definitions from 1951 and 1984, we need a mechanism that allows members of Parliament to act more effectively and in a way that's better adapted to today's realities.

● (1855)

Mr. René Villemure: Thank you very much.

The Chair: Thank you, Mr. Villemure.

[*English*]

We'll go now to Mr. MacGregor for six minutes.

Mr. Alistair MacGregor: Thank you very much, Mr. Chair.

Thank you to all three of you for joining us today.

Professor Leuprecht, I want to revisit the issue of part 4 being country-agnostic, because I want to present to you a hypothetical situation. Of course, the government of the day is guided by different political leanings, and it may view certain countries in different lights from its competitors in the House of Commons.

I'm wondering about a situation in terms of listing a country. Could there not be the potential of the government of the day's trade interests colliding with the country's national security interests? It's a very political decision to list a country. Does that not come with some pitfalls because that's essentially a political decision? There could be other things guiding a government's decision rather than the purely national security interests of Canada. Is that not a danger?

Prof. Christian Leuprecht: We had exactly that situation very recently in terms of the reimposition of certain visa requirements on Mexican nationals to Canada, where there was a vigorous internal debate on precisely this sort of trade-off. Ultimately, this gives the Minister of Foreign Affairs a stake on both sides, because the Minister of Foreign Affairs can ultimately make the trade argument, and the Minister of Foreign Affairs would also have the opportunity to list a country.

The listing regime is important, because we've been very poor in the last 20 years in anticipating the evolution of the international security environment. In a case of a rapid degradation of the international security environment, where the government feels it might need to take fairly aggressive, rapid measures to protect Canadians, Canadian interests and Canadian institutions, this is an important tool that we will—not “may” but “will”—regret within your and my lifetimes if it is not inserted into the bill.

Mr. Alistair MacGregor: In the interest of transparency, would we not also have an interest to know how some of our closest friends and allies are influencing our political processes?

Prof. Christian Leuprecht: Yes, but they don't need to resort to covert, clandestine, coercive—

Mr. Alistair MacGregor: That wouldn't be covered by a registry. Clandestine wouldn't be covered by the registry.

Prof. Christian Leuprecht: Our closest allies have plenty of legal mechanisms. For me, the primary purpose of the registry is to lower the evidentiary threshold for investigations, because, in many cases, it is very difficult for security and criminal intelligence to reach the current threshold as defined in law in Canada. With the registry, you are now giving the agencies a much lower threshold for the purpose of investigation. That, I think, is the primary purpose.

Mr. Alistair MacGregor: Okay. Thank you for that.

I also want to recognize that, from your comments, you see Bill C-70 as a bare minimum, and you did mention other statutes that you wish could have been enacted.

We're limited by what's before us. We can't go beyond the scope of the bill, but in the amendments to the CSIS Act, you did make mention of the fact that a lot more could have been done with section 16. However, are you happy with what the government is proposing here in its amendment to section 16 as an addition? Do you see any improvements that we can make as a committee?

Prof. Christian Leuprecht: I think what I was hoping to signal is that there's nothing in this bill that you can really reasonably strip out of the bill. This is the minimum threshold. That's the primary signal that I was hoping to send.

I appreciate that the government did have the guts to tackle section 16, because that is inherently a long-standing controversy. Just going there shows that there's some willingness to engage constructively on some key matters that might subsequently come up in other bills for further amendment.

● (1900)

Mr. Alistair MacGregor: Thank you.

Ms. Rheault, I'd like to turn to you and your expertise in criminal law.

Of course, there are some significant amendments to the Security of Information Act, with significant offences and punishments, pretty much all of them involving life imprisonment. I know that other offences involving life imprisonment can be treason, mutiny and things like that.

On the offences listed in these new amendments to the SOIA, do you think the punishments match how serious the offences are?

[*Translation*]

Ms. Emmanuelle Rheault: You have to understand that, basically, I'm a defence lawyer. So my practice is always guided by the humanistic approach I take with my clients.

Of course, traditionally, offences punishable by life imprisonment involve violence. These are offences that pose a certain risk to someone's life or a very high risk to their physical integrity, or terrorism offences.

Certainly, when I read the bill, I find life sentences somewhat disproportionate to the offences I see. The 14-year maximum penalty under the Criminal Code is widely used for many offences of similar gravity.

[*English*]

The Chair: Thank you, Mr. MacGregor.

We will start our second round with Mr. Lloyd for five minutes and end it with Mr. MacGregor.

Mr. Dane Lloyd (Sturgeon River—Parkland, CPC): Thank you, Mr. Chair.

Thank you to the witnesses.

It's good to be back at committee. My wife and I welcomed our third child three weeks ago, so I've been taking a bit of time.

Some hon. members: Hear, hear!

Mr. Dane Lloyd: Thanks to my colleagues for supporting me during that time.

I'm going to talk about an issue that I don't think gets talked about enough. It's not really controversial.

In proposed section 31, we have the five-year mandatory parliamentary review. In this legislation, different from the NSICOP Act, there's also a report that needs to be given to Parliament within one year of that review. We're currently almost two years overdue for the report on the NSICOP Act. I'm concerned that, if this legislation goes forward as is, a future Parliament.... It might not be until two Parliaments from now, given that there's a four-year mandate if there's a majority government. It might not be until two Parliaments from now when this critical legislation gets reviewed.

Dr. Leuprecht, I wonder if you have any suggestions or recommendations about shortening that five-year review period, or about whether we should put additional language in there to ensure this review takes precedence at committee, rather than just being shuttled off whenever another piece of legislation or an important issue comes up—just like the NSICOP Act review has been delayed.

Thank you.

Prof. Christian Leuprecht: We live in a democracy and it's ultimately up to the government of the day and our elected representatives to decide what the priorities are and how they're going to tackle them. I think the Prime Minister has also made that very clear with intelligence and national security. There are, of course, other examples, such as the Proceeds of Crime (Money Laundering) and Terrorism Financing Act, where the review is long overdue.

The first thing my students always want to do is change legislation. I always tell them that changing legislation is probably the single hardest thing you could possibly think of doing. Think of a tax incentive, policy or regulation—whatever. Don't try to change legislation, because you might spend a decade on it. You have to look for a politically opportune moment to bring in legislation such as this, Bill C-51 or others. Nonetheless, it keeps the attention on the matter. Otherwise, it just drops off the radar and nobody will pay attention to it until we run into some sort of crisis.

If we think that the first and foremost obligation of the state is the safety and security of the citizens and its political, economic and societal institutions, we need to have a mechanism to at least try to keep our eye on the ball. That's what I think these reviews do.

Mr. Dane Lloyd: Do you feel that the mechanism that currently exists...? This bill has mechanisms similar to what we've seen—you know, a five-year review—but the language is slightly different. The language in this bill says “must”, but the language in previous legislation says the committee “is to”. I'm not sure that gives any more clarity on whether or not committees will be mandated. It will be up to, as you said, whether or not the government at the time places a high priority on it. Clearly, this is a high priority, and it's been something that's been neglected for far too long in this country.

Would you recommend expediting those reviews to less than five years? Also, would you recommend language that makes it stronger and puts the emphasis on this needing to take priority at the same level as legislation, which usually takes priority at committees?

● (1905)

Prof. Christian Leuprecht: When the current government came to power, I think it had 85 reviews on the go at the same time. My concern is that we are too specific with the reviews, and it is generating too many reviews. We would probably be better off with either a national security intelligence review or, within the remit of this committee, a five-year review on countering foreign interference and the mechanisms at our disposal—what we did five years ago, what's working, what's not working and what could work better—rather than trying to limit our swim lane so precisely to one agency and one particular act.

Mr. Dane Lloyd: Thank you.

There was some discussion with the last panel discussing whether this needs to be an independent officer of Parliament.

Did you have any feedback on the pros and cons? What would be your recommendation on that matter?

Prof. Christian Leuprecht: I've written on this publicly. I'm not a big fan of the proliferation of independent officers of Parliament, in part because I think reporting to the executive actually gets us more timely, more efficient and, in many cases, more effective action. I have a lot of faith in whatever executive is in power to take action.

An independent officer of Parliament will help with transparency. I do not believe that an independent officer of Parliament will help get things done or will help to get it done faster, better or more efficiently.

I think the bureaucrats are very well intentioned...or an independent outside judge or some combination thereof, as Australia has done in the past with people who understand the system. I'm not sure you'll get something better out of an independent officer of Parliament, but I'm married so I know I'm wrong all the time.

The Chair: Thank you, Mr. Lloyd

We go now to Mrs. Zahid.

Go ahead, please, for five minutes.

Mrs. Salma Zahid (Scarborough Centre, Lib.): Thank you, Chair.

Thanks to all the witnesses. My first question is for Madame Rheault.

This legislation takes a country-agnostic approach instead of creating a list of the so-called problematic countries it would apply to. A list-based approach would be hard to update with changing and emerging threats. It would be open to political influence and considerations, and potentially stigmatize innocent members of the diaspora communities.

Can you outline the risks of a list-based approach? Why is it important to not unfairly stigmatize diaspora communities, which are often at the greatest risk from foreign interference and threats?

[*Translation*]

Ms. Emmanuelle Rheault: Based on my knowledge of Bill C-70, the list you mentioned would not have any consequences on the Criminal Code or the Canada Evidence Act, logically, since the Criminal Code applies to offences committed in Canada, with certain exceptions. In addition, it focuses primarily on individuals, not entities. You can't prosecute a country under the Criminal Code.

As for the rest, I apologize, but it's somewhat outside my area of expertise.

[*English*]

Mrs. Salma Zahid: Mr. Leuprecht, would you like to comment on that?

Prof. Christian Leuprecht: You heard the witnesses before us. The concern that I hear from my friends, colleagues and in public isn't so much about stigmatization. It is about foreign repression in their lives by hostile state actors.

I have written publicly about my concern that all this talk about stigmatization risks playing into the narrative that our hostile state actors are using to impede our ability to pass precisely the legislation that not only will keep our diaspora communities safe from foreign repression, but will protect the freedom of expression in this country.

● (1910)

Mrs. Salma Zahid: Thank you.

My next question is again for Madame Rheault.

This legislation adds the word “intimidation” to section 20 of the Security of Information Act:

> Every person commits an offence who, at the direction of, for the benefit of or in association with, a foreign entity or a terrorist group, induces or attempts to induce, by intimidation, threat or violence, any person to do anything or to cause anything to be done.

I agree with the spirit here, but do you feel that there needs to be clarity on just what constitutes intimidation in this context?

[*Translation*]

Ms. Emmanuelle Rheault: Certainly, threats and violence are defined concepts in criminal law, whereas intimidation is not. If Parliament does not define it, it opens the door to the courts, which will then have the opportunity to define it themselves and have the definition go all the way up to the Supreme Court.

So yes, it would be better to clearly and accurately define what Parliament considers to be intimidation.

[*English*]

Mrs. Salma Zahid: Thank you.

My next question is for Mr. Neiman.

Can you please explain how the threat sharing with U.K. companies has worked out? Are there any lessons to be learned from that?

Mr. Trevor Neiman: I'm not intimately familiar with how the U.K. operationalizes the threat intelligence; however, at the highest level, I do understand that amongst the Five Eyes nations, Canada is an outlier in terms of the lack of authorities our domestic security agency has to share threat intelligence with the business community.

We just spent a week in the United Kingdom last month, and we met with the U.K.'s domestic security agency, MI5. They have a special body that is designed purely for the purpose of collaboration with the private sector. They told us quite specifically that they have the authorities that CSIS is now seeking through clause 34. They tell us that those authorities are working effectively and have allowed them to build very robust partnerships, and this has been starting to build increased resiliency across the economy.

We've also had an opportunity to recently travel to Washington, D.C., to meet with the office of the private sector of the Federal Bureau of Investigation. They have similar authorities.

The model we looked at in the United States that has worked quite effectively is something called the Domestic Security Alliance Council, which is a joint partnership between 700 strategically important U.S. companies, the Department of Homeland Security and the FBI. Through two-way exchanges of information between the United States government and U.S. corporations, they're able to advance the United States' mission of protecting that country's national and economic security while at the same time helping U.S. corporations better protect their employees, their customers and the communities in which they operate.

By participating in this organization, both the public and private sectors gain access to senior leaders within those two sectors. The private sector gains tailored access to threat intelligence specific to their sector, and then the public and private sectors also gain access to a very large and robust network of senior security executives, who can work together jointly to solve security issues and to share best practices.

We believe that Canada is really well positioned, CSIS in particular, the Department of Public Safety and the business community, to establish a body similar to DSAC to operationalize the authorities contained within clause 34.

If we're looking for examples to operationalize what's contemplated in the legislation, the FBI and the DHS's Domestic Security Alliance Council would be a model we should look for.

Mrs. Salma Zahid: Thank you.

Prof. Christian Leuprecht: There's a competitive issue here in terms of prosperity. Why would you invest in Canada if you know you can get better threat intelligence in the United States, the United Kingdom or Australia?

The Chair: Thank you.

[*Translation*]

Mr. Villemure, you have the floor for two and a half minutes.

Mr. René Villemure: Thank you, Mr. Chair.

Ms. Rheault, I was startled by a comment my colleague made. I'm asking you to weigh in on the dilemma. As a great linguist once said, translating is betraying.

Section 31(1) of the proposed bill deals with the review of the act. It says that “a comprehensive review of this Act and its operation must be undertaken by the committee”. The French version reads “*est entrepris*”. Honestly, the phrases “must be undertaken” and “*est entrepris*” are not of equal strength, semantically speaking.

● (1915)

Ms. Emmanuelle Rheault: That's right.

Mr. René Villemure: Does this happen on a regular basis?

Ms. Emmanuelle Rheault: In criminal law, it's not uncommon for the English and French versions not to be identical, or even for there to be a difference between them. According to the principles and protections of the Canadian Charter of Rights and Freedoms, the most favourable version for the accused prevails, but only in criminal law.

Mr. René Villemure: If, in a bill like Bill C-70, I find four significant semantic differences between the French and English versions, should I be concerned?

Ms. Emmanuelle Rheault: The simple answer is yes.

Mr. René Villemure: In that case, I think we'll have to do a more in-depth review, because just after my colleague's comment, I found four.

Would you like to use the minute and a half I have left to tell us more?

Ms. Emmanuelle Rheault: I'll be brief.

Actually, I'd like to apologize for the question Ms. Zahid asked me. Intimidation is covered in section 423 of the Criminal Code. However, this clause details the techniques that can be used and that constitute intimidation. To answer Ms. Zahid's question, I'd say that I'm not sure to what extent the description of intimidation in the Criminal Code could apply to another piece of legislation.

In closing, I would also like to talk about the Canada Evidence Act. As set out in the bill, leave to counter-appeal under subsection 37.1(1) of the Canada Evidence Act is being removed. Since it is required that the accused be previously found guilty to complain about the interim decision, they will only be able to do so at the end of the trial. Your predecessors realized how important these decisions are and decided that it was an interim appeal. I see no reason anywhere in the bill for removing this interim appeal.

Mr. René Villemure: I'm nevertheless concerned to see so many omissions and oversights, so much lack of precision and differences in translation in this bill, which we are having to study at lightning speed. So I will take just five seconds to express my concern, quite simply.

Thank you very much.

The Chair: Thank you, Mr. Villemure.

[*English*]

Mr. MacGregor, please bring us home. You have two and a half minutes.

Mr. Alistair MacGregor: Thank you, Mr. Chair.

Ms. Rheault, I want to talk to you about the Criminal Code amendments in this bill. This bill largely follows the theme of combatting foreign interference. You then get to the section about the Criminal Code, and it just seems to have been thrown in there. It doesn't seem to flow with the rest of the bill.

I was trying to follow your remarks about the sections you found problematic and too broad. In the time I have left, where do you think we, as a committee, should focus if we're considering amendments to fix the problems you addressed?

Should it be the sections that clarify for greater certainty and provide an out for someone so that they're not committing an offence if they're involved in advocacy, protest or dissent? Is that probably the best focus for us? I'd like to hear your thoughts.

Ms. Emmanuelle Rheault: That's one of the best things to focus on, especially in the last three lines of that paragraph. Proposed section 52.1 needs, in my humble opinion, to be looked over again by the committee. It's the one that adds a section to the Criminal Code. It's more problematic. It's too large. It doesn't focus, I think, on what the committee wants to focus on, and it would create a section whereby a lot of infractions would be thrown in, disregarding the purpose of that bill.

Mr. Alistair MacGregor: Okay.

Ms. Emmanuelle Rheault: Also, with proposed section 52.3, if the the committee wants the federal government to stay in control of those articles, 52.3 needs to be changed by adding “Attorney General of Canada”.

Otherwise, you would lose all control. The provinces would get control of those.

Mr. Alistair MacGregor: Okay. I appreciate that.

I think I have only a few seconds left, so I'll just thank all three of you for helping guide us through this study. I appreciate it.

The Chair: Thank you, Mr. MacGregor.

Thank you to all of our witnesses for appearing today, especially on short notice. It's been most helpful.

With that, we will adjourn. Thank you all.

To the committee, I'll see you tomorrow morning at 8:15.