HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 093 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, January 30, 2018

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Tuesday, January 30, 2018

● (1100)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Ladies and gentlemen, may we bring this meeting to order, please?

This is the 93rd meeting of the Standing Committee on Public Safety and National Security. For the first hour we have, from the office of the Communications Security Establishment commissioner, the Honourable Jean-Pierre Plouffe. Accompanying him are Monsieur Gérard Normand and Mr. William Galbraith.

As you are a person who appears frequently before this committee, I'll let you go forward and make your opening presentation, and then, as you know, members will want to ask questions afterwards. We look forward to your presentation, Mr. Plouffe.

Thank you.

Hon. Jean-Pierre Plouffe (Commissioner, Office of the Communications Security Establishment Commissioner): Thank you, Chair.

[*Translation*]

Mr. Chair, honourable members, I am pleased to appear before this committee again, this time on the subject of Bill C-59. I am accompanied by William Galbraith, the executive director of my office, and by Gérard Normand, special legal advisor.

I have been the Communications Security Establishment (CSE) Commissioner for over four years. I am responsible for reviewing the activities of CSE, primarily to determine whether they complied with the law. This naturally includes everything to do with protecting the privacy of Canadians and persons in Canada. I am a retired judge of the Superior Court of Québec and of the Court Martial Appeal Court of Canada. As I like to often say when I appear before you:

[*English*]

I'm a young 75.

[*Translation*]

The phrase retired judge means that you cannot expect someone 40 or 50 years old. In order to retire, we have to be at least 69 or 70. That explains my somewhat advanced years.

The law requires the CSE Commissioner to be a supernumerary judge, meaning a judge who is on the bench part-time, or a retired judge of a superior court. My current term expires in mid-October this year, in 2018.

[*English*]

However, once Bill C-59 receives royal assent and part 2 enters into force, my role will change into a completely—and I emphasize completely—new function for intelligence accountability in Canada.

Indeed, the CSE commissioner will no longer perform after-the-fact review of CSE activities. The intelligence commissioner, or the IC if you prefer, will have a quasi-judicial role, of which the first part is reviewing and the second is approving authorizations issued by ministers for certain activities of CSE and CSIS before those activities can be conducted.

This specific role will be to determine whether the minister's conclusion to authorize the activity was reasonable. The test I have to apply is reasonability. In essence, this is similar to the function performed by a court of law when undertaking what we call “a judicial review”. This is, in my view, a critical role, intended to provide a quasi-judicial review of an intelligence agency's activities that may have charter and/or privacy implications.

● (1105)

[*Translation*]

Part 2 of Bill C-59, the Intelligence Commissioner Act, expressly provides for the transition of the CSE Commissioner into the new role of Intelligence Commissioner. The functions of post-facto review of CSE activities that I now perform will be assumed by the new National Security and Intelligence Review Agency, also proposed in Bill C-59.

[*English*]

This bill also requires the intelligence commissioner to be a retired judge of a superior court, which is appropriate, in my view, given the quasi-judicial function of this new position. However, this bill does not include the possibility of appointing a supernumerary judge, as is the case now with the National Defence Act for the CSE commissioner. I believe this bill should retain the possibility of a supernumerary judge, in part to ensure a broader pool of potential candidates. I was a supernumerary judge when appointed CSE commissioner four years ago, and a short time afterward, I fully retired as a judge.

The problem is the following. The pool of candidates for this job, the new intelligence commissioner, is very narrow. You must find a retired judge who has the proper background to be appointed—for example, a background in security matters or in national defence matters. The pool is very narrow. That's why I'm suggesting that we should keep in the bill what we have in the National Defence Act with regard to the appointment of the intelligence commissioner. In other words, a supernumerary judge should be appointed as the IC and then would retire maybe a few months later. It would be a transitory measure. I can see that if a sitting judge remained the intelligence commissioner for years, he might have some problems with conflicts of interest and what have you. I think for transition purposes, it might be very useful.

Previously, I submitted to this committee a written copy of substantive proposals for amendments to Bill C-59. Those comments were sent to your chair on December 6, 2017. I am also submitting today lists containing additional substantive and technical proposals that I sent to Minister Goodale and Minister Sajjan. I think you have a copy of those comments before you. I will highlight a number of these in my remarks.

[*Translation*]

The importance of the process the government has chosen to follow for this bill is, as stated by Minister Goodale, to allow new ideas and alternative suggestions to be presented before second reading in the House.

[*English*]

In this context, I will speak to changes I am proposing for three parts of the bill: part 2, the intelligence commissioner act; part 3, the CSE act; and part 4, amendments to the CSIS Act. While I am of the view that the proposed legislation is generally sound and that it addresses most of the recommendations made by me and my predecessors to amend part V.1 of the National Defence Act. I am also of the view, following in-depth analysis and discussions with officials and agencies directly involved, that certain amendments should be proposed. Among my substantive proposals, I will describe seven that I consider the most important.

First, I believe the intelligence commissioner should be involved in approving authorizations for CSE active cyber and defensive cyber operations which may also implicate privacy interests. Some commentators have remarked that this is a new and very broad mandate for CSE and that it is too permissive. By comparison, the CSIS Act requires CSIS to go before a federal court judge, in some instances, to have a warrant issued for similar activities.

● (1110)

[*Translation*]

Second, as the bill is written currently, the Intelligence Commissioner does not approve the minister's decision to extend the validity of a CSE foreign intelligence or cybersecurity authorization for an additional year. I believe the commissioner should be involved, given that he was involved in approving the initial authorization. Otherwise, in effect, the authorization would be for two years. However, this is not what the bill proposes. It proposes that this type of authorization is valid for a maximum of one year. If the minister granted extensions almost automatically without the commissioner being involved, the duration could end up being two years, instead of the one year provided for in the act.

[*English*]

Third, emergency authorizations for CSE issued by the minister for purposes of foreign intelligence or cybersecurity should also be reviewed by the commissioner immediately after they have been issued. This would be similar to the approach that exists in the Investigatory Powers Act in the United Kingdom. Under the U.K. legislation, the period of validity for these emergency authorizations is five days, the same validity period as in Bill C-59. However, in the U.K., the Judicial Commissioner must review and approve these authorizations within that time frame.

The Chair: Unfortunately, we're going to have to.... Are you able to wind up your final four points in less than 30 seconds?

Hon. Jean-Pierre Plouffe: If you give me maybe two or three minutes, I think I can do it.

The Chair: My only problem with that is that when I give you two or three minutes, then I get grief from all of my colleagues. I can give you a minute and you can wind it up.

Hon. Jean-Pierre Plouffe: I'll try to finish the proposal, because I know one of the questions will be on those particular points.

The Chair: Okay.

Hon. Jean-Pierre Plouffe: I've been warned.

The Chair: Okay. Thank you.

[*Translation*]

Hon. Jean-Pierre Plouffe: Fourth, I also believe that the commissioner should have the authority, when engaged in the review and approval process, to request clarifications about the information provided to him that was considered by the minister in making a decision. Without this ability, the commissioner, if not clear on some of the information, may well have no option but to determine that the minister’s conclusion to authorize an activity was not reasonable.

[*English*]

Fifth, I believe the commissioner should be able to conditionally approve an authorization, subject to the minister agreeing to incorporate a condition identified by the commissioner.

I have only two left.

[*Translation*]

Sixth, the Intelligence Commissioner should prepare a public annual report to the Prime Minister, to be tabled in both chambers of Parliament. This would emphasize the independence of the commissioner and help enhance transparency and public trust.

[*English*]

Seventh and finally, I believe a regulation-making authority should be inserted into the proposed intelligence commissioner act for carrying out the purposes and provisions of the act.

[*Translation*]

Thank you for this opportunity to appear before you today. We would be pleased to answer your questions.

Thank you, Mr. Chair.

[*English*]

The Chair: Thank you for your thoughtfulness and preparation.

I'm going to turn now to Mr. Spengemann for seven minutes.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): I don't think that's the agreed-upon order, Mr. Chair.

The Chair: You must have a list different from mine.

It's Ms. Dabrusin, then. Thank you.

Ms. Julie Dabrusin (Toronto—Danforth, Lib.): Thank you very much for that presentation. It was very interesting, because when I talked to people in my community about what they wanted to see in our national security regime, one of the things was better oversight. That was a big focus. Hearing a bit more about your ideas and about how this bill goes towards that end is very helpful for me, and I appreciate that.

I was looking at a report prepared by the Citizen Lab at the Munk School of Global Affairs. It had several different recommendations in respect of the Information Commissioner and oversight. I was wondering, given that you've been involved in the system a little bit and understand how it works, if you might be able to give me some insights as to the workability of some of these.

One of them I think touches on one of the last points that you were raising and might fit in with it. They recommend that an emergency authorization under proposed section 41 be reviewed *ex post* by the intelligence commissioner. How does that fit in with your suggestions? Do you think that works well with what you've proposed today?

● (1115)

Hon. Jean-Pierre Plouffe: I'll ask the general counsel to answer. I did touch upon that subject matter in my introductory remarks—

Ms. Julie Dabrusin: Yes.

Hon. Jean-Pierre Plouffe: —but I'll ask Normand to reply to it.

Mr. Gérard Normand (Special Legal Advisor, Office of the Communications Security Establishment Commissioner): Essentially, they're not the level of detail that we provided, because we based it on the U.K. legislation, but the idea is the same. Basically it would enable the minister to make a decision in exigent circumstances, but that would be reviewed within five days by the commissioner. Then, depending on his review, depending on the decision, there would be an impact or not on the ongoing authorization. In a sense, it's basically the same thing that we're proposing.

Ms. Julie Dabrusin: It's the same idea. Perfect.

The other suggestion was to require written reasons when approving an authorization, not just when an authorization is refused. What would you think about that as a suggestion?

Hon. Jean-Pierre Plouffe: The bill actually provides that if the intelligence commissioner turns down the request submitted to him by the minister—or his conclusion, I should say—then he has to give reasons. On the other hand, if he approves the authorization issued by the minister, he doesn't have to provide reasons.

As a retired judge, I don't mind providing reasons. I've been doing that all my life. When you issue a judgment of any sort, you provide reasons. I'm not against the suggestion that even if I approve the conclusion reached by the minister with regard to the issuance of an authorization, the commissioner should provide some reasons. Obviously those reasons would be rather short compared to when the conclusions of the minister are judged unreasonable by the IC, but I'm not against that suggestion.

Mr. Gérard Normand: Actually, especially in the first few years, I think reasons would be helpful in enabling the agencies to see where the commissioner is coming from in the way of thinking within the reasonableness process.

Ms. Julie Dabrusin: Thank you for that.

You mentioned in your remarks that you saw the Information Commissioner being involved in authorizations for active and for defensive cyber operations. I was wondering if you could elaborate. How would you see that role? How would that look?

Hon. Jean-Pierre Plouffe: This is a complex matter. Those are complex provisions within the bill, those provisions concerning the active and defensive cyber operations.

Ms. Julie Dabrusin: I have the bill in front of me, so if you want to—

Hon. Jean-Pierre Plouffe: In essence, it was explained to me that the IC will not have a role to play because, unlike when information is collected in active and defensive cyber operations, no collection will occur. They suggest that there are no charter or privacy rights that would be affected by these techniques that will be used outside of Canada. This is with regard to the CSE.

Unfortunately, I don't necessarily agree with that view, and neither does the Department of Justice, which is the legal adviser to the government. I'm quoting from the justice department's legal opinion, page 9 of a document entitled “Charter Statement - Bill C-59”. It's short, but it explains my position. I quote:

> The provisions authorizing active cyber operations would not by definition engage any Charter rights or freedoms. However, specific activities authorized under this scheme could potentially engage rights or freedoms. The considerations that support the consistency of this aspect of the mandate with the Charter are very similar to those supporting the consistency of the defensive cyber operations mandate. One difference is the distinct purpose of active cyber operations, which would be to further the government’s compelling objectives in relation to Canada’s international affairs, defence or security.

Although no information is collected, people's private communications will be disrupted, influenced, and interfered with, and this could very well, in my view, affect Canadians in the same way as inadvertently collecting information on Canadians abroad. In my view, there should be no difference between collecting communications of Canadians abroad and disrupting and interfering with communications of Canadians abroad, so—

● (1120)

Ms. Julie Dabrusin: The only reason I'm jumping in is that I know I'm about to run out of time—

Hon. Jean-Pierre Plouffe: This is my answer—

Ms. Julie Dabrusin: I just wanted to know what you would want to see as the Information Commissioner's role, then.

Hon. Jean-Pierre Plouffe: I think the IC should be involved with regard to those operations.

Mr. Gérard Normand: If I may just add, the role would be a similar one. Reviewing and approving would be the same scheme as the other authorizations, basically. You would look at the facts presented to ministers and you would look at the factors in the statute that would be required for the decision to be made and ensure that the facts supported that.

The Chair: I can see that I'm going to have difficulty reining in time, here. It's an important discussion.

Before I turn it over to Mr. Motz next, you were quoting from a.... I wonder if you could make that available to the committee, if it's not already available to the committee? Is it in a bulletin?

Hon. Jean-Pierre Plouffe: I'll leave it with you afterwards.

The Chair: Okay. Thank you for that. I appreciate it.

Mr. Motz, you have seven minutes.

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

Thank you, Commissioner and your team, for being here today.

I understand that proposed section 61 of the proposed Communications Security Establishment Act provides cabinet the authority to change parts of the act, commonly known as the Henry VIII clause. Proposed section 61—

Hon. Jean-Pierre Plouffe: This is the CSE act, proposed section 61?

Mr. Glen Motz: —provides cabinet the authority to change parts of that act. It goes back centuries.

Why is it necessary for cabinet to have the ability to take on the role of Parliament?

A follow-up to that question is that if this is what Parliament is doing, if this is what cabinet is going to do, shouldn't some of the things that they want to change—the legislation, the parameters for regulations, and anything about that—be put in regulations so that if...? We know that the cyberworld changes quickly, and if there is a need to add some flexibility in the legislation, wouldn't it be better, rather than giving a cabinet that authority, to put it in the regulations to allow that?

What are your thoughts on that, sir?

Hon. Jean-Pierre Plouffe: The reason I made that suggestion with regard to the possibility for the Governor in Council to make regulations is the following. When the bill has passed and has received royal assent, if you look in one of the provisions—I don't recall the exact section number—it says that the minister concerned must provide to the IC, the intelligence commissioner, "all information" that he had before him.

This is not defined. We don't know what exactly the legislator is talking about. Are we talking about briefings? Are we talking about reports? We don't know. In my view, a regulation could be written whereby the IC's office, with regard to the minister's office, would lay down what would be required to be transferred to the IC with regard to this "all information".

This is similar, for those who have a legal background, to the rules of practice of a court of law. We talk about procedure. We talk about, in this particular case, what this "all information" should be, and I think this adds flexibility to the bill.

● (1125)

[*Translation*]

The "nuts and bolts", if you will.

[*English*]

Since the IC has a quasi-judicial role, you need rules of practice that are equivalent.

Mr. Glen Motz: If I understand you correctly, you're suggesting that there might be some change necessary to proposed section 61 to provide those parameters, if you will, to provide clarity in the regulations and not provide a provision for cabinet to have that sole authority. Am I hearing you correctly?

Hon. Jean-Pierre Plouffe: Yes.

Mr. Glen Motz: Thank you.

One of the things that I'm curious about is, based on your experience in this role and your past experience on the bench, your thoughts on the utility of offensive cyber-attacks. I know that's something that some people have some concerns about, but if we're talking about our national security and public safety, what are your personal thoughts on the act allowing offensive cyber-attacks or cyber operations?

Hon. Jean-Pierre Plouffe: I'm not trying to evade your question, but I think it's a question that is more appropriate for CSE.

All I can say, though, is that this is a very broad mandate for CSE, and I think it's reasonable for commentators, legislators like you, to raise the point and ask questions. In essence, do we need that type of technique with regard to security? If so, how should it be limited? Should we have oversight with regard to those powers?

As I say, it's very broad.

Mr. Glen Motz: You mentioned CSIS. How do you think the coordination of your work between CSE and CSIS will occur to ensure both agencies don't overlap in your effort to prevent attacks? How do you coordinate those things now, and how do you see this act enhancing that, moving forward?

Hon. Jean-Pierre Plouffe: As you may realize, the first task of the IC would be to review and approve the authorizations that are issued by the respective ministers. That's the first thing.

On the other hand—and again, it's similar to what a court of law would do—you need expert advice at times. That's why, in my office, I need experts—in other words, people who know what CSIS is doing and also people who know what CSE is doing—to advise me accordingly. It's a bit like when you're sitting as a judge and you have expert witnesses who come to court to advise you, because the judge is not an expert.

In my office we are restructuring right now, and I do have those types of experts in my office.

Mr. Glen Motz: Thank you, sir.

I have one last question. I have limited time.

You've already given us seven recommendations that you'd like to see, and you have some technical proposals as well. In an ideal world, given some flexibility in your role, what would you take out of the bill and what would you add that you maybe haven't had the flexibility to mention?

Hon. Jean-Pierre Plouffe: In my introductory remarks, I made seven substantive suggestions, and those are contained in the document that I sent to the chair. I did underline five or six of those in my introductory remarks. Would you like me to repeat them?

Mr. Glen Motz: No.

I have one last question.

How do you think we do currently in comparison to our Five Eyes partners in combatting cyber-threats? Will Bill C-59 make us even more nimble to deal with them?

The Chair: That's an extremely broad question, and we've already run out of time. Can you do it in 15 seconds?

● (1130)

Mr. Gérard Normand: Yes.

Essentially, we had a look at the legislation of four other countries. Our understanding, subject to the review of others, is that it's mainly aimed at defence activities and at providing assistance to other agencies. Proposed section 31 provides for the ability of CSE to do things on their own and to disrupt, for the purpose of international affairs, defence, or security, but not necessarily in an assistance role or a defence role, which they can do as well. There seems to be something different with respect to the other countries.

The Chair: Thank you, Mr. Motz.

[*Translation*]

Mr. Dubé, you have seven minutes.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Mr. Chair.

Gentlemen, thank you for being here today.

I have one question, but I have the feeling that you will not want to be too definite with your answer.

There was not a lot of time for this bill. That is not a criticism, on the contrary, but it explains why extremely major changes are proposed.

Your suggestions mainly affect three different parts of the bill: parts 2, 3 and 4. In your opinion, would it have been appropriate for the parts that create new structures and vastly expand the authority of the CSE to be dealt with in a separate bill, instead of being included in a 130-page bill with a number of objectives?

Hon. Jean-Pierre Plouffe: Once again, that is up to the government to decide.

I know that, at one point, there were discussions to decide whether we should divide up the bill and study its various parts separately. The government decided that was not necessary. So the bill has to be studied in its entirety. That makes it more complicated, of course, but it does not stop us from making suggestions and proposing the amendments we feel are needed.

Mr. Matthew Dubé: Of course.

In the answers you have provided to some of my colleagues, you discussed the mandate of the CSE. Ms. Bossenmaier, the CSE chief, appeared before us, and I asked her specific questions on the proposed subclause 24(1), the first paragraph of which presents exceptions for cases of publicly available information. This concerns us, as do the paragraphs that follow. Ms. Bossenmaier mentioned that the mandate of the CSE essentially affects foreign entities, and not Canadians. I would like to ask you a number of questions about that.

First, is the mandate legal or is it understood as such by the CSE?

Also, these types of exceptions are included in the bill, but we really have yet to hear why. For example, it reads: “The Minister may, by order, designate any…electronic information or information infrastructures as…of importance to the Government of Canada.” All these matters are unclear, and we are not able to justify the scope.

I have touched on several questions, some of them in the form of comments. I would simply like to know your point of view on these subjects.

What is the mandate of the CSE? Is the bill widening its scope without us being able to justify the concrete reasons for doing so and the intended objective?

Hon. Jean-Pierre Plouffe: The mandate of the CSE is not to target Canadians or people in Canada. Under the legislation, the CSE must target foreign entities. This does not change. If by chance the CSE decided to target Canadians, it would be illegal. In my opinion, this is what gives the oversight agencies their importance, whether it is the proposed new committee or the intelligence commissioner, although I think his title should be “judicial commissioner of intelligence”, since he plays a quasi-judicial role. I am proposing this amendment, by the way.

It is necessary to consider a set of data to ensure that the role of our intelligence agencies, whose activities are partly secret, is scrutinized by monitoring agencies worthy of the name. That way, public trust in these agencies is maintained.

Mr. Matthew Dubé: Although the mandate isn't to target Canadians, some aspects of the bill are worrying in this regard. I'm going to address several points quickly.

Subclause 22(1) states:

> 22(1) The Minister may, by order, designate any electronic information, any information infrastructures or any class of electronic information or information infrastructures as electronic information or information infrastructures—as the case may be—of importance to the Government of Canada.

Although the target is foreign entities, the designated infrastructure may be in a global ecosystem and be used by Canadians.

The other thing I want to draw your attention to and get your comments on is the proposed section 23, which talks specifically about the targeting exceptions for Canadians. However, it says in proposed subsection 24(1):

> 24(1) Despite subsections 23(1) and (2), the Establishment may carry out any of the following activities in furtherance of its mandate:
>
> (a) acquiring, using, analyzing … publicly available information;

The following is stated further on:

> Information acquired incidentally
>
> (4) The Establishment may acquire information relating to a Canadian or a person in Canada incidentally in the course of carrying out activities under an authorization issued under subsection 27(1), 28(1) or (2) or 41(1).

Despite the mandate and what is understood by the agency, there are a lot of loopholes. Canadians could be affected.

Given the exchange of information between the agencies and with our allies, particularly the Americans, and the absence of a prescription regarding the length of time the data will be retained, don't you think that risks might be incurred?

● (1135)

Hon. Jean-Pierre Plouffe: The executive director or the legal adviser will surely be able to answer, but just before that, I would like to clarify one point. At present—and this will still be the case if the bill is passed—if the CSE is engaging in targeting abroad and incidentally intercepts conversations or communications from Canadians, it must obtain authorization each time from the minister, who must personally authorize these activities. In addition, remember that the authorization, once granted by the minister, is reviewed by the oversight agencies. We want to ensure that everything is done in accordance with the legislation. This means that parameters are set to ensure that the activities of the agencies are legal and do not violate the privacy of Canadians.

From your question, I can see that the public is having a little difficulty in identifying certain aspects, because some of the activities are secret. That goes without saying, since these are intelligence agencies.

[*English*]

The Chair: Thank you, Mr. Dubé.

Go ahead, Monsieur Picard.

[*Translation*]

Mr. Michel Picard (Montarville, Lib.): Thank you, Mr. Chair.

I find this fascinating. I will move directly to my questions because I want to give our guests more time to expand on the subject.

First of all, I would like a few clarifications. In your—

Hon. Jean-Pierre Plouffe: I'm sorry, Mr. Picard, but I can't hear you very well. It may be age-related; I'm not sure.

Mr. Michel Picard: I can tell you that you don't seem 75.

In your sixth proposal, you state that the Commissioner of Intelligence should prepare a public annual report for the Prime Minister. I'm not convinced, and I would like some clarification.

In your current role, is the annual report issued to Parliament or to the Prime Minister?

Hon. Jean-Pierre Plouffe: Currently, the commissioner of the CSE that I am produces an annual report through the Minister of National Defence, which, by law, must be tabled in both Houses of Parliament within a legislated time.

Given that, according to the new bill, it is the Prime Minister who recommends the appointment of the Intelligence Commissioner, I propose that a public report be submitted every year and that, in the same way as the Minister of National Defence does currently, the Prime Minister undertakes, by law, to table it before both Houses. In my opinion, there must be a public report. The bill does not mention anything about it.

What is the purpose of a public report? First, it emphasizes the commissioner's independence. Second, it is a matter of public trust. Not only the public, but parliamentarians and commentators, too, want to know what the Intelligence Commissioner is doing.

Mr. Michel Picard: Since you are intervening, the version submitted to the Prime Minister will have to be amended to make it public, because of the sometimes very sensitive nature of the information.

Hon. Jean-Pierre Plouffe: The commissioner is the one who does this work. That would be done in advance, much like we do today. In other words, we could produce two reports, in theory: a classified report for the Prime Minister or the committee of parliamentarians, and a public report for the general public.

I think this would be essential for ensuring public trust and accountability.

● (1140)

Mr. Michel Picard: I would like to go back to another point on which the debate has been rather limited. Your second proposal concerns the famous one-year extension of the validity period of a foreign intelligence authorization.

If the activity has already been approved by you at the start and it's just a matter of validation, why is it necessary to ask for permission again for an ongoing activity? Have you taken into account the fact that circumstances are likely to change during the year and that it might make you change your mind, perhaps even to the point where you would not have allowed the mission from the outset if you had known a number of things?

Hon. Jean-Pierre Plouffe: My philosophy is this: if the Intelligence Commissioner needs to approve the initial application, which is valid for one year, I don't see why he shouldn't be involved a year later when an application for renewal of the validity period is made.

Why is an application for renewal made a year later? It must be presumed that new facts have arisen, since a renewal is wanted. At that point, the agency in question will have to submit a written request to the minister, who will have to determine whether the reasons given by the agency are sufficient to authorize the one-year extension.

I don't understand the reasoning for the commissioner's involvement initially, but not for the renewal. I'll make an analogy. It's like appearing before a judge to request a search warrant. It's fine, but a year later, if you want to get an extension of the term, you have to go back to the judge and make a request. It's a bit like that.

Mr. Michel Picard: Thank you.

I'd like to come back to your first recommendation. It's a philosophic discussion, but I can never get a grip on the principle: we're talking about active cyber operations, at worst, and defensive cyber operations. We are cautious in our choice of words when we say that cyber attacks are not made in particular circumstances.

I had a whole series of questions, but I'm going to start backwards. The first question may be a bit silly: would conducting a cyber operation targeting a foreign country constitute an act of war?

Hon. Jean-Pierre Plouffe: I'm not an expert in this area. The people from CSE should be the ones to answer your question.

I don't know if Mr. Galbraith has an answer.

Mr. Michel Picard: Would it be an act of war, legally speaking? I think there's the whole legal aspect.

Regardless of the number of laws involved, if an organization that is a government organization by definition is conducting a foreign operation, the same way that we are victims of overseas operations that greatly justify cyber operation defensives, are we on the playing field of acts of war?

Hon. Jean-Pierre Plouffe: As a first step, with the CSE, the government determines that in the area of national and international security, it is essential to give the CSE the previously mentioned authority for active and defensive powers.

I think the mandate is very broad, and there may be implications for the charter and the privacy of people. That's why I say that there needs to be some sort of oversight from an independent body. Currently, this independent body is the Intelligence Commissioner. I don't understand why the Intelligence Commissioner should be excluded from this oversight because, supposedly, information is not being collected.

As I mentioned in my remarks, and the Department of Justice seems to agree as well, there may be implications for the charter and privacy. It seems to me that, for that reason, it would be good if any kind of oversight was done.

Mr. Gérard Normand: Mr. Picard, I would add that Parliament gives itself the legislation that it wants to give itself.

Bill C-44, which clarified the mandate of CSIS to act externally, also gave federal court judges the power to authorize activities abroad. This is something we would not have seen before, but which is now inserted in the Canadian Security Intelligence Service Act. These are the same reasons for the proposed new powers of the CSE. If accepted, they will become part of the legal system, even though, in the process, charter issues will need to be addressed.

● (1145)

[*English*]

The Chair: Thank you.

[*Translation*]

Mr. Paul-Hus, you have five minutes.

Mr. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, CPC): Thank you, Mr. Chair.

Thank you, gentlemen.

First, thank you for the very comprehensive document you submitted to the committee. Bill C-59 is, indeed, complex to study, and the document you have provided contains very important elements.

I would like to come back to one point, the approval process.

The problem right now is cyber threats. In cyber defence, there is a maximum number of resources that can be in the know and that can counter cyberattacks. We work together on this. However, when we talk about active trading, that is, when Canada conducts cyber operations, I find that there are many levels of intervention, given the secret nature of the information. If you want to carry out an operation, you need to collect information or make computer-based interventions in the systems.

This morning, I attended the meeting of the Standing Committee on National Defence. We have heard from people who work on cyber operations. According to them, in defence, the important thing is to provide protection. In case of attacks, they will especially turn to the CSE.

According to Bill C-59, when we talk about conducting operations, we seek the approval of the Minister of Foreign Affairs. On your side, you also ask for supervision by the Intelligence Commissioner.

Don't you think there are too many people involved in secret operations?

Hon. Jean-Pierre Plouffe: It's difficult for me to answer that question, because I don't know everything it implies, operationally speaking.

However, from what I do know, since the CSE observes foreign entities, I imagine those concerned also considered that the Minister of Foreign Affairs should be involved as well, regarding active and passive cybersecurity operations. Because this is something that happens on foreign soil, we think the minister should authorize these operations, or initiate them. I don't see a problem there. However, as I said earlier, I have a problem when people say that the Intelligence Commissioner should not be involved in reviewing everything, either because of the charter or privacy issues.

Mr. Pierre Paul-Hus: For the committee's information, could you provide two examples of operations Canada could request be conducted abroad? Could that be, for instance, collecting telecommunications intelligence in particular circumstances? I'd like to hear some examples. The debate is theoretical right now, and no one wants to actually say what type of active operations Canada might need to carry out.

Could you provide some examples to us?

Mr. Gérard Normand: Clause 27 of the current bill concerns gathering foreign intelligence. Clause 28 concerns cybersecurity. Clause 31 concerns active measures, as you said earlier. Active measures, as defined in the law, are not meant to apply to gathering intelligence. We are not supposed to interfere with the system.

The examples are many. There could be operations for military purposes. At this time, the military would turn to the CSE to reach their goal, which is fine. The CSE could also help other agencies.

Clause 31 implies that the CSE could carry out activities that might intercept communications, for instance involving international relations. This goes beyond the framework involving other countries where operational purposes are security and defence. The term "international affairs" can mean many things.

We have to consider the fact that the commissioner will be involved in such decisions. Clause 27 would authorize the same type of information-gathering activity, and the activity will be reviewed. We do not really understand why the commissioner would be excluded when it comes to active operations. As you said, this is something new.

Mr. Pierre Paul-Hus: Since I only have one minute left, I will conclude by highlighting proposal 7, for the benefit of the members of the committee. It's an important proposal that concerns the National Defence Act. This act states that "the expected foreign intelligence value of the information that would be derived from the interception justifies it." However, that provision does not appear in Bill C-59. So that is a good recommendation, and I thank you for it.

● (1150)

[*English*]

The Chair: Thank you.

[*Translation*]

Ms. Damoff, you have the floor for five minutes.

[*English*]

Ms. Pam Damoff (Oakville North—Burlington, Lib.): Thank you, Chair.

Thanks to all of you for being here today. It's been quite insightful, and we appreciate the recommendations you're providing to us.

As you know, the current scope of CSE's mandate is to acquire and use information from global information infrastructure. Under the current infrastructure, there really isn't clear direction on how to address the possibility of a Canadian citizen or someone who's residing in Canada having their information collected.

Do you see a benefit in recommending that Bill C-59 be amended to clarify that ministerial authorization be required when CSE does acquire information from or through global information infrastructure when a Canadian or someone residing in Canada has a reasonable expectation of privacy?

Hon. Jean-Pierre Plouffe: Could you summarize your question? I'm sorry; I didn't catch exactly what....

Ms. Pam Damoff: If a Canadian or someone residing in Canada has an expectation about the privacy of their information, they're not really covered. Do you think it would be beneficial to have ministerial authorization involved when you're collecting that information?

Hon. Jean-Pierre Plouffe: Do you mean with regard to CSE?

Ms. Pam Damoff: Yes.

Hon. Jean-Pierre Plouffe: Well, according to the actual mandate, as well as the mandate that is provided for in Bill C-59, CSE cannot target Canadians or persons in Canada. It cannot. It can target people or entities abroad only.

Ms. Pam Damoff: If I'm away on holidays in Scotland—

Hon. Jean-Pierre Plouffe: Well, you're abroad.

Ms. Pam Damoff: Do you think there should be authorization for Canadians when they are in that situation?

Hon. Jean-Pierre Plouffe: Well, CSE cannot target Canadians.

Go ahead, Bill.

Mr. J. William Galbraith (Executive Director, Office of the Communications Security Establishment Commissioner): If you're on holiday in Scotland, CSE would be able to intercept a communication involving you only if they were targeting a foreign entity abroad. All the other privacy protections that apply would be there, and that's what the commissioner would be looking at.

On a question like that, you may want to ask for more detail from CSE itself.

Ms. Pam Damoff: Okay.

Hon. Jean-Pierre Plouffe: In other words, in your example, it's only incidentally that your conversation would be intercepted, because maybe you are talking with somebody else abroad, another entity, and CSE wants to target that other entity, not you. If you happen to be there, this is what we call "incidental". While targeting foreign entities, CSE might intercept private communications involving Canadians incidentally. That's why they need an authorization from the minister to do that, okay? The prime target is not the Canadian; the prime target is the foreign entity.

Ms. Pam Damoff: Okay. That leads me to this question.

Publicly available information is one of the things you're able to collect, and I don't think Canadians understand particularly well how much private information we actually share publicly.

When I'm logging into an app and it says to use Facebook, can you buy that information from things like my Facebook picture or things that I might have shared that I don't realize are private?

Hon. Jean-Pierre Plouffe: Mr. Normand will respond.

Mr. Gérard Normand: As of now, the definition does cover information that you can buy. Some have expressed the position that it should not be covered. PIPEDA, for instance, the legislation we have in Canada, does not cover that type of information for it to be part of the publicly available information. Again, that is basically a matter for the government to look at to decide what they want this scope to be.

One thing I would say is that if you look at the definition in the proposed CSIS act, it's even more nebulous, because they refer to a section, so it's circular. They're not defining it at all. For one thing, I think this committee should ensure that the definition they take will apply to both statutes.

● (1155)

The Chair: Thank you, Ms. Damoff.

Mr. Motz, go ahead, please, for the final five minutes. Thank you.

Mr. Glen Motz: Thank you, Chair.

Thank you again for your comments.

I want to ask a question, Mr. Commissioner, with respect to your third recommendation. I appreciate the interest you have in being involved in approvals, and to be able to do your job effectively, you need to be involved in a lot of them.

When you talk about the emergency authorizations that the minister issues, you suggest that you should also be reviewing those immediately after they have been issued, which is before they're actioned, as I understand it. If that's the case, would that not, in something that's exigent, maybe put a further timeline or hindrance on the work of the security agency to do their job and maybe prevent an imminent threat?

Mr. Gérard Normand: The provision we're aiming for would not be to suspend the application of the authorization until the IC has looked at it. It would proceed with this authorization immediately, but the review *ex post facto* would be to ensure that the decision that was made was reasonable. It has to be made within the five days, so after two or three days, if he decides that it's not, then it has to stop, but it would not prevent it from starting.

Hon. Jean-Pierre Plouffe: It's actually similar to what they have in the U.K. In other words, the operation is going on and proceeding for the maximum duration of five days, but let's say that in this particular case the IC could intervene after two days or three days, look at it, and say, "Well, I'm sorry, but what you have done in the last two or three days is unreasonable, and it should stop." This is the purpose, or the gist, if you wish.

Mr. Glen Motz: Okay. If I'm hearing you correctly, you're suggesting that the authorization will proceed in an imminent threat situation. It's a review for the next time.

Hon. Jean-Pierre Plouffe: Yes.

Mr. Glen Motz: Okay. Thank you.

When you look at your resources and at what Bill C-59 is proposing, do you feel confident in the capacity that you have? Do you have enough resources to monitor anyone deemed to be a threat, or would those resources deal only with those who are deemed to be a top-level threat?

Mr. J. William Galbraith: In terms of whether or not we have adequate resources, the transitional clauses in the bill are quite clear. What we have in terms of the commissioner, the employees, and the appropriation from Parliament all transition to become the intelligence commissioner and his office.

What are the requirements? The requirements are having intimate knowledge of CSE activities and of CSIS activities. Clearly we have the knowledge of CSE from the work that we conduct currently in reviewing the activities of CSE, but we also have on staff now individuals who have experience and knowledge of CSIS. We had the opportunity to do some staffing over the last year, or since June at least, and we have hired individuals with knowledge and experience of CSIS activities. As well, we have engaged special legal counsel, which we have with us here, to deal with the complexity of Bill C-59.

As to whether the staff is going to be adequate going forward, there are a number of unknowns in terms of the number of authorizations that will be required from CSIS or CSE. Only once the bill is enacted and the activities begin will we have a sense of what the volume of authorizations will be, but clearly there was a sense that we have a reasonable starting point. The drafters of the legislation and the government must have felt that we at least had a good start with what we have to transition into the new organization.

● (1200)

Mr. Glen Motz: Speaking of the transition, are you clear and comfortable with, and do you understand the impact of, the new parliamentary committee and its role with the intelligence community and CSIS and those operations and how that's going to play out?

The Chair: Be very brief.

Mr. J. William Galbraith: We are studying all of the aspects and following the development of the committee of parliamentarians. We are meeting with CSIS and CSE with respect to how they're preparing and, to the extent that we can, we are keeping abreast of their work in developing the new authorities that they may have.

The Chair: Thank you, Mr. Motz.

That brings to a close our first hour for this committee. On behalf of the committee, I want to thank you for your contributions. As you can see, time is the enemy here, and much of what you raised certainly needs to be thought about extensively by the committee. Again, thank you for your contributions to this study.

With that, we suspend for a moment or two and re-empanel as quickly as possible.

● (1200)

(Pause)

● (1200)

The Chair: I call to order this second half of our meeting.

We have with us Mr. Ray Boisvert, who is with the Ontario Ministry of Community Safety and Correctional Services, and Ms. Micheal Vonn, who is with the BC Civil Liberties Association.

I don't know who wishes to go first, but whoever wishes to go first, please do so. You have 10 minutes.

● (1205)

Ms. Micheal Vonn (Policy Director, British Columbia Civil Liberties Association): I'm happy to go first. Thank you, Mr. Chair, and thank you to the committee for this invitation.

My prepared remarks are about the CSE and CSIS bulk data collection.

In his testimony to this committee, Professor Craig Forcese made a very important point about the thresholds for authorizations for CSE data collection.

Proposed section 23 of what would be the new CSE act sets out that activities carried out by the CSE in relation to its various mandates must not be directed at Canadians or persons in Canada. This is of course a continuation of the current situation in which the CSE is required not to direct its activities in this fashion.

Nevertheless, it is well established and conceded that the information of Canadians and persons in Canada is collected, because some collection, and by no means insignificant collection, is unavoidable due to the complexity of communication networks. Thus, Canadians' information is collected incidentally or unavoidably.

Part of the new regime proposed for the protection of Canadians' privacy interests is to require that the CSE seek a ministerial authorization that is then approved by the intelligence commissioner. The trigger that initiates this process of authorization and intelligence commissioner vetting would occur when the CSE's activities would otherwise contravene an act of Parliament.

We agree with Professor Forcese that this trigger is underinclusive, a view that is now echoed by Citizen Lab, the Canadian Internet Policy & Public Interest Clinic, and others.

As Professor Forcese notes, there is concern that the proposed threshold would not ensure that the authorization process would, for example, be initiated for activities that incidentally collect Canadians' metadata, which is obviously of critical importance.

Craig Forcese proposes a more expansive trigger, in which the authorization process is required for activities that would otherwise contravene any other act of Parliament or "involve the acquisition of information in which a Canadian or person in Canada has a reasonable expectation of privacy", a threshold that has already been referenced.

Our problem with this proposed addition is simply this: that the question of what precisely attracts "a reasonable expectation of privacy" is typically the central dispute in almost any emergent privacy issue, and this threshold would be adjudicated internally by the CSE.

We know, not least from years of reports from the CSE commissioner, that disputes over the interpretation of legal standards and definitions have been of ongoing concern, and national security activities in general are plagued with the "secret laws" problem of having words in a statute or directive interpreted in sometimes obscure or deeply troubling ways, and ways that may not be unearthed for years. Therefore, a trigger that involves a colourable definition is inherently problematic, in our view.

However, we read the latest CSE commissioner's report as indicating that the CSE has conducted its signals intelligence activities under just three ministerial authorizations since 2015. It appears that these authorizations tend to authorize a broad sphere of activities. Our understanding that the frequency and scope of "incidental collection" suggests that most, or even all, of the authorizations are apt to at least implicate Canadians' data. In other words, there are only a small number of authorizations, and almost all are apt to require the authorization regime of vetting by the intelligence commissioner.

Surely, then, it is best and still entirely feasible and efficient—to ensure that this authorization process does indeed examine everything that we are hoping it will—to simply have one uniform process of authorization approval by the intelligence commissioner for all classes of activities undertaken outside of the technical and operational assistance mandate, which is, as you know, its own sphere of activities.

● (1210)

For everything else, we recommend that the question of threshold be resolved by eliminating the need for a threshold and ensuring that every class of activities authorized be subject to the new accountability procedure of ministerial authorization and vetting by the intelligence commissioner.

I will turn now to bulk data collection by CSIS. It was most certainly our concern coming out of the national security consultation that the government response to the CSIS bulk data scandals, if you will, would be to simply empower the agency to do what it had previously been doing unlawfully without having a meaningful democratic debate about mass data acquisition in the context of national security. We certainly appreciate that having bulk data collection squarely on a legislative footing does improve transparency, but we are deeply concerned with the low threshold that is proposed in Bill C-59 and that this critically important matter is, quite frankly, receiving insufficient attention in the context of a large omnibus bill.

It was only recently that SIRC did its first-ever audit of the bulk data collection programs of CSIS. SIRC is of the view that appropriate bulk data collection by CSIS can occur under CSIS's current section 12 standard of strict necessity for data collection. In our view, it is hard to imagine a body that would be better positioned to assess this, both from the perspective of accountability and respect for the rule of the law and from the perspective of the operational needs of CSIS.

SIRC's proposal for the standards and criteria for bulk data collection is a three-part test: that there be a clear connection to a threat to the security of Canada, that no less intrusive means are available, and that there be an objective assessment of intelligence value.

Now, compare that standard with the standard set out in Bill C-59. Bill C-59 allows CSIS to collect publicly available datasets, with no definition of that term, on the basis of a bare relevance standard. With respect to Canadian datasets—which, we need to remember, are expressly defined as datasets that contain personal information expressly acknowledged as not directly and immediately relating to activities threatening the security of Canada—the test for their acquisition is simply that the results of their querying or exploitation could be relevant and that this assessment must be reasonable.

It may be argued that this vast scope for bulk data collection is at least mitigated by the requirement for judicial authorization for the retention of those datasets, but rather than providing significant gatekeeping, this authorization simply compounds the effects of the very low standards that lead up to it. Personal information that does not directly and immediately relate to threats to the security of Canada is allowed to be collected if it "could be relevant", if this assessment is "reasonable", and if the judge then decides that the dataset can be retained on the standard of "is likely to assist".

These, then, are the thresholds of what most Canadians would call mass surveillance, and we believe most Canadians would reject these thresholds as shockingly low standards. Thus, a genuine opportunity to meaningfully shape these surveillance practices is being squandered in Bill C-59.

The proposed standard represents a mass erosion of the privacy protections from the strict necessity standards that currently apply. We recommend that the CSIS bulk data provisions be revised to be expressly within the strict necessity standard, and not in exception to it, and that the criteria for bulk data collection, such as that fashioned by SIRC as implicitly principled and workable, be set out within the legislation.

Those are our prepared remarks. Thank you.

The Chair: Thank you, Ms. Vonn.

Go ahead, Mr. Boisvert.

Mr. Raymond Boisvert (Associate Deputy Minister, Office of the Provincial Security Advisor, Ontario Ministry of Community Safety and Correctional Services): Thank you very much, Mr. Chairman, and thanks for this opportunity to speak to everybody today.

As you know, I am the provincial security advisor for Ontario. I began this role in January of 2017. Prior to that, I spent almost five years as a consultant to private and public organizations in the area of national security-related risks, including cyber-threats. Prior to that, I was with the Canadian Security Intelligence Service, CSIS, and left that organization in 2012 as the assistant director.

As a result of joining CSIS at its inception in 1984, I've witnessed a tremendous number of milestones that shaped Canada's security intelligence environment, more specifically in regard to the organizations that are central to Canada's threat response.

At this moment, we find ourselves yet again at the cusp of change, and obviously important change. Although the CSIS Act has been widely viewed as a model of effective security intelligence legislation, it has required renovation from time to time, perhaps not so much due to any particular failings but rather to the necessity of changing times socially, culturally, politically, and, now more than ever, technically.

Of all the elements of import in Bill C-59, it is time to consider essential changes for an organization that I did not work for but to which I maintained important operational connectivity over many years. It is time for CSE to have its own enabling legislation, as its current mandate is 16 years old.

Most critical to that transformation of mission and mandate is the area related to cyber-threats. Canada must now join the community of like-minded nations determined to resist the growing threat of globalized criminal enterprise, nation-state-directed theft of intellectual property or interference in our society, and the potential for catastrophic destruction of critical infrastructure, be it the result of fifth-dimensional warfare or terror attack. We must support and connect and keep pace with our allies, from Australia to the EU. They themselves have recognized the nature of this new 21st century threat environment.

The nations that do not support or believe in these values certainly have discovered the benefits of hybrid or fifth-domain warfare. They are extremely active in targeting our key infrastructure and our future prosperity through the theft of the best and most important intellectual property the country has to offer. They've also noted the ease and the immediate benefits of undermining our democratic processes by undermining people's trust in institutions, as well as our ability to conduct respectful and constructive dialogue.

There are a number of areas to explore in this discussion today, but first let me say that I've also been a long-serving and vocal advocate of increased accountability for the security intelligence community. The establishment of the National Security and Intelligence Committee of Parliamentarians and the National Security and Intelligence Review Agency will now meet the majority of my concerns on the need to enhance accountability and transparency across the security establishment.

However, as part of my opening proposition, let me now address more directly aspects of the threat and our need to effectively respond to that reality.

We live in unprecedented times. Never in my career, which has spanned a little over three decades, have I perceived such a set of local and global challenges, from climate change and food security to irregular migration and unprecedented numbers of refugees, as well as social and political upheaval, nuclear threats, and shifting global hegemony. Threat actors from around the globe now target Canada with ease. Conversely, Canadians with the intent to harm others or target Canadian interests abroad can now operate from far-flung regions of the world, not just from typical conflict zones.

In this security intelligence equivalency of globalization, it is critically important that CSE continue to support CSIS, the Department of National Defence, and law enforcement agencies in the pursuit of lawful investigations or mission requirements wherever threats may emerge around the world. Whether that means assisting CSIS to collect intelligence on an emerging violent extremist network targeting Canadian travellers or diplomats abroad, assisting the Canadian Forces in the protection of a deployed unit delivering training, or perhaps even helping the RCMP bring human traffickers to justice, we need to provide the best available toolsets. The tools or capabilities I'm suggesting here are ones that only our signals intelligence organizations can provide.

● (1215)

Equally important, and I believe critical, is that we rely on Canadian-controlled and accountable capabilities rather than on the efforts or competencies of other nations that may not share our full set of standards and intentions.

With respect to part 3 of the bill, specifically dealing with cybersecurity and information assurance, let me say that as the provincial security advisor for Ontario, I am concerned most about this area, the cyber-threat targeting our vast investments in critical infrastructure.

Outside of the protection of intellectual property from either front-door or backdoor acquisition, what is key to our current and future prosperity is the protection of life-sustaining critical infrastructure assets, be they publicly owned or in private hands. Therefore, the enhanced ability for CSE to provide assistance towards protecting our critical infrastructure is vital for Ontarians and, I dare say, for all Canadians.

I believe this to be true because we now exist in a hazardous environment where 400-plus new malware threats are produced every minute and where ransomware attacks a person somewhere in the world every 10 seconds. As localized proof, the Government of Ontario's cybersecurity operations team manages approximately 40 billion security events per month. Yes, that's billions per month. Although we are within industry norms, over 90% of the emails the Ontario public service receives are blocked due to botnet or spam threats.

With respect to defensive cyber operations, I believe that only CSE can bring to bear the technology, know-how, and library of threat-related data necessary to build effective cybersecurity resilience so necessary in this kind of environment. From conversations I've had with private industry and with large independent agencies of government, such as those involved in energy, health care, education, and transportation, I know that all feel the effects of constant cyber-threats. In essence, we and they can no longer do this alone. It is a global threat phenomenon requiring a national-level strategy and capability.

With regard to active cyber operations, let me simply say that the best defence always begins with a good offence. When more than five dozen countries around the world are reported to be actively developing cyber-operational capabilities, in my view, we must develop offensive cybersecurity measures to respond, and on certain occasions that means beyond our borders.

Offensive cyber-tactics have been developed and are being applied by the best private security firms in the world. Engaging the so-called dark web or darknet to gather intelligence in advance of an attack and to protect systems, such as those in the financial sector, has been the norm for some time. I know that because I've worked directly in that sector. When the time comes to face a targeted attack intended to manipulate the operating systems of an energy facility to cause a malfunction or perhaps even to destroy something, as we've seen in cases from Ukraine to Germany and even New York State, we will need CSE to "degrade, disrupt, influence, respond to or interfere with the capabilities [or] intentions" of those threat actions or their actors.

More commonly, and as another example, the frequency and prowess of so-called denial of service attacks or DDoS events are intensifying. One day soon, I predict, CSE will be required to assist a Canadian service provider or a subnational level of government to repel a massive DDoS attack.

With the advent of the Internet of things, we've already seen or witnessed botnets created out of smart devices being harnessed to launch attacks of one terabyte per second against institutions typically associated with information sharing, anti-spamming facilities, social networks, human rights workers, and mainstream media. Rest assured that this will only get worse, especially when we are facing autocratic regimes around the world that have no inhibitions.

On the issue of changing times, my current role as provincial security advisor is an important example of how the world has changed and how Canada's view of itself and how it operates must also change. Ontario is but one of 14 core jurisdictions in this country. By itself, Ontario's economy would rank 18th in a G20 context. No doubt, like Ontario, all subnational jurisdictions are conscious of the multitude of threats that continue to adversely affect prosperity and security.

To my mind, an effectively legislated security establishment that balances security requirements with accountability, transparency, and respect for the rights of Canadians is indeed the blueprint for our future success as a nation in this increasingly tumultuous world.

Thank you.

● (1220)

The Chair: Thank you, Mr. Boisvert.

We go now to the round of questioning.

Ms. Damoff, go ahead for seven minutes, please.

Ms. Pam Damoff: Thank you, Chair.

Thank you to both witnesses for being here today.

Ms. Vonn, it's nice to see you again. My first question is to you. I think you were here when I was asking CSE a question. I wonder if you could respond to what I was asking. If a Canadian or a person who resides in Canada and is abroad has a reasonable expectation of privacy, if that information gets caught up in what CSE is doing, do you think a ministerial authorization should be required?

● (1225)

Ms. Micheal Vonn: That's the essence of our proposal here: to find a way to harness the accountability mechanism that is being proposed for all collection of Canadians' information, whether or not it hinges on this finding of a reasonable expectation of privacy. How are you ever going to get to that adjudication unless you have a mechanism? It becomes a circular argument, because what is frequently collected, in our understanding, is metadata, if not a direct interception. In our view, that is certainly one of the issues that is critical to maintaining Canadians' confidence in the proposals. Having more authorization accountability is always going to be better than having less.

Ms. Pam Damoff: Do you think there's a misconception amongst Canadians about this? Are they thinking about people who are perhaps sending emails and making phone calls overseas, a terrorist talking to a Canadian who's plotting, versus.... I know I didn't understand exactly how all-encompassing this metadata was until I was on this committee. Do you think Canadians understand how they can get caught up in that loop because they're on Facebook or Instagram or Twitter or something like that, where things are being collected that they think are private and but aren't?

Ms. Micheal Vonn: Certainly Canadians are becoming increasingly alive to the sense that what constitutes incidental collection—again because of the nature of the communication networks—could very well implicate them. This is a growing awareness, I would say, in Canada, and it becomes problematic when we keep hearing.... It's fair language to say that CSE doesn't target, but the way that the actual operations occur certainly implicates Canadians' data frequently. When I say it's not insignificant collection, again this is something that Canadians are becoming increasingly alive to, so they want to see mechanisms that are robust enough to provide the kinds of assurances that would be protective of them.

Ms. Pam Damoff: While I agree with you, I think that if more Canadians understood what's actually being collected, you would have more Canadians speaking out about it.

This does bring me along to data collection. I know you've spoken to this in the past, about data collection and how long it should be retained and whether there should be mechanisms for destruction of data that's collected. I'm wondering if you believe that there should be an amendment to the bill to introduce a necessity threshold for the retention of personal information, as well as a destruction obligation for personal information that does not meet the necessity threshold. Would it help to increase transparency and protect individual privacy?

Ms. Micheal Vonn: Is that question related specifically to CSE...?

Ms. Pam Damoff: It's to the bill itself in its entirety, because it's CSE that's collecting data, right?

Ms. Micheal Vonn: That's right. There are a number of aspects of data collection that are touched on. I think, in the main, depending on the kinds of collection, that introducing elements of necessity would clearly be of privacy benefit to Canadians. In terms of whether or not that's appropriate across all of the channels of data collection, we would suggest there may be some standards of variation that are nevertheless appropriate.

That said, what you're asking about retention is a very interesting piece and it's part of this sense of compounding, low-threshold authorizations. It's the point that we make about simply compounding the first mistake of having an insufficiently high threshold in the beginning by thinking we can retain this on some kind of "might prove useful" standard. This compounds the first problem, as opposed to addressing the problem, which is the fundament of what we're saying in relation to retention.

Ms. Pam Damoff: Thank you.

I wanted to talk about reporting. I'm wondering if you see a benefit in mandating the intelligence commissioner to produce an annual report about the activities and the bodies that it oversees, and also if you think that it would be beneficial if CSIS published an annual report.

● (1230)

Ms. Micheal Vonn: Certainly we have found, for example, the annual reports from SIRC and the CSE commissioner to be immensely valuable. If we were going to make a recommendation, over-reporting as opposed to under-reporting would absolutely be the direction we would want to go for accountability and maintaining trust.

Ms. Pam Damoff: Thank you.

I have about a minute left, and Mr. Boisvert, I don't want to leave you out, so this will be a fairly quick question.

Some of the testimony we heard earlier about Bill C-51 was that the new offence of advocating or promoting the commission of terrorism offences in general was so general that it was impossible to prosecute under. When the minister was here, he talked about changes to it so that charges actually could be laid. I'm wondering if, in probably 30 seconds, you can give some brief comments on that.

Mr. Raymond Boisvert: In my time at CSIS, although now dated —it's been almost six years since I left—when I was responsible for the counterterrorism operations team, a number of charges were difficult in this even more complex choreography around intel-into-evidence. In other words, we were proceeding against certain targets that met the CSIS threshold of reason to suspect, versus then transferring some information protecting sources. Of course, Bill C-59 provides new tools to assist with that in some respects.

However, many operational opportunities were left wanting, first because we had difficulty transitioning information from intelligence into usable evidence, and secondly because, quite often, I found the perspective of crown prosecutors was always extremely cautious. As a Canadian, I think that's very important, because it adds one more check and balance, definitional things, so that we essentially have a prosecutorial system that is inclined to ensure that there is very little chance this prosecution could not proceed successfully. More often than not, cases ended up dropping below the threshold, even though perhaps in another jurisdiction—south of the border, as one example —they would have proceeded full guns.

The Chair: Thank you, Ms. Damoff.

[*Translation*]

Mr. Paul-Hus, you have seven minutes.

Mr. Pierre Paul-Hus: Thank you, Mr. Chair.

Good afternoon, Mr. Boisvert and Ms. Vonn.

Mr. Boisvert, I'll start will you.

I want to say a few words about the Islamic State group. We now know that that group has lost a lot of ground in Syria and Iraq, but it has begun to carry out cyber-attack operations. The 2017 public report on the terrorist threat to Canada confirmed that Daesh had used cyber exploitation to draw up hit lists. These lists included the names and personal information of people chosen at random, and Daesh sympathizers were encouraged to attack them.

Regarding the threat posed by the Islamic State group, do you think we should focus mainly on cyber-attacks of that type, and on monitoring?

Mr. Raymond Boisvert: I would say no. I am more concerned about cyber-attacks. As I explained in my opening remarks, these attacks are a direct threat to society, as well as to our current and future prosperity.

Given the nature of terrorism, such attacks have more serious effects as compared to other threats to national security. However, we haven't seen the end of Daesh. This group still has sufficient operational capacity to attack Canadians or Canadian interests here and abroad.

Mr. Pierre Paul-Hus: Let's talk about those economic interests. A few days ago, the newspaper *Le Monde* informed its readers that African Union headquarters located in Addis-Ababa were being spied on by Beijing. The building was built in 2012 by the Chinese, who took the opportunity to install systems allowing them to transfer all of the information from African Union headquarters to Shanghai.

Are you surprised by this type of thing?

The government is trying to forge economic ties with China, but several countries consider China and Russia to be major actors behind cyber-attacks and the gathering of information through these means. Do you agree with that?

● (1235)

Mr. Raymond Boisvert: Yes.

With your permission, I will make a few comments in English, since I mostly work in English currently.

[*English*]

There's no doubt about the threat capabilities of Russia. They have been demonstrated through the interference in democratic processes through western Europe and in the United States and increasingly in a number of specific states in the U.S. Russia's malicious intent in supporting autocratic regimes from Syria and elsewhere is clear. Those are much more predictable and traditional types of quasi-military activities. In the hybrid warfare threats that we've seen them conduct, they are using proxies in Internet-type attacks, and in convergence with organized criminal groups in Russia, we have seen them launching a number of important negative effects on jurisdictions, including Canada.

China is a much more complex issue, and I understand the challenges of national jurisdictions like ours. State-owned enterprises and authoritarian capitalism seem to drive a lot of business opportunities and business decisions, but they represent complexities from time to time that I'm not sure we have fully examined as Canadians.

There's also the issue that China is now in the age of self-admitted “sharp power”, and they exercise that power with very little reservation anymore. There's no longer even a question of hiding their intentions. They are taking a very aggressive approach around resources and intellectual property, and they also are very clear in dealing with dissidents and academics. They've arrested some of them, and they punish others, including academic institutions in North America, at their will, so I think there's a value challenge that Canadians have to consider along with the economic opportunities discussion. The Cold War is over, but a new version is rapidly emerging, and I think our focus on counterterrorism is not always our best play.

[*Translation*]

Mr. Pierre Paul-Hus: We were just talking about warfare. I don't remember if it was here or at the meeting of the Standing Committee on National Defence. I believe it was Ms. Damoff who raised the topic. We discussed certain ill-intentioned activities on the part of China and Russia that targeted Canada.

Earlier, you said that offence is the best defence. Is Canada in a position to conduct offensive operations in order to protect our country, or is that process too complex?

I know it is complex, but I wonder what sort of activities Canada could undertake to protect itself.

Mr. Raymond Boisvert: In the hyper-competitive world we live in, offence would indeed be the way to go. We are dealing with foreign nations that are in no way subject to the same rules as we are, or to the scrutiny of organizations like the one Ms. Vonn represents; these things mean that the government here must be accountable.

Earlier I spoke about the possibility of a cyber-attack against one of our organizations. It's hard to say if we could easily tell if such an attack came from a particular country or its representatives. In any case, I think it is increasingly possible for us to determine specifically which computers and operations centres we could target, attack and remove from the international communications network.

Mr. Pierre Paul-Hus: The current government had some critical comments to make about Bill C-51. We then proposed Bill C-59 to change certain things. We are often reminded that we must not violate the rights and freedoms of Canadians; we all agree on that. However, in a defensive context, we have to have the means to protect ourselves.

In your opinion, will Bill C-59 excessively constrain or weaken the government's safeguards?

[*English*]

Mr. Raymond Boisvert: No, I'm of a view.... I very much appreciate the work that Ms. Vonn and her colleagues in other organizations in Canada and the western democracies do. It's an important part of that debate and discussion, but quite often I do feel a little concerned that we spend so much time focusing on what are, I believe, organizations that operate by the rule of law. They're subjected to multiple layers of review, including everything from the Auditor General to the Privacy Commissioner. We now have a number of additional bodies, which, as I said, I've welcomed. I think we live in the age of transparency and accountability, and agencies that operate with these special powers must accede to them, but I also think that sometimes we forget, as we focus on the incidental collection of some Canadians, that despite the characterization, it's not massive, in my view. I know from my time it was minuscule, but it's incidental. It will happen because of the convergence of all the global information and communications infrastructure. It does occur, yet Canadians don't seem to be having the same debate about all those data brokers out there that have hundreds, if not thousands, of unique identifiers about them.

Sometimes I wish Ms. Vonn's organization or others would focus a bit more on that, just to have some sense that Canadians need to look at their data and their privacy and their personal information, and not worry about the security establishments as much because they have rules of engagement and overview and review. We need to look at those who don't.

● (1240)

The Chair: Thank you, Mr. Paul-Hus and Mr. Boisvert.

Go ahead, Mr. Dubé.

Mr. Matthew Dubé: Thank you, Chair.

Thank you both for being here. It's interesting, given the comment that was just made about incidental information, because there's incidental information, there's the publicly available information, and there's this notion that there's clearly an intent in the legislation to expand the powers for this new threat that's being described, but when we ask the chief of CSE to explain why those powers would be used, there's no example that's able to be provided.

This question is for you, Ms. Vonn. I want to understand, because there's a link here. One of the answers that was given to me when these officials were before the committee was, “Don't worry. If you look at part 3 of the bill, in proposed section 25, they have to ensure measures are in place to protect the privacy of Canadians", but that's a very vague notion, because it then goes on to say, “of Canadians and persons in Canada in the use, analysis, retention and disclosure of...” and then goes on to describe the information.

The use of the word “disclosure” is particularly troubling, because that's how the government has rebranded the information sharing that was created under former Bill C-51. I'm wondering if there's some concern about that information. It's seemingly for research and other innocuous purposes by CSE, but it can nonetheless be shared, and I'm wondering if there's some concern about what consequences there might be, in particular if it's being shared with Five Eyes allies, when we see examples like what was reported in *La Presse* at the end of last week about the RCMP acquiring information on Canadians from the DEA without the proper judicial oversight that would normally be involved if they were doing it here in Canada.

With that very broad portrait I've painted, I just want to understand, because I think a lot of people don't quite understand how maintaining, even with a cosmetic change, information sharing as was brought in by the former Bill C-51has an impact on how these new powers of CSE are going to potentially play out.

Ms. Micheal Vonn: Thank you.

It's of critical concern to civil libertarians that the public understand that collection, incidental or otherwise, of personal information into national security agencies is not innocuous. In part because we do have these alliances, information sharing does flow in ways that are potentially problematic for those individuals, even with the notion that perhaps we're not exploiting it and perhaps we're not using it.

We're going to try to give assurances, but we don't know what's being used in terms of exploitation. We know it's everything from network mapping to profiling, which has been identified as a huge problem. It definitely resonates with Canadians as a threat to their own personal security. All those aspects of trying to figure out what the jeopardy is for this collection, use, retention, and exploitation are critical. It's critical to figure out those tentacles and ensure that we have mechanisms that are not merely paper mechanisms when we say we have measures. What are those measures? How do we know where they work? Do they cover off all the aspects?

Those are aspects behind the curtain that goes on with national security that most Canadians cannot see. We've come to have reason to distrust, because we haven't seen, for example, the simple definitions for things that would allow us to have the insight that we should have for democratic accountability.

When we see failures of definitions in Bill C-59 around things like publicly available information, to pick up my colleague's point, and a national security agency can acquire data through a data broker using the kinds of techniques that were just being described and ingest that into a system in which information may get shared with allies abroad, you can see the magnification effect of the impact on security of individuals—not national security, but personal security—in relation to all of those data practices.

People are not as alive as we would like them to be to these threats, but they're increasingly alive that these are the problems, as you illustrate.

● (1245)

Mr. Matthew Dubé: I'd like to hear from you both on this.

The words "information infrastructure" get thrown around a lot. There's a definition there. We can debate that, but the definition of a foreign entity being attacked or information being collected on them by CSE is not the same as it was when the CSE act first came in. These information infrastructures.... I'm thinking in particular of Ms. Damoff's questions over the last two witness panels about this notion that....

Even when we look at telecommunications companies in this country, we would have blinders on if we believed that things like LTE networks and stuff like that are being developed in a silo. There are obviously international efforts going on to make these networks better and more robust, but while that's happening, these legal definitions of what's.... It just seems that it's a bit out of date in terms of what's foreign and what's not. As soon as we give the power for the minister to identify information infrastructure, inevitably that net is going to be wider than it ever was before. I'm wondering what your thoughts are on that.

Perhaps we could start with Mr. Boisvert and then go back to Ms. Vonn.

The Chair: That's really an important question. Unfortunately, Mr. Dubé has left you one minute to answer it, so could you be very brief?

Mr. Raymond Boisvert: It's going to be very difficult. It's a very complex world and it's getting more complex. Data is growing exponentially.

It's a two-part play. One part is the opportunity that technology will allow us to do many things. The second part, of course, is that it's an enlarged threat surface for attackers to focus on to break into those same networks to steal personal identifiable information in the same way as is being suggested the security establishment can under warrant, in a predicated investigation—lawful work—go in there.

We have a big problem around data and around privacy and about the invasion or the loss of security of the person. I think as much or more of it is occurring from the threat actor side than from security agencies and others.

Ms. Micheal Vonn: You see the tension around this when you give the CSE broad, active cyber-powers that exploit vulnerabilities in the system that of course Canadians need to protect themselves against. Are you going to disclose those or are you going to exploit them? It's one of the tensions inherent in this new power.

Mr. Matthew Dubé: If I may, really quickly, like 20 seconds—

The Chair: You have 20 seconds.

Mr. Matthew Dubé: When I led myself to the exercise that CBC/Radio-Canada did with the cellphones and CSE not commenting on what that does for public confidence, is that potentially because those same loopholes are being exploited, and inevitably there's that risk?

The Chair: You're going to have to work that into another answer. I'm sorry.

Go ahead, Mr. Fragiskatos, for seven minutes, please.

Mr. Peter Fragiskatos (London North Centre, Lib.): Thank you very much, Chair. Thank you to both of you for being here today.

Mr. Boisvert, I want to start by talking about cybersecurity and offensive capability. In your presentation, you talked about a community of like-minded nations coming together and taking cybersecurity very seriously for a number of reasons, not just from a public safety perspective or traditional national security perspective but also for the defence of basic democratic principles.

I wonder if you could talk about where we are—or where CSE is, I should say—in terms of what's being proposed for an offensive cyber ability and how that compares to other middle powers. I won't talk about the U.S., but, for example, the Australian Signals Directorate, the equivalent to the CSE, has an offensive cyber capability. In New Zealand, the Government Communications Security Bureau is the equivalent to CSE. It's not directly involved in mounting an offensive cybersecurity strategy, but that is in effect conducted by the defence force. That's in place there.

Where are we in terms of our Five Eyes allies? Let's look at what they're doing and compare that to what we're doing.

Mr. Raymond Boisvert: At the present moment, I think we're on the low side of response in terms of investment and I think in terms of empowerment for the security establishment to respond.

I think that may shift. We have a pending government cyber-strategy that may boost us into a new level of the atmosphere, but currently I think Canada is seen as being somewhat trailing its key allies, from the United Kingdom to Australia and New Zealand and elsewhere. To me that's very problematic, because while my responsibility as the provincial security advisor is to help or assist in certain strategic issues around the prosperity agenda, it's mostly around protecting critical infrastructure and around cybersecurity.

With that in mind, as I said, we or they—those who own that critical infrastructure—cannot do it alone. These are some of the large independent agencies of the Ontario government in, let's say, the health care sector, education, transportation. We need to bolster our capabilities to make ourselves on par with places like Australia.

● (1250)

Mr. Peter Fragiskatos: I'm glad you mentioned critical infrastructure, because I wonder if you could tell us how an offensive cyber ability allows us to protect critical infrastructure. You've been very public about concerns around hydro and nuclear power stations as well as health care systems and hacking attacks meant to retrieve personal and private information from Canadians or basic R and D data. How critical is an offensive strategy, an offensive capability, from a cybersecurity perspective, in protecting all of these things?

Mr. Raymond Boisvert: First let me affirm too that it's really important to understand that the health care sector in general is now the most targeted area of governments around the world. Right up there with .mail and .gov domain addresses, most health care sectors are under attack. Why? It's because data is the new oil. It's the most expensive and most sought-after commodity in the world, and threat actors of all varieties and types are converging upon it. Those are also arguably the least defended sectors of our society, unlike the large government and military sectors.

I think we need to quickly move to a place where we can bring to bear some of those cyber-offensive tools. One example would be to go out into the dark web consistently and look for early indicators of compromise and look for where threat actors are talking about you, talking about your domain and talking about your strategies, as early opportunities to get at them.

There are also the opportunities in a sort of offensive way. Should a massive DDoS attack occur, as we've seen against places like Spamhaus, *The New York Times*, and other organizations—and they are amplifying in size—without the aid of large agencies, those particular important aspects of our democratic societies will fall. It's about going out there, targeting those servers—of course consulting with the Minister of Global Affairs, and of course with the approval of the Minister of National Defence—and hopefully exercising some sort of kinetic effect on those servers and taking them offline.

Mr. Peter Fragiskatos: I appreciate that.

You've been very clear about the importance of securing critical infrastructure. My colleague opposite has already asked about it.

In the case of the threat of Daesh, for instance, the pendulum swings, and has swung over the years. Particularly after 9/11 there was an emphasis on radical Islam, if I can put it that way, and countering that particular threat. However, can you go over what you said about how important it is to secure our critical infrastructure?

If we're listing threats and ranking them in terms of danger to our national security, do you think critical infrastructure is a more important area to focus on right now than what we've been looking at in the past, after 9/11?

Mr. Raymond Boisvert: Yes. As I was saying earlier, terrorism is effective because it terrorizes. It has a disproportionate effect. The number of Canadians adversely affected by a terrorist event is very small.

Conversely, though, infrastructure is everything that sustains our life. It's the heat, the lights, the food at the grocers, the petrol at the service stations. All those fundamentals that allow us to exist are all now increasingly built on automated systems—on a machine, on machine learning. It's interconnected interdependencies across the board. That's why those are at risk. They're at risk mostly in the age of fifth-domain warfare. We went from land to sea to air to space, and now it's about cyber. We probably won't see another debate over an F-35 again, because most of that money in most jurisdictions is moving toward information warfare.

They will do what Russia's done in Moldova, Ukraine, and Georgia, which is to go after something and signal. You might just take out something small, then something a little bit bigger, and then something that threatens to be cataclysmic. I think that's really where the big threat is.

Are terrorists using cyber-tools? Not so much yet. Is Daesh going to go from dominating social media to tuning its skill sets toward attacking? I think that's very possible.

The Chair: Thank you, Mr. Fragiskatos.

We have Mr. Paul-Hus and Mr. Eglinski for five minutes.

I'm going to take the immense power of this position and allow Mr. Spengemann the final five minutes, even though we'll have gone past time, if that's all right with colleagues.

There are five minutes for the two of you.

● (1255)

[*Translation*]

Mr. Pierre Paul-Hus: Thank you, Mr. Chair. I will be brief.

My question is addressed to Mr. Boisvert.

Canada has adopted a laissez-faire approach to Chinese investments in Canadian businesses, in the technology sector in particular. Does that concern you, all the more so since one of Canada's closest allies has criticized us for selling a high tech business that sells satellite communications systems to the Chinese?

Mr. Raymond Boisvert: I recognize that this is a very complex area, as I have pointed out previously. New opportunities are cropping up. Canada has to deal with a new economic reality, just as negotiations are ongoing with its North American partners.

China represents a real opportunity, but we have to keep our eyes open. As for investments in certain sectors, particularly the technological sector, I do in fact have several concerns.

Mr. Pierre Paul-Hus: Fine.

I now yield the floor to my colleague.

[*English*]

Mr. Jim Eglinski (Yellowhead, CPC): The committee has heard that the Five Eyes community is critical to Canada's intelligence community. What are the consequences if new reporting and regulations reduce our capacity to do that?

Mr. Raymond Boisvert: At least in my time at CSIS and within the intelligence community, I think Canada was always a very powerful and respected net contributor to the group. However, at times it may have changed.

At the end of the day, I'm inclined to believe we're in a new era. Things change all the time. Legislation has to change. We need to improve our ability to respond to new technological advances. Equally, though, we're still in part of what I call the "post the story of Ed Snowden" age. Once we get through that, society will nevertheless have been transformed. He was a consequential figure. I recognize and respect that.

Therefore, we're in the age of accountability and transparency. As long as you have a mechanism such as emergency powers to invoke, as the chief of CSE has, I think having more layers is fine. I wouldn't want to respond to any alarmist comments to the effect that now we'll be stuck and won't be able to respond effectively. I think it's a pretty good balance overall.

Mr. Jim Eglinski: Do you think this could put Canadians at risk?

Mr. Raymond Boisvert: Do you mean if Bill C-59 is passed in its current form or if we have more layers?

Mr. Jim Eglinski: Yes, in relation to the first parts of my question.

Mr. Raymond Boisvert: Again, I think Bill C-59 is a good balance. I think Canadians will be better served by it and I think we'll have as good an opportunity as in the past to deal with emerging threats.

Mr. Jim Eglinski: Okay.

Does the increase in the reporting pose an issue for operations if more money goes towards administration? Do you see any...?

Mr. Raymond Boisvert: There's no doubt that there's a cost, and that cost could be nimbleness. I always have to measure that. I think of a moment in time when I was responsible for the counterterrorism sector, or the principal one. Over 30% of my management team was involved in Security Intelligence Review Committee hearings and security certificate hearings, and at that time about 87% of our staff had less than two years' service.

That was one highly risk-managed environment. We had a number of kidnappings. We had Robert Fowler, Louis Guay, Amanda Lindhout. We had probably half a dozen kidnapping cases around the world running at the same time.

It's tough. If you add more layers, you should probably think about the resourcing question in terms of trying to ensure that we do not affect operational capability.

Mr. Jim Eglinski: Thank you.

On November 20, I spoke in the House on Bill C-59, and I talked about part 5, which amends the Security of Canada Information Sharing Act. We have heard and read repeatedly that information sharing and breaking down the silos for information are critical to protecting Canadians. Do you believe that Bill C-59 is increasing or decreasing our ability to share information?

Mr. Raymond Boisvert: Let's just say that we've gone from almost zero capability to considerable capability, and now back to something perhaps a little less than perfect. I guess, from a security practitioner and not from somebody, of course.... I would take Ms Vonn's points on that. You really have to be careful about this.

I'll share a quick anecdote. I was posted to the Middle East in the early 2000s. Suddenly one of the employees at the embassy came to me and said, "You know, there's a Canadian passport"—we had lots of serial losers of passports—"that has popped up in five different countries in the last six months, it seems, because we're getting reports, yet that person is supposedly still living in this country." I said, "Okay, can I get their name?" He said, "Can't do that, sorry."

Anyhow, we ended up having a long debate. It escalated up to the ambassador and all the way back to Foreign Affairs and CSIS, and I don't know if it ever got resolved. To me that was the worst example of how things used to be. We can never go back to that, because the lives of Canadians would be put at risk.

● (1300)

The Chair: Thank you, Mr. Eglinski.

Mr. Spengemann, the floor is yours for the final five minutes, please.

Mr. Sven Spengemann: Thanks very much, Mr. Chair.

Thank you for being here.

Ms. Vonn, you're joining us during the week of the one-year anniversary of the shooting at the mosque in Sainte-Foy, Quebec. The country is still coming to grips with this incredible tragedy. I'm wondering if you could, just in a very general way, give us your thoughts on where you think Canada is today with respect to the balance between civil liberties and good security. Perhaps from an organizational lens you have data to back up Canadian opinion, but more personally, where do you think Canadians are vis-à-vis the time prior to January 1 of last year?

Ms. Micheal Vonn: Thank you for the question. I hope it's appreciated that the BC Civil Liberties Association takes security very seriously. The importance of getting this correct, getting these rights and freedoms of Canadians to fit together with the ability of the government to provide national security protection occupies a great deal of our bandwidth.

Canada, as you may know, was really—to use some of the language that has already been introduced—a bit of a laggard in a number of arenas, including having the kinds of transparency and accountability mechanisms that are standard in many of our ally countries. We welcome the ability to enshrine in legislation and make more transparent the accountability that is needed for Canadians to trust that national security is working in their interests. We have advanced in that regard.

Our concern about Bill C-59 is that there is a sense in which this is the moment to get the big pieces right. When we bring forward our concerns about the thresholds for bulk data surveillance, which has never been appropriately debated at a parliamentary level, we are saying that we welcome this opportunity to put the big thinking together in relation to these pieces, but that in part because we have an omnibus bill before us, some of those aspects are being given insufficient attention.

Mr. Sven Spengemann: Very briefly, one of the sets of provisions that's very important—it's near the end of the bill—is the one dealing with youth, clauses 159 to 167. They bring in the Youth Criminal Justice Act, and youth, in many respects, are vulnerable.

Could you very quickly give us your thoughts on whether you think those provisions adequately protect the privacy and personal interests of Canadian youth?

Ms. Micheal Vonn: Could I get back to the committee on that? It's because I feel I have given insufficient attention to that particular aspect of the bill, being focused on other ones. We would be happy to share our views with you.

Mr. Sven Spengemann: I think it would be helpful.

Mr. Boisvert, if we can take advantage of your position, you'll have a lot to say about this. Canadian youth are vulnerable not only because they are youth, but also because they are preyed upon by terrorist organizations such as Abu Sayyaf, Al Shabaab, and ISIS.

Could we have your perspective on the protection of Canadian youth with respect to terrorist organizations that prey upon them, as related to the provisions in the bill?

Mr. Raymond Boisvert: I'll speak more perhaps at a higher level and from a practitioner's perspective.

I don't blame the Internet for radicalization, but it certainly is an important pathway and part of an ecosystem that leads somebody to falling prey to negative messaging.

I'd also like to underline, as it has been recently underlined once again in the United States in a more recent study, that the biggest threat of radicalization is actually the extreme right and not Islamic extremism. I think that's a very important piece.

Radicalization or extremism is extremism is extremism. It's the idea that we're now increasingly living in a world in which we're able to purvey hatred, and we can entice people and we can motivate them. The challenge for the security agency is that a person will come to their attention sometimes quite often through the issue of data exploitation and quite often through the issue of people posting online. Aaron Driver, the case in Ontario just about a year and a half ago, is a great example of that.

That's still an important toolset. The question is how to know when somebody goes from becoming radicalized—becoming incensed and thinking about it, maybe making some comments about mobilizing towards operational planning—to knowing when they really intend to do it. That's the big dilemma for the intelligence agencies and the law enforcement groups such as the RCMP that work together on those cases.

● (1305)

Mr. Sven Spengemann: The remaining time is very limited, but I have a very brief question, if I may.

The Chair: You have 13 seconds.

Mr. Sven Spengemann: You'll be the perfect person to answer this. What are your views on a Canadian youth who has been inside a terrorist organization and comes back onto our shores?

Mr. Raymond Boisvert: I think it's going to be a difficult and expensive process, because for one thing, it's difficult to understand. Once somebody has been exposed to extreme levels of violence, once they have been highly radicalized and have been schooled in warfare, you'd hope that they would have just had enough, that they've seen it and know they've made a terrible mistake. I think probably the majority are exactly in that kind of mindset, but how do you know?

If my responsibility is to keep Canadians safe, if I'm responsible for our counterterrorism program, we would say, “Well, we have to run this to ground to make sure that.... Let's go out and speak to that person as frequently as we can to get a better sense of what's behind their motives and whether they've turned the corner or whatever.” The expensive part is that you still have to afford some level, I think, of coverage in the early portions of that process, but you can't cover everybody. The number of persons who are of concern greatly outstripped the capability of the security establishment back in 2012, and I hate to even think of what it is today.

Mr. Sven Spengemann: Thank you.

The Chair: Thank you, Mr. Spengemann. I hate to bring this conversation to a close.

On behalf of the committee, I want to thank you for your thoughtfulness.

With that, we're adjourned.