HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 101 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Thursday, March 22, 2018

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Thursday, March 22, 2018

● (1100)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Let's get started.

This is the 101st meeting of the Standing Committee on Public Safety and National Security. Our witness this morning is the Honourable Harjit Sajjan, Minister of National Defence.

Welcome to the committee, Minister. You appear to be among many old friends. With that, I'll ask you for your opening remarks.

Hon. Harjit S. Sajjan (Minister of National Defence): Thank you, Mr. Chair.

I've actually had a little bit of de déjà vu this morning, given that I was at the defence committee and I see most of the same people here. It's nice to see everyone again.

I'd like to start by thanking all of you for the tremendous work that you have done in studying Bill C-59. These discussions and the experts you have talked to have helped inform the development of this important legislation, so thank you for all of your efforts.

I am accompanied today by Greta Bossenmaier, the Chief of the Communications Security Establishment; Shelly Bruce, the Associate Chief of CSE; and senior officials from CSE, National Defence, and the Canadian Armed Forces. It's our pleasure to be here today as you continue your review of the National Security Act, 2017.

This legislation demonstrates our government's recognition that the pursuit of national security involves two inseparable objectives: the protection of Canadians and the defence of our rights and freedoms. This commitment is apparent in part 3 of Bill C-59, which would establish stand-alone legislation for the Communications Security Establishment.

Last November, I had the opportunity in the House to speak to CSE's proud history of serving Canadians. For over 70 years, CSE has been Canada's foreign signals intelligence agency and the lead federal authority for information technology security in the Government of Canada. Over that long history, CSE has successfully adapted to remarkable change, including very rapid technological advancements and evolutions in the global threat landscape. However, what is needed now are modernized authorities to ensure that CSE is able to continue to adapt in this ever-changing environment both today and into the next 70 years.

In my remarks this morning, I'd like to underscore the importance of this legislation to ensuring that our security and intelligence agencies can keep pace with security threats, while at the same time enhancing accountability and transparency.

First, the CSE act would modernize the foreign intelligence aspect of CSE's mandate by allowing CSE to use new techniques to acquire intelligence through the global information infrastructure. CSE's foreign signals intelligence program is essential to keeping the government informed on matters of national security, national defence, and international affairs. These proposed changes will ensure that CSE is able to continue to collect this vital intelligence.

Second, as Canada's centre of excellence for cyber-operations, CSE operates at the forefront of changes in technology. The act would strengthen the cybersecurity and information-assurance aspect of CSE's mandate. Notably, the act would improve CSE's ability to defend important non-Government of Canada networks and to share cyber-threat information and mitigation advice. Taken altogether, the CSE act will strengthen Canada's cyber-defences by better protecting Canadians' most sensitive information and important cyber-networks from compromise.

Third, and of particular interest to National Defence, the technical and operational-assistance aspect of CSE's mandate would clarify that CSE is allowed to provide assistance to the Canadian Armed Forces and the Department of National Defence. This will enable CSE to better support Canada's military missions and the brave women and men of the Canadian Armed Forces serving in theatre.

Of course, CSE already provides important intelligence to the forces under the foreign intelligence aspects of CSE's mandate. This legislation would allow CSE to do more to help them to, among other things, conduct active cyber-operations in support of government-authorized military missions. Bill C-59 will enable CSE and the Canadian Armed Forces to better co-operate to ensure the best use of tools and capabilities to meet mission objectives.

The Department of National Defence and the Canadian Armed Forces look forward to the opportunity to work more closely with CSE to leverage its capabilities and expertise, as outlined in Canada's new defence policy “Strong, Secure, Engaged”.

I also want to discuss a crucial element of the proposed CSE act: foreign cyber-operations. I know that in her appearance before committee last month, the associate chief of CSE, Shelly Bruce, spoke to you about the active cyber-operations and exactly what they would look like in practice. Today I want to reiterate why these operations are important and why they are needed to protect the security of Canadians.

CSE's foreign cyber-operations mandate will provide Canada with the cyber-means to respond to serious foreign threats or international crises as part of a broader strategic approach.

For example, CSE would use active cyber-operations to prevent a terrorist's mobile phone from detonating a car bomb, or CSE could impede the ability of terrorists to communicate by obstructing their communications infrastructure.

CSE's active and defensive cyber-operations would be carefully targeted, by law, to the activities of foreign individuals, states, organizations, or terrorist groups that have implications for Canada's international affairs, defence, and security. Foreign cyber-operations would be subject to strict statutory prohibitions against directing these operations at Canadians, any person in Canada, or the global information infrastructure in Canada, and would require a robust approval process.

This brings me to my final point. This bill will considerably enhance oversight and review of Canada's national security and intelligence community, which includes CSE, the Department of National Defence, and the Canadian Armed Forces.

The oversight and review positions in the national security act demonstrate our government's commitment to enhancing lawfulness and transparency. I look forward to working with the proposed new bodies, including the national security and intelligence review agency and the intelligence commissioner.

By updating, clarifying, and clearly outlining in legislation what CSE is permitted to do, this legislation will empower Canadians to better understand what CSE does to protect Canada and Canadian interests. By adding new oversight and accountability measures, the national security act should also give you and all Canadians confidence that the measures are in place to ensure that CSE will continue to abide by the law and protect the privacy of Canadians.

To the members of the committee, I'm very proud of Bill C-59. This is very important legislation that will deliver on our government's promise to protect Canadians and their rights and freedoms.

Thank you.

● (1105)

The Chair: Thank you, Minister.

Before I go to questions, I want to say to members that I've taken a fairly generous interpretation of relevance on previous appearances by ministers, particularly on estimates and supplementary estimates. I remind all members that we are here to discuss Bill C-59, and I'm rather hoping that members will tie their questions in some manner or another to Bill C-59, however remote that tie might be.

With that, Monsieur Picard, go ahead for seven minutes, please.

[*Translation*]

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

[*English*]

I will ask my questions in French for those who need the earpiece.

[*Translation*]

Minister, it is a pleasure to see you and your entire team again. Welcome to the committee.

I have just come from a two-hour meeting of the Standing Committee on Access to Information, Privacy and Ethics, where representatives from Estonia talked about e-governance.

Clearly, beyond what is done on land, on sea and in the air, information is becoming the new battlefield. Big data is becoming a new target and a new playing field for conflicts between countries.

How will those new powers granted by Bill C-59 serve the CSE?

[*English*]

Hon. Harjit S. Sajjan: With Bill C-59, one of the things we started to address when we consulted with Canadians is making sure that we stay at the cutting edge of our technology. However, if we're at the cutting edge of technology, we need to make sure we have the right legislation to be able to adjust to the methods that are being used out there. Bill C-59 will finally allow CSE to be able to protect Canadians from foreign threats.

This is something that's very unique to this bill, because it has never been done before. What it also does is create a separate CSE act that gives exact direction on what CSE is able to do while at the same time putting a very robust mechanism in place to protect the privacy of Canadians.

From a policing perspective, I think Canadians are also looking for protection from identity theft with regard to how they do their banking. CSE has the ability and knowledge base to be able to assist Canadians with the right advice. It has already started to do that through its social media campaigns.

This is what this legislation is about; it's about protecting Canadians and Canadian interests.

● (1110)

[*Translation*]

Mr. Michel Picard: In this committee's previous discussions, we have received comments on the offensive dimension of certain powers or capabilities of the CSE. It is well known that groups that are terrorists or associated with terrorists, such as Daesh, benefit from online informal networks of sympathizers, structures and communications. This new armada or new equipment at the disposal of these terrorist groups represents an additional threat.

How should the offensive approach of the CSE be defined? How will this offensive approach respond to the new threat?

[*English*]

Hon. Harjit S. Sajjan: One aspect in particular that is extremely important, since the Minister of National Defence is also responsible for our Canadian Armed Forces, is that CSE will now actually have the ability to provide the right support to the Canadian Armed Forces. They obviously provided the right intelligence, but now with Bill C-59 they can provide the right expertise. They'll be able to leverage their knowledge base and their technology and keep up to date with some of the terrorist networks and what they're trying to do, especially when it comes to keeping our soldiers safe. That includes everything, as I mentioned, from somebody detonating an IED to disrupting the network to keep it from getting to that point.

We also have to be mindful that even with the best technologies, we had to wait for a cyber-attack on us to occur before we could actually do anything about it. We need to make sure that we are proactive in having a defensive mechanism so that when we see a threat we are able to shut it down beforehand. These are the things that are very important here to making sure that we protect our infrastructure in a very proactive manner.

[*Translation*]

Mr. Michel Picard: You talk about the CSE's support for the various operations, which are not military only. This support is necessary because of the disadvantage of being unable to respond quickly enough to an attack, thereby having to wait for the attack to take place before it can react. This new capacity will support various operations.

Will this support become a new instrument for conducting military operations around the world? Asking the question is sort of answering it.

[*English*]

Hon. Harjit S. Sajjan: Especially when it comes to our Canadian Armed Forces, this finally gives CSE the ability to assist our Canadian Armed Forces more correctly in this way. It puts us in line also with our Five Eyes partners. It was either overlooked in the past in previous legislation.... I actually found it quite surprising that CSE didn't have the legislative ability to assist the Canadian Armed Forces in this manner. Now with this bill the Canadian Armed Forces will be allowed to leverage the technical expertise of CSE.

[*Translation*]

Mr. Michel Picard: You are comparing our capabilities with those of our Five Eyes partners. Those new powers will enable us to be at the same level as our partners abroad, even ahead, if our technology allows it. By default, I take it that we have some catching up to do, and this bill allows us to do that.

[*English*]

Hon. Harjit S. Sajjan: Greta, do you want to answer that?

Ms. Greta Bossenmaier (Chief, Communications Security Establishment): Thank you, Minister.

Thank you, Mr. Chair and others, for being here this morning.

I think it's safe to say that Canada, allies, and countries in general are really facing a very dynamic cyber-threat environment. The technology has been changing. If you think back to when our legislation was first put in place some 17 years ago, this was before we were talking about things like cloud computing and artificial intelligence, the dynamic cyber-threat environment. Different types of actors were involved in the types of threats we're facing. I think it's safe to say that countries around the world, our allies, and Canada are all facing this very new dynamic threat environment.

As the minister said, this is really about putting the legislation in place that will allow us to have the authority to be able to operate and to protect Canada and Canadians in this new space.

To the question that was posed in particular—

● (1115)

The Chair: Unfortunately, we're going to have to leave it there and possibly work your answer into another question. We're out of time.

[*Translation*]

Mr. Paul-Hus, you have the floor for seven minutes.

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

Minister, welcome to the Standing Committee on Public Safety and National Security.

Bill C-59 states that you must work with the Minister of Foreign Affairs. We already know that, as Minister of National Defence, you have a close relationship with the Minister of Foreign Affairs. Probably weekly, you have to discuss a number of issues and the deployment of the Canadian Armed Forces around the world. I am wondering why the bill has to require you to contact the minister, since this co-operation is already part of your day-to-day work, I think.

There is a problem that you will surely be able to help me understand, given your close co-operation with the Minister of Foreign Affairs. It's about a security breach. I do not know how that expression will be translated, but as a former member of the military, you must know what I'm talking about. The incident took place in India, namely the invitation sent to Jaspal Atwal. We are hearing two contradictory stories. According to the Prime Minister, Mr. Atwal was invited by rogue elements in the Indian government. On your side, your colleague, the Minister of Foreign Affairs, confirmed that the invitation came from Canadian government officials. So we have two versions, that of the Prime Minister, to whom you are accountable, and that of the Minister of Foreign Affairs, with whom you work every day.

Which version do you believe?

Mr. Michel Picard: Mr. Chair, I have a point of order.

The Chair: You have the floor, Mr. Picard.

Mr. Michel Picard: I do not see the relevance of the question; it is not about the CSE's communications or role.

[*English*]

The Chair: I thought Mr. Paul-Hus was very clever in the way he introduced Bill C-59 into this question, but I do call relevance of his question as to the working relationship between the Minister of National Defence and the Minister of Foreign Affairs.

Hon. Harjit S. Sajjan: Mr. Chair, I will leave the second portion of the question for question period.

You raise a good point in terms of the importance of having the Minister of Foreign Affairs as part of this. I think it's absolutely prudent to do this. This is to make sure that when it comes to threats and any type of potential actions that we as the government can take, it's not just about one minister making that call. We need to make sure that we have a prudent look at the threats from different perspectives, especially that of the Minister of Foreign Affairs.

Yes, we do have have a very good, seamless relationship, but we want to make sure that at the same time that our relationship is extremely good.... We don't know about how the relationships. We can't rely on that. Canadians want to make sure that there is a good process in place, and that when governments make decisions of this nature, they have the right oversight and have been looked at properly when we take actions abroad.

[*Translation*]

Mr. Pierre Paul-Hus: Mr. Minister, I understand that you talk to the Minister of Foreign Affairs on a regular basis. The need to incorporate this co-operation into a bill is one thing. However, I would like to come back to the event in India.

You were on that trip. How did you see the situation? Do you know who's telling the truth? Is it the Prime Minister or the Minister of Foreign Affairs? Since you were there, you must have witnessed the events and you must be able to answer my question.

[*English*]

The Chair: You're welcome to comment on the relationship but possibly not the exact—

Hon. Harjit S. Sajjan: On the first portion of your question—I'll answer again—it is absolutely important to put it in legislation, so that, as in this case here, when a government takes its operations overseas—and especially when it comes to this very new field of the cyber-domain, in which technologies will continually change—we can be sure we have the right oversight on this. Canadians expect us to make sure we have this.

As the Minister of National Defence, I don't go on operations even with the military. It's a decision that's made through government. I am given authorities by cabinet to move forward, and that allows me, in this case here, when it comes to the cyber-domain.... It is a very prudent step to make sure that we work with the Minister of Foreign Affairs and that we have it in legislation. Canadians expect us, while protecting them, to make sure we have the right oversight and transparency moving forward.

[*Translation*]

Mr. Pierre Paul-Hus: Mr. Chair, since the minister cannot answer my question even though he was in India and is working closely with the Minister of Foreign Affairs, I would like to introduce the following motion, which I sent to the committee earlier this week:

> That pursuant to Standing Order 108(2), the Committee invite the Prime Minister's National Security Advisor, Daniel Jean, to provide the committee with the same briefing he gave to journalists on Friday, February 23, 2018, and that the briefing take place in public and no later than Friday, March 30, 2018.

I'm introducing this motion because the Conservatives and the New Democrats on this committee have serious questions about the Atwal case in India.

On February 23, the Prime Minister's senior adviser on national security told reporters that the officials responsible for the invitation sent to Mr. Atwal were officials from India. This created a diplomatic incident with India. On February 27, the Prime Minister confirmed in the House of Commons what Mr. Jean said. Then the Minister of Foreign Affairs mentioned that the invitation was from Canada's officials. The MP for Surrey Central, Mr. Sarai, confirmed that the invitation came from him. Mr. Atwal also confirmed that the invitation was from Canada, not from India. So we have two versions of the facts now.

Parliamentarians have the right to know what happened in India. The briefing was given publicly to journalists. We should be able to receive the briefing as well. That's why I think the committee should pass this motion.

In addition, Liberal members of the committee can vote independently, with full freedom of conscience. At his last appearance, the Minister of Public Safety and Emergency Preparedness confirmed that he was not responsible for giving direction to the committee and that its members were independent. If the Liberal members vote against the motion, we can assume that the Prime Minister's Office makes the decisions.

We need to shed some light on this. I think Liberal Party members would also like to shed light on this diplomatic incident that is serious for Canada.

● (1120)

[*English*]

The Chair: Thank you, Monsieur Paul-Hus.

We did receive the motion in a timely fashion. The motion is in order. It does bear similarities to your previous motion, which was rejected by the committee, but it is sufficiently different that it is a valid motion. Notwithstanding that the same subject matter is being debated in the House as we speak and you're not waiting for the resolution of the House debate, it is still in order and there is no impediment to this motion being debated.

With that, Monsieur Picard, go ahead.

[*Translation*]

Mr. Michel Picard: I think all diplomatic issues deserve to be taken very seriously. Furthermore, it is also the subject of debate in the House today. I think we have to wait until we know what will be said in the House and let the House get to the bottom of the issue as planned.

Under these circumstances, I request that the debate be adjourned.

[*English*]

Mr. Blaine Calkins (Red Deer—Lacombe, CPC): Can we get a recorded vote, please, Mr. Chair?

The Chair: I perceive that as a dilatory motion that is without debate; therefore, we call for the vote.

I am assuming that you want the vote recorded.

Mr. Blaine Calkins: Yes.

The Chair: With that, I'll ask the clerk to call the vote.

Mr. Michel Picard: Is it to adjourn debate, Mr. Chair?

An hon. member: It's to adjourn debate on the motion.

(Motion agreed to: yeas 5; nays 4)

The Chair: The motion has carried

With that, we go to Mr. Dubé.

Go ahead for seven minutes, please.

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

Minister, thank you for being here today, and thank you to the folks around the table as well.

My question—and you mentioned this in your comments—is about the capability sharing that's happening between CSE and the armed forces, in particular with regard to active cyber-operations. There have been concerns raised about the evolving landscape that was alluded to and what exactly that means for a civilian organization when you're talking about, in particular, foreign-state actors that might be involved in some of the activities that those active cyber-operations are being used against. It feels as if there might be a slippery slope there in terms of international law, as to what is military action and what is not.

I'm wondering if you could comment on that and perhaps explain how those capabilities go together and in what way we're making sure we don't have CSE as a civilian organization engaged in what other states might perceive as military attacks, especially with the concept of sovereignty being very nebulous in this digital age in terms of international law.

Hon. Harjit S. Sajjan: I'll let Greta speak to the technical side of things. However, I think I need to be very clear on this. We, in Canada, are leveraging a repository of phenomenal excellence that resides in CSE. With regard to the expertise that's here, we as a government, and previous governments, have kept it there for that reason, to make sure we stay at the cutting edge.

The Canadian Armed Forces, with the new legislation, will be able to allow us to leverage that technology. Any type of military action that's taken, as with any other military operation, will be conducted with the proper targeting procedures, the proper rules of engagement, and in accordance with international law and, more importantly, our laws as well.

● (1125)

Mr. Matthew Dubé: Before I get to the technical side for a more precise aspect, the bill calls for authorization by you, in consultation with the Minister of Foreign Affairs, for any active cyber-operation. Let's say there's a foreign state actor involved in the activity that requires that active cyber-operation. Can you walk us through the process of how you make the decision as to whether the Armed Forces should be intervening with their cyber-capability or whether it's CSE as a civilian organization?

Hon. Harjit S. Sajjan: Let's make a distinction in terms of whether it's a military operation that's providing.... For example, we're in Iraq right now. We have to look at the threats that are there. If a threat was developing capability in terms of creating a new type of IED, CSE will have the ability to support them on how to defeat that type of technology, and they will come out with that. But when it comes to active cyber-operations, it could be strictly, for example, that we as a government have to take some type of action to protect Canadians. That is a separate piece that CSE would be looking at. We have to separate the two. That will go through an appropriate process, as outlined in the legislation here, that will look at the proportionality, making sure that all the laws are respected, and a decision will be made.

Greta, do you want to add to that?

Ms. Greta Bossenmaier: Sure. Thank you, Minister.

When the National Defence Act was amended some 17 years ago to recognize the role of CSE, at that point CSE was actually part of the Department of National Defence. We've always had an assistance mandate, the so-called part (c) of our mandate, that allows us, upon request from another organization such as a federal law enforcement organization, to request whether CSE could be supportive of their work under their lawful mandate. Again, given that we were part the Department of National Defence, assistance to National Defence or CAF wasn't explicitly spelled out because we were part of that department.

About six years ago, to give a bit of history here, we separated from the Department of National Defence and became a stand-alone agency, the Communications Security Establishment, albeit still reporting to the Minister of National Defence. Therefore, this proposed legislation adds the Canadian Armed Forces and National Defence as an organization that could request our capability, request our support, as the minister explained, on one of their lawful missions. We would be in a support operation to the Canadian Armed Forces.

We also have representation here this morning from the Canadian Armed Forces. They may also want to speak to their operations.

Mr. Matthew Dubé: I appreciate that. My time is limited, so perhaps we can come back to that in a second. While the minister is here, though, I have a couple more questions.

We mentioned the mandate and the relationship with the Department of National Defence. That leads me to the question I asked the officials from Public Safety. We've spent a lot of time on this aspect of the bill. I think your presence here today is proof of the need to drill down on that aspect of it. This committee doesn't necessarily have the same kind of institutional memory that the committee of national defence would have. Can you explain why the decision was made to take a bill that essentially was moving on elements that were in the previous bill, Bill C-51 in the last Parliament, and essentially add this big block of stuff dealing with some significant changes to CSE as opposed to having it as stand-alone legislation?

Hon. Harjit S. Sajjan: I think it's very important that we demonstrate to Canadians, when we're looking at reviewing legislation of this kind, that we're looking at it in its entirety. We owe that to Canadians. We can't just look at it in a separate chunk. We need to be able to demonstrate to Canadians that we're looking after their security from foreign threats and making sure that they are educated and that we have the right advice for them to be able to be far more cyber-savvy as well while at the same time we are looking at, and making sure of, proper transparency and the protection of privacy.

● (1130)

Mr. Matthew Dubé: I appreciate that, Minister, even though I remain unconvinced.

The other point I want to get to quickly, with the minute I have left, is on publicly available information. The deputy chief mentioned last time that information obtained unlawfully would not be included under that definition. When we look at the situation right now with Facebook, for example, it's not quite clear whether that information was obtained unlawfully. Under the current definition, as spelled out in the law, could the type of information we're looking at in this scandal, essentially, fall under the definition of publicly available information that—

Hon. Harjit S. Sajjan: I can assure you that the CSE will...and that everything is followed in accordance with the law, and we make sure that we have the right processes in place. It's in here—

Mr. Matthew Dubé: I'm talking about information that is out there, that is obtainable, that's not necessarily obtained in an illegal fashion, and that is therefore technically legally obtained, even if it's nebulous at best. What happens in those situations?

Hon. Harjit S. Sajjan: I just want to make sure I got your question. You're talking about—

Mr. Matthew Dubé: I mean with, for example, Facebook.

The Chair: Excuse me, Mr. Dubé.

I apologize, Minister.

Hon. Harjit S. Sajjan: That's okay.

The Chair: That's an important question, and I doubt I'm going to get unanimous consent from the committee to extend your time, but if we could somehow or other circle back in on that question, that would be good.

Madam Dabrusin, go ahead, please.

Ms. Julie Dabrusin (Toronto—Danforth, Lib.): Thank you, Minister, for coming to speak with us today about Bill C-59. Cybersecurity is an issue top of mind for a lot of people, so it's a really important time to be talking about what we will be doing with CSE and how that will enhance cybersecurity.

There are parts in here about how CSE operates with critical infrastructure. It's not federal infrastructure. Can you explain how CSE will be able to use the new framework we have in Bill C-59 to provide assistance to non-federal infrastructure?

Hon. Harjit S. Sajjan: I will set the stage and let Greta get into the technical details of this. This is something extremely important. This is about protecting Canadians as they change to the technological advances of such things as new phones and social media, and making sure they have the right education about what they need to do to make sure they protect their own privacy in their own way.

More importantly, this is also about protecting the institutions Canadians use as well. That's critically important. Canadians expect us to make sure that everything from banking to our electoral grids operates properly and cannot be taken down. This is why it's important for us to work with non-governmental agencies to be able to provide the right advice to make sure they are protected, because ultimately this goes back down to making sure Canadians are protected.

Greta.

Ms. Greta Bossenmaier: Thank you, Minister.

I seem to always go back to history, but I think a little bit of history is important. For over 70 years, as the minister noted in his opening remarks, we have been in the business of protecting Canadians' most sensitive information.

Today, fast forward 70 years, we're now blocking on average every day over a billion malicious attempts to compromise government systems. We operate sophisticated cyber-defences on behalf of the Government of Canada on Government of Canada systems. That's our reality today.

We also provide advice and guidance and services to the public and to critical infrastructure owners about how best to defend themselves, everything from our top 10 actions that one should take to protect themselves in cyberspace to more detailed technical advice.

If a critical infrastructure owner were to request that CSE provide them with additional services to help protect them, for example when under attack, this proposed legislation would allow us to do that. The minister would have to designate the critical infrastructure owner as a system of importance to the Government of Canada. The critical system owner would have to make a written request to us. We would do it only at their request and if the minister had designated them as being critically important. It would allow us to use some of our sophisticated tools to help protect them. For example, if they were under attack from a malicious cyber-actor who was trying to steal their information or infiltrate their systems, this act would allow us to try to provide some of the sophisticated techniques and methods that we use to protect Canadians' information every day on behalf of the Government of Canada and to do that on behalf of critical infrastructure owners as well, for example.

Ms. Julie Dabrusin: Thank you.

I was reading a report by The Citizen Lab that made a number of suggestions about CSE and Bill C-59. I've referred to it a few times along the way. One of them was to allow federal institutions to opt out of cybersecurity advice and monitoring if they want to.

If there were such an opt-out, what would be the impact on your ability to provide cyber-defence?

● (1135)

Hon. Harjit S. Sajjan: I think it's prudent, especially in this day and age. What I'm sensing from my travels and from discussions I've had is that agencies want better protection, but more importantly, Canadians expect that, when they are going to be doing business with an entity, they will actually have the right tools and expertise to move forward.

I think we're going down that path, but I think if it is their choice, each institution will have to make their own choice on that.

Greta.

Ms. Greta Bossenmaier: You're absolutely right, Minister. This very much is upon the request of a critical infrastructure owner. Again, we put out a lot of, I believe, really important information, advice, and guidance that can be used by citizens and by critical infrastructure owners, for example, to better protect their systems and their information, but it's up to them to take that on board. We have a lot of interest in using that, but in terms of the new legislation, it definitely would be at the request of a critical infrastructure owner.

Hon. Harjit S. Sajjan: Can I just add to this? One thing that is very important is that CSE has been involved behind the scenes in protecting Canadians in this manner, but it's only recently that the vice-chiefs have been very open, getting out their social media, making sure that Canadians understand what they need to do. I think this is the thing that's been very important. We are shifting the landscape as well, to demonstrate to Canadians that CSE is a phenomenal agency with the right expertise that's recognized by our Five Eyes partners as being top in the world. More importantly, we have Canadians protecting Canadians, so they can have tremendous confidence in what they do. The advice that's given is actually having an impact, especially the top 10 list.

Ms. Julie Dabrusin: Budget 2018, in fact, allocated $115 million for a Canadian centre for cybersecurity. How does that tie into what we're looking at right here when we're talking about Bill C-59 and CSE?

Hon. Harjit S. Sajjan: This is about keeping up to date, with us as a government making sure that all our agencies have a place where they can go for the right expertise, and creating a cyber centre of excellence, at which you have the expertise of CSE to make sense of this for us. This is going to provide not only a one-stop shop that can allow agencies to come and Canadians to know how to deal with threats....

Greta, do you want to add something?

Ms. Greta Bossenmaier: Budget 2018 did propose a Canadian centre of excellence for cyber. It would be housed within CSE. It would bring together the operational components within the government of Canada that work on cybersecurity operations. Very much to the minister's point, it would provide a one-stop shop of expertise—to use that terminology—a place where the Government of Canada, Canadians, and Canadian infrastructure could go to get that trusted advice, guidance, and services.

The Chair: Thank you, Ms. Dabrusin.

Mr. Motz, you have five minutes. Go ahead, please.

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

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

Minister, given your role within C-59 and as Minister of Defence, did you hold any meetings with your counterparts about national security or Bill C-59 on your tour of India?

Hon. Harjit S. Sajjan: If you want to know about my trip to India, I was disappointed that I didn't get to visit the village where I was born.

Mr. Glen Motz: So you're not going to answer the question. Let me ask it a different way.

Bill C-59 requires you, as the Minister of Defence, to consult with Foreign Affairs on anything related to CSIS or CSE.

Hon. Harjit S. Sajjan: Could you repeat that?

Mr. Glen Motz: Bill C-59 requires you, as the Minister of Defence, to have interactions and contact with Foreign Affairs on CSIS matters and CSE matters. Given the fact that the national security adviser was asked by the PMO to brief the press, I'm wondering whether you were consulted on that. If you were not, should we write into this bill that the national security adviser should not brief the press until he has first consulted you?

The Chair: Minister, given my previous discussions with all members that we are here to discuss Bill C-59 and notwithstanding the cleverness with which Mr. Motz has phrased his question, I would encourage you, Minister, to answer the first part of the question, but as to any travels—

● (1140)

Hon. Harjit S. Sajjan: It's getting more difficult to figure out what the different parts of the question are. If you could rephrase that Bill C-59 piece, I'd be happy to try to answer it for you.

Mr. Glen Motz: Again, I'm going to ask the same question because, respectfully, Mr. Chair, this is related to Bill C-59.

It's related to your role as Minister of Defence and your role within Bill C-59. It has to do with Foreign Affairs. Given the fact that we have seen the national security adviser brief the press before he briefs you—and I take it by your non-answer that you were not consulted before he briefed the press—I'm wondering whether there should be some amendments to this legislation—because it doesn't provide us any direction on who the national security adviser should talk to or who he should consult before he does brief the press—to ensure that doesn't happen in the future.

Hon. Harjit S. Sajjan: My responsibility as Minister of National Defence is national defence, the Canadian Armed Forces, and CSE.

Mr. Glen Motz: That's it. So you weren't consulted, then, when this particular...?

Hon. Harjit S. Sajjan: I'm giving you my answer in terms of what my responsibilities are.

Mr. Glen Motz: That's interesting.

Terrorism certainly is part of Bill C-59. Part of your responsibility as Minister of Defence, as well as the primary focus behind Bill C-59, is to protect Canadians.

You were at the event in India with Mr. Atwal. Did that not raise any alarm bells for you on national security issues?

Hon. Harjit S. Sajjan: When it comes to threats on a daily basis around the world, I look at making sure that, as Minister of National Defence, I have the right resources in the right place to make sure that we're able to interpret the various threats. That's what we'll continue to do. That's what Bill C-59 is about.

On this point—

Mr. Glen Motz: Given that comment, Minister—

Hon. Harjit S. Sajjan: This is how important it is.

Mr. Glen Motz: Sorry, I have limited time.

Given the comment you just made, is it fair to suggest then that...? Being that you're responsible for national security issues, did you launch an investigation into what happened in India with the Atwal affair?

The Chair: At this point, Minister and Mr. Motz, the phrasing of your current question has almost nothing to do with Bill C-59. I'll just point out that we've not yet passed this as legislation, so it's not —

Mr. Glen Motz: Fair enough.

The Chair: With that immense guidance from your chair, I would ask you to continue by asking another question.

Mr. Glen Motz: In your opinion, Mr. Minister, who is the top person for national security in this country? Is it you, as Minister of Defence? Is it Minister Goodale? Is it the Prime Minister? Who, in your estimation, is the top person for national security?

Hon. Harjit S. Sajjan: When it comes to national security, this is one of the reasons why in a government we have things that are also.... For example, the Minister of Public Safety is responsible for the security within Canada. That's why I, as the Minister of National Defence, look at foreign threats. This makes sure that there is a separation, but at the same time, on request, we can provide the right level of support.

For example, with forest fires, we can provide a domestic response if there's a threat, if that's needed. If there's terrorism, I need to make sure that our special forces, our capabilities, are there if needed, upon request, inside Canada.

This is something that I look at very seriously every single day, and it's a responsibility that is shared by me, Minister Goodale, and also the Minister of Foreign Affairs. We're constantly working together. More importantly, our officials constantly work together to make sure that we keep Canadians safe, and that's something that we take extremely seriously.

The Chair: Be very brief, please.

Mr. Glen Motz: In your testimony, then, you're saying that you, the Minister of Foreign Affairs, and the Minister of Public Safety are the only ones who.... The buck stops with you three with respect to national security and not with the Prime Minister or anyone else.

Hon. Harjit S. Sajjan: When it comes to security, it's the government's responsibility to keep Canadians safe, and that's exactly what we do.

The Chair: Thank you, Mr. Motz.

Thank you, Minister.

Mr. Fragiskatos, you have five minutes. Go ahead, please.

Mr. Peter Fragiskatos (London North Centre, Lib.): Thank you, Mr. Chair.

Thank you to the Minister and to the officials for being here today.

My questions will focus on Bill C-59 and cybersecurity.

First of all, Minister, you said in your comments when you opened things that cyber-operations "would be subject to strict statutory prohibitions against directing these operations at Canadians, any person in Canada, or the global information infrastructure in Canada, and would require a robust approval process." To me, that's very much in line with democratic principles, but could you speak to the importance of that, to ensuring that when we have legislation, when we're talking about CSE and its powers, that those powers are consistent with democratic principles?

● (1145)

Hon. Harjit S. Sajjan: Absolutely, and in fact, this is extremely fundamental. I was trying to address that in the answer that I gave about my responsibility with regard to CSE and the military's focus on foreign threats, and that's where CSE's at.

However, with what CSE currently has and with Bill C-59, we'll have additional ability to provide support for other agencies with judicial authorization. I think what's extremely important is making sure that we as a government leverage all the right resources within our government and within the laws. However, at the same time—and I want to stress this immensely, because Canadians expect this—we must have a process in place that respects privacy and transparency. This is something that hasn't happened before. More importantly, we are the last Five Eyes nation to finally come up to that transparency level.

Greta, do you want to add anything to that?

Mr. Peter Fragiskatos: By all means, go ahead.

Ms. Greta Bossenmaier: If I take your question, particularly around the foreign cyber-operations, active cyber-operations, and defensive cyber-operations, I'll say that it's very clear in the legislation. There are two pieces that I would draw folks' attention to. One is the strict approval processes that would need to be put in place. Active cyber-operations would require the approval of both the Minister of National Defence and the Minister of Foreign Affairs, given that these are operations that would be happening outside of Canada, not in Canada, so there would be Foreign Affairs implications or considerations as well. That's on the approvals side.

Also, in terms of the limitations, there are very clear limitations as to what an active or a defensive cyber-operation could entail. CSE would be prohibited, for example, from directing its active cyber-operations at Canadians, at any person in Canada, or at the global information infrastructure. It would have to be sure that it is not causing death or bodily harm, or wilfully obstructing justice or democracy. There would be significant, serious, senior-level approvals in addition to very clear limitations on what those activities could be.

Mr. Peter Fragiskatos: Thank you very much, Minister.

I want to ask you about your assessment of the current threat environment that we face. Traditionally, threats to national security have been understood in terms of states posing a primary threat, rogue states in particular, but non-state actors have now come onto the scene, in particular, terrorist movements. Now we're talking about cybersecurity. All of these issues exist in the threat environment. Where does cybersecurity rank for you in terms of risks to our national security?

Hon. Harjit S. Sajjan: In the overall context, we have to look at current threats, threats that are potentially emerging, and what we can predict as future threats. This is the responsibility of the government, to make sure that we have the right resources to be able to deal with threats today and tomorrow.

We've been dealing with non-state actors for some time, as well as with state actors.

Cyber is a significant concern, but I also want to say that, because we have done extremely well in Canada, CSE has the ability, the expertise, to give Canadians the assurance of tremendous safety when it comes to cyber. However, as you know, with technology, we need to stay at the cutting edge.

My bigger concern, I'll be honest with you, with nations like Russia, is how they can take cyber and what we call hybrid warfare, such as with what's happening in Ukraine, and try to manipulate and influence populations. That is a concern and not just strictly from a government perspective. We have to make sure we educate our citizens and our media. We've noticed this, and we are actively engaged in making sure that we speak with the right nations who have good experience with this, and that's the reason we're making the right investments in the right area. We're looking at the really tough threats, but at the same time, we have to be looking at the emerging threats out there as well.

Mr. Peter Fragiskatos: Thank you, Minister.

The Chair: Thank you, Mr. Fragiskatos.

Mr. Calkins, you have five minutes. Go ahead, please.

● (1150)

Mr. Blaine Calkins: Thank you, Mr. Chair.

Minister, thank you for being here today. We truly appreciate it.

This is just a point of quick clarification. At any point in time, in your role as Minister of Defence, have you ever held back, requested, or asked that any officials, from either your area of expertise or anywhere else within the Government of Canada not testify before any of the standing committees before the House of Commons?

The Chair: Could you tie that to Bill C-59?

Mr. Blaine Calkins: The Minister of National Defence needs to consult with the Minister of Foreign Affairs, under part 3 of Bill C-59, and will now be junior in that role if the act does come to pass, and will need the advice of the Minister of Foreign Affairs to make decisions. I'm asking right now, given that link, whether he has been advised by the Minister of Foreign Affairs per se. Has he had any conversations with any of his ministerial colleagues? Has he had any conversations with any of his colleagues who are members of the legislative body and not members of the executive with regard to who should or shouldn't appear before a standing committee of the House of Commons?

The Chair: Bearing in mind the issue of national security here, I'll let you answer that in the absence—

Hon. Harjit S. Sajjan: I'm sorry. My policing experience of listening to how people talk and question is coming in here.

I see where you're trying to go with this, and I can assure you, when it comes to the Minister of Foreign Affairs and me, we have a very good relationship when it comes to looking at threats. That's what Bill C-59 is focused on, making sure that we keep Canadians safe but at the same time give Canadians the confidence that their privacy is going to be looked after. More importantly, finally we have CSE being given the ability to leverage their expertise. That wasn't there before, especially when it came to Bill C-51.

Mr. Blaine Calkins: But my actual question was whether you had ever advised anybody not to speak to department officials. It's a non-threatening question. I would have assumed that your answer would have been no, that you'd never done that, but I didn't get that answer, which is unfortunate.

Given your responsibilities for the Communications Security Establishment, to your knowledge, what threat, if any, do so-called rogue elements of the Indian government present to the reputation of the Government of Canada?

Hon. Harjit S. Sajjan: When it comes to threats, as I said, on a daily basis we look at threats from around the world. We keep monitoring on a regular basis and making sure that we mitigate anything. I work very collaboratively with Minister Goodale on this, and more importantly, our officials work very collaboratively on this to make sure we keep Canadians safe.

Mr. Blaine Calkins: You gave me a very general answer to a very specific question, so I'll ask the question again. Given your responsibilities for the Communications Security Establishment, what threat, if any, do so-called rogue elements of the Indian government specifically present to the reputation of the Government of Canada?

Hon. Harjit S. Sajjan: One thing that Bill C-59 will do is to make sure we give CSE the right tools, the legislative ability to be able to leverage their technical ability to keep Canadians safe from all threats and emerging threats.

Mr. Blaine Calkins: If we're talking about the abilities then, is there anywhere in the National Defence Act, in comparison to what we're doing here with Bill C-59, that the defence minister has to ask permission of any other minister, and the foreign affairs minister specifically, to carry out any operations?

That's kind of a yes or no. Is there anywhere in the Defence Act that says you need the permission of the foreign affairs minister to conduct any operations?

Hon. Harjit S. Sajjan: We as a government and I as the Minister of National Defence, when it comes to what we do overseas, for example—

Mr. Blaine Calkins: I'm asking a very specific legislative question, Minister.

Hon. Harjit S. Sajjan: I'm trying to understand—

Mr. Blaine Calkins: To your knowledge, is there any place in the Defence Act where it's legislated that you would need to consult or need the permission of another of your colleagues in order to carry out any lawful duties within the Defence Act?

Hon. Harjit S. Sajjan: I cannot conduct operations overseas without cabinet approval. Once I'm given my authority, that gives me the ability to be able to conduct—

Mr. Blaine Calkins: In the act.

Hon. Harjit S. Sajjan: —the operations.

Mr. Blaine Calkins: That's just the MO of how business is operated. When we go to Bill C-59, part 3 says that you must consult with the Minister of Foreign Affairs.

My question to you is, has the Minister of Defence's role been diminished to being a junior minister to the Minister of Foreign Affairs? If so, why would we want to set that precedent?

Hon. Harjit S. Sajjan: I can assure you that when it comes to the actions that are taken by our government, we are given the appropriate authorities. This gives the Canadian Armed Forces and CSE the authority to act.

The other aspect of what our government has done is to make sure that we have fully funded our Canadian Armed Forces to be able to meet those needs.

More importantly, it gives CSE, within Bill C-59, the legislation to now be able to actively protect Canadians, whereas it couldn't before. Your previous government, at the time of Bill C-51, neglected to do that.

● (1155)

The Chair: Thank you, Mr. Calkins.

Ms. Damoff.

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

Minister, it's wonderful to have you here at the public safety committee, so welcome, and welcome back to the officials who are here.

Bill C-59 allows you to conduct active cybersecurity operations against hostile foreign entities. We had some discussion when your officials were here last time about the global infrastructure. I have concerns about how the data of Canadians could get swept up in that, for example, if I'm on holidays in London, England, and you're conducting an operation and I get caught up in that.

You're dealing with strictly foreign entities. What safeguards do we have in place to ensure that you continue to be dealing with strictly foreign entities, as opposed to Canadian citizens?

Hon. Harjit S. Sajjan: That's a really good question. When I became minister, I was walked through the actual process that we currently have now. It is extremely robust.

We do have a responsibility. If information is accidentally collected, there is a very strict process that is taken. More importantly, the current process that the CSE commissioner goes through to make sure that information....

I want to make sure I get this right, so I'm going to pass that on to you, Greta.

Ms. Greta Bossenmaier: Thank you, Minister.

In terms of active and defensive cyber-operations, which I believe was the nature of your question, this legislation, the proposed law, says that CSE will not be able to direct active or defensive cyber-operations against Canadians, against any person in Canada, or at the global information infrastructure in Canada. It's part of the legal framework we'd be operating under.

In addition, as I mentioned before, these operations would require senior-level approvals and, as the minister has mentioned, review by the new national security and intelligence review committee and also the committee of parliamentarians that has been put in place.

By law, the activities we would undertake could not be directed at Canadians or Canadian infrastructure, or anyone in Canada.

Ms. Pam Damoff: I guess that's where I have the disconnect, though, because how do you know they're Canadians? When you're dealing with the cyberworld, how do you know who is a Canadian versus who is foreign?

I'm not an expert on the cyberworld to any extent, but you're not dealing with a physical person; you're dealing with an entity in the cyberworld. How do you know whether that's a Canadian or not?

Ms. Greta Bossenmaier: Shelly, do you want to talk a little about it, more from a collection perspective?

Ms. Shelly Bruce (Associate Chief, Communications Security Establishment): If you think of an active cyber-operation or a defensive cyber-operation as a plan that has been pulled together, it doesn't happen spontaneously. A lot of research and a lot of analysis have to go into getting to the point where you have an idea of what you could do online in a defensive or disruptive action.

The information that leads up to that plan, that informs that plan, is going to be the information that is pulled together through our foreign intelligence mandate and by understanding the players and the infrastructure that are involved. It could be from our cyber-defence mandate and understanding how the Internet works and which servers are configured in which way and how they interact.

It would have to be a very well-informed, thought-through plan in which you'd look at downstream implications. The intelligence commissioner is working at the beginning of those processes and helping to ensure that the ministerial authorizations that are allowing us to gather that information are sound, reasonable, and proportionate, in addition to all of the measures that go into it. We have protections for privacy in that space as well.

Ms. Pam Damoff: I have only about a minute left, and I want to get in another quick question.

Minister, in the last budget there was a fairly significant investment in the national cybersecurity strategy. Having the legislation is one aspect, but I'm wondering if you can speak to how those kinds of investments will assist in the work you're doing.

Hon. Harjit S. Sajjan: They're absolutely critical. The right investments are going to allow us not only to operate at the proper capacity and have the cyber centre of excellence but, more importantly, to stay at the cutting edge of technology. That aspect is so important.

There's one thing I tried to stress early on. It's about our people. You can have the best technology, but it's actually developed by people. I want to stress that the people who are at CSE....

You won that award again, right?

Ms. Greta Bossenmaier: We did.

Hon. Harjit S. Sajjan: It's one of the top employers in Canada again.

This ability to track the best is absolutely amazing. This is one of the reasons we've been able to stay at the cutting edge, but it requires research and development and the right network to do so. This investment is the step that's going to keep us at the cutting edge.

● (1200)

The Chair: Thank you, Ms. Damoff.

I could actually see the clock as three minutes slow for Mr. Dubé if he wished to pursue his final question.

Hon. Harjit S. Sajjan: We're looking at the clock, but that's the official clock, is it?

The Chair: Yes, well, there's the official clock and then there's the clock that I see.

Mr. Dubé, you can finish off your question.

Mr. Matthew Dubé: It's the first time I've ever liked daylight saving time.

Voices: Oh, oh!

Mr. Matthew Dubé: Really quickly, I have just one question. I want to get back to the details I asked about on the Cambridge Analytica situation with Facebook.

There's clearly not a situation here of the information having been obtained illegally. It's nebulous, and perhaps dubious and immoral, but it's not quite clear that it's illegal. Information like this that is being obtained and being used by political parties in a variety of countries around the world arguably could fall under the definition of publicly available information. How do you see that, Minister, and how does CSE see that?

Hon. Harjit S. Sajjan: For CSE, the credibility of the great work they do and the credibility of any government to be able to function in a rules-based order is based on working within the law. That's exactly how CSE has been functioning.

More importantly, we're actually putting even more robust measures in place to make sure that CSE's activities and the activities of all our security agencies are done and that we have a mechanism in place for everything from the intelligence commissioner authorizing ministerial authorization to the national security and intelligence review agency and now actually having parliamentarians from all parties.

My answer to you is that CSE will always function within the law.

Mr. Matthew Dubé: I appreciate that, Minister. If we're talking about operating legally, and this information is obtained legally—although arguably the laws should be changed in that context—doesn't that mean that CSE could obtain that information under publicly available information?

Hon. Harjit S. Sajjan: As I stated, not only from a legal perspective, CSE's activities are designed to make sure that we are protecting Canadians and Canadian interests, and we will continue to do so.

Mr. Matthew Dubé: I appreciate the chair's indulgence. I'll leave it there.

The Chair: Thank you, Mr. Dubé.

Minister, on behalf of the committee, I thank you for your appearance here. With that, we will suspend to let you leave.

Everybody else, please stay, and we'll continue, because the time is precious.

Again, thank you.

● (1200)

(Pause)

● (1200)

The Chair: I will ask members to return to their seats.

I'm going to work on the assumption, Ms. Bossenmaier, that there are no further statements to be made and we can simply proceed to questions.

Ms. Greta Bossenmaier: That's correct, Mr. Chair.

The Chair: With that, Mr. Fragiskatos, you have seven minutes. Go ahead, please.

Mr. Peter Fragiskatos: Thank you very much, Chair.

The first question builds from the conversation I just had with the minister, on the place of cybersecurity conversations with our allies. Certainly this is happening on a minister-to-minister level, but in terms of officials collaborating and having conversations, certainly that's taking place, I imagine. Where are we in terms of a priority on that? There are so many threats to national security.

● (1205)

Ms. Greta Bossenmaier: Absolutely cybersecurity is more and more a topic of conversation with our allies, with our partners. I don't think a meeting with our colleagues and with our allies goes by when we're not talking about cybersecurity now. Again, IT security has been part of our mission for 70 years, with the new demands and the frequency and the new kinds of challenges. For sure the nature of the discussion and the importance of this issue across the various issues that we deal with within CSE has risen.

To your point, there's definitely a high level of priority and a lot of conversation and a lot of sharing of best practices as well. I think one of the things we all appreciate is that in this domain no one has all the answers. The more we can share best practices, look at lessons learned, and bring various capabilities to the table the more those really enrich the conversation.

Where cybersecurity fits within other types of threats, I think, is a question this committee and other committees have asked, and I know some of my colleagues in other organizations have also answered that. We focus on the intelligence priorities the government sets. Cyber for sure is one of those key issues we deal with, but it's part of a broader landscape of intelligence priorities we work against, based on what the government sees as the priorities of the day.

Mr. Peter Fragiskatos: Could you point to a best practice? Obviously, these are sensitive security measures, but have you gained something from the conversations that you could point to to say that it is the result of collaboration with our allies and that this is why having conversations on these matters is really important?

Ms. Greta Bossenmaier: I'll just point to the new Canadian centre for cybersecurity that was mentioned in budget 2018 and that has been brought up a number of times around this table today.

A number of our allies who moved to this kind of model when they saw that they needed to integrate within their own cryptologic agencies—our sister organizations—to consolidate their cyber-operations' capabilities within their cryptologic agencies, see a couple of things. Number one, I think they see the need to have a unified, trusted source, and a single source of information, advice, and guidance, a place for their citizens and their businesses to be able to turn to.

Number two goes a bit to the minister's earlier comments about expertise. I feel very fortunate for the men and women who work in CSE, truly some of the best and brightest minds in our country, whether they be mathematicians or engineers or computer scientists or linguists, who are dedicating their time and attention to work in CSE and to bring their capabilities and skills to bear. Again, one of the best practices, I think, we've seen from allies is to consolidate their cybersecurity operations within the sister organizations to CSE and to truly leverage the skills and capabilities they have to be able to better protect their own citizens.

Mr. Peter Fragiskatos: Thank you very much.

We heard the minister speak about threats to our security, from a cybersecurity perspective, emanating from state actors, rogue states in particular, and non-state movements such as terrorist organizations. I wonder if you could speak to whether or not cyber-attacks take a different form, depending on whether they're launched by a state actor or by a terrorist organization. I think there could be a perception that terrorist organizations are not capable of carrying out very sophisticated sorts of attacks. That is changing. The fact is they can mount sophisticated attacks. It wasn't the case before, but now we're seeing that. Could you speak to that?

Ms. Greta Bossenmaier: Sure.

I'm going to ask Scott Jones, our deputy chief of IT security, to come in on this as well. Without stealing all his thunder, before I offer him that opportunity to speak, I'll just say that one of the things Scott often talks about is that now we're seeing a wide variety of cyber-threat actors. Yes, we've been worried about nation states for a long time and non-state actors, as you mentioned. We're worried about hacktivists, cybercriminals. In Scott's portfolio, in defending the Government of Canada's systems and providing advice and guidance to Canadians and Canadian critical infrastructure, he often says we have to protect and defend against this whole variety of threat actors. They are diverse, but our responsibility is to be able to protect Canadians' information and Canadians' most private information from this variety of threat actors.

With that, I'll ask Scott to speak a little about the threat environment he sees.

● (1210)

Mr. Scott Jones (Deputy Chief, Information Technology Security, Communications Security Establishment): Just building on that, I think some of the key points are that the cyber-techniques are within the reach of anybody, and that's more a result of the resilience level that we all face. There are simple actions we've been trying to promote that we can all take to make ourselves more resilient against any sort of actor, because to your point, no matter who they are, cyber-techniques are within their reach. These are our top 10, some simple things we can all do to increase our resilience.

The second piece of that is how we are able to purchase things that are better and more secure from the start. That's some of the work we do internationally. To your previous question about working internationally, there are things like asking for products to have better security features, things that are secure by default, things we don't have to worry about. One example of that is the common criteria program we have with 27 different nations.

How do we then share information quickly to let people take action on our behalf? We can't necessarily rely on ourselves. Some of these techniques are really sophisticated, but we can look at critical infrastructure to help us raise that bar.

Mr. Peter Fragiskatos: You said something there, and I'm going to stop now, because the chair has said I've run out of time, but thank you very much for the....

The Chair: Thank you for your timely look at the chair.

Mr. Motz, go ahead.

Mr. Glen Motz: Thank you, Mr. Chair, and I can assure the chair that I might be more focused on my questions in this round.

The Chair: We always appreciate focus. I expect penetrating questions from you.

Mr. Glen Motz: In part 3 with regard to clause 76

> Activities carried out by [CSE] in furtherance of the foreign intelligence, cybersecurity and information assurance, defensive cyber operations or active cyber operations aspects of its mandate must not be directed at a Canadian or at any person in Canada.

As we know, the Internet is full of encryption; it's full of IP modifiers; it's full of virtual private networks, and on and on and on and on.

How will you be sure you aren't targeting a Canadian? How do you go about doing that? And here's a follow-up question, if I may, so you can answer them both. If you come across propaganda in the case of a known ISIS terrorist, and the person is spreading mass propaganda to Canadian citizens from a foreign country, would you then have to refrain from using cyber-operations and let that information get out to Canadians? How do you interpret the bill to manage that nuance?

Ms. Greta Bossenmaier: I'm going to start with the first answer, and I'll likely also look to Shelly Bruce, the associate chief, to chime in on this one. Then I think I'll have to come back to your second question just to be sure I've captured it.

In terms of your first question, you're absolutely correct that the legislation as it is proposed—and actually our current legislation as well—prohibits us in law from directing our activities at a Canadian or at anyone in Canada. We're focused on foreign targets in foreign lands, hence the foreign intelligence aspect of our mandate. Having that focus on foreign intelligence is something we've been doing for over 70 years.

This is a bit of the discussion that Shelly has already started in terms of how we actually ensure that we are focusing our efforts on parts of the information infrastructure that are outside of Canada. Ensuring that Canadians are not involved is a process that the foreign intelligence analysts go through.

With that, Shelly, I'll turn it over to you to provide a bit more information regarding how we ensure that.

Ms. Shelly Bruce: Sure. You've referred to both the foreign intelligence mandate and the active cyber-operations aspect of the proposed authorities. I can maybe start by speaking about the foreign intelligence side.

Before any activities are undertaken, there is a really robust process in place around policies and training and testing. Every analyst does an online test and is not allowed access to any systems until they are very cognizant of all of the restrictions and the requirements to ensure that they are directing their activities against foreign entities outside of Canada and in a way that is consistent or directly related to an intelligence priority that the government has. There are three tests—

Mr. Glen Motz: I'm sorry, but let me go to my second part of the question.

You become aware of terrorist propaganda being launched at Canadians, but it's by a Canadian on foreign soil. How do you interpret the act as being able to respond to that? Do you have to let it go or can you respond?

● (1215)

Ms. Shelly Bruce: We are prohibited from targeting Canadians anywhere, so if there is a direct correlation, and that activity is emanating from a Canadian's communications, it's off limits.

Thank you.

Mr. Glen Motz: Thank you for that.

Given the fact that we live in a new environment now, we have Canadians who, whether they are homegrown terrorists or they've gone away and come back, pose a threat, will pose a threat, and continue to pose a threat to national security. In your experiences collectively as a group, is there something we need to do to change things so that, if there is an imminent threat to Canadians by a Canadian, you can do something about it?

Ms. Greta Bossenmaier: Maybe I'll start by answering your question, and then, again, we'll look to Shelly to further my description.

It goes back to mandate. The Communications Security Establishment's mandate is foreign signals intelligence that's not directed at a Canadian or anyone in Canada, which is a foreign focus. Suffice it to say that there are other pieces within the national security apparatus that focus on threats to Canada that may emanate from a Canadian. Some of our partners in that....

Shelly, do you want to speak a bit about how we work with partners in that regard?

Ms. Shelly Bruce: Looking at terrorist activity is very much a team sport in Canada. The RCMP, CSIS, CSE, as well as others each have a role, and we work together to understand what each of us is bringing with our mandates, authorities, skills, and capabilities. In this case, it may be within the services' remit to be looking at a Canadian outside of Canada who was involved in these activities.

Our legislation currently allows us to provide an assistance role to the RCMP and CSIS. Generally it is for national security agencies and law enforcement agencies, but in practicality, it is mostly CSIS and the RCMP. In that case, if they had the authority, they could ask us for assistance in that space, and we could use our capabilities to assist them as long as it was done within the parameters of whatever legal authority they're operating under.

Mr. Glen Motz: Last year we learned that Canada's National Research Council was the victim of Chinese computer network exploitation. The damage was in the hundreds of millions. Under your direction, as given in part 3, clause 76, what sorts of things will you do as the chief of CSE to curb these attacks and protect the integrity of our tax dollars?

Ms. Greta Bossenmaier: A key part of our mandate is around cybersecurity, and it was a core part of our mandate well before this new proposed legislation. One of the cornerstones of what we do is to try to protect, as well as we can, the Government of Canada systems and, more so even with this legislation, systems of importance to the Government of Canada.

I mentioned in my earlier remarks that right now, through the technology and people we have, CSE is deploying very sophisticated cybersecurity defences on Government of Canada networks. Those help us on a daily basis. I've already quoted that we're blocking up to a billion malicious actions per day. The magnitude of these malicious cyber-actions is extremely high, so we work every day to block those actions.

When something actually happens—and we always say that no one is immune in this environment as it's a very challenging environment—we also have a very important responsibility. We work with the implicated department, for example, and with others across government to ask how we can remediate this as quickly as possible to ensure that information is being protected and that services are back up and running.

The Chair: Unfortunately, Mr. Motz, we're going to have to leave it there. I apologize.

Mr. Dubé, you have seven minutes. Go ahead, please.

[*Translation*]

Mr. Matthew Dubé: Thank you, Mr. Chair.

I want to go back to the question I asked the minister, but to which I did not get an answer, in my opinion.

In a context where the information can be obtained legally by a company, such as Cambridge Analytica, even if it can be said that it is immoral and that it should be illegal, does that correspond to the definition of publicly available information?

● (1220)

[*English*]

Ms. Greta Bossenmaier: The whole issue around publicly available information, I understand, has been considered around this table. I'll just try to perhaps add a couple of pieces to it.

For us, mandate is critical. Mandate matters, and it matters throughout the entire piece of legislation that is in front of you, and that includes publicly available information. We can use publicly available information only if it is related to our mandate, our foreign signals intelligence mandate or our cybersecurity mandate. We do not have within our legislation, currently or proposed, any mandate to focus our activities on Canadians, to have an investigative capability, to create dossiers on Canadians. That is not within our current or proposed legislation.

I would start with the fact that mandate matters.

The second piece I would relate is that, as I think has been raised before here, publicly available information—and it's defined in our act—would not comprise information that has been hacked or stolen. This is information that would be publicly available to any Canadians.

Also—

Mr. Matthew Dubé: If I may, before you continue—

Ms. Greta Bossenmaier: Yes.

Mr. Matthew Dubé: The part of the bill dealing with publicly available information specifically exempts the prohibition on targeting Canadians. So you might not be actively collecting it, but you are permitted to collect it as part of the research that's being done under clauses 24 and 25, if I'm not mistaken.

You mentioned information that's hacked or stolen, but under the current legislation, arguably, the information that we're discussing in this particular example—I'm sure there are others that we just don't know of—was not obtained unlawfully. So the work Cambridge Analytica—and probably other companies of that sort—was doing for political parties, for example, was obtaining information through Facebook on people, and that's being done legally.

Would that not fall under publicly available information, if a company like that is able to obtain it? There are no legal repercussions because it's not illegal. Could CSE not do the same thing under those dispositions even if incidentally, as laid out in the law, in Bill C-59?

Ms. Greta Bossenmaier: Mr. Chair, I have to go back to the point that, even on publicly available information, it goes back to our mandate. We would access publicly available information only if it were related to our mandate, and we do not have a mandate that focuses on Canadians or anyone in Canada. For the particular case you're referring to, I understand the Privacy Commissioner is looking into it, and I guess the details around it are still unfolding, so I can speak only to our legislation. Again, it goes back to our mandate. It would be very specific: what's the case for which we would need it? Also, very much, the proposed legislation talks about two other things.

Number one, it says we'd have to have privacy protection measures in place, even for publicly available information. Number two, like every other aspect of the proposed legislation, it would be subject to review by the national Security Intelligence Review Committee. This is not CSE having the authority to go look at any publicly available information. It's very targeted and very focused on fitting within our mandate, and again, with privacy protection measures in place, and finally, with review from an independent review agency looking at all of our activities.

I hope that answers your question.

Mr. Matthew Dubé: That's fair enough.

You mentioned the Privacy Commissioner's investigation, but I'm understanding that both your organization and CSIS have also been tasked with looking into that situation, and so in that particular context, when you're doing the research that's prescribed in the legislation where these exemptions exist, notwithstanding section 25, which talks about protecting privacy, would research not be done on, for example, things like Facebook, as part of this information infrastructure? I don't know if that would fall under the definition of information infrastructure, but if you're being tasked with looking into the situation as well, would you not inevitably come across Canadians' information and be allowed to obtain it even if incidentally under what's prescribed in Bill C-59? And under those circumstances, even though it would be in respect of the mandate—I understand that—while I understand you're taking steps to protect privacy, the information nonetheless could be collected over the course of that type of investigation.

Would that not be accurate?

● (1225)

Ms. Greta Bossenmaier: You covered a lot of territory there. Maybe I'll start with the piece about CSE being asked by the Minister of Democratic Institutions to look at this issue around democratic institutions.

I'm thinking back and I'm looking to Scott. About a year ago, in about June 2017, CSE was asked by Minister Gould, the Minister of Democratic Institutions, to look at cyber-threats to Canadians' democratic institutions. For the first time in our history we actually produced a report that's available to this committee, if you haven't seen it, which looked at broad cyber-threats to democratic institutions.

We really looked at three different aspects of that. We looked at the electoral process per se, so how the electoral machine works. We also looked at cyber-threats to politicians and political parties, and we also looked at cyber-threats to the media. We came out with an assessment at that time, about a year ago.

The Minister of Democratic Institutions now is asking us to review our threat assessment in light of changes that have occurred over the past year. Even when we put out the initial report, we said that this would probably be an evergreened report based on new information and new threat information.

That's the kind of work we expect to be doing over the coming weeks, to review our threat assessment based on information and activities that have occurred over the past year. This is refreshing it.

The Chair: Unfortunately we'll have to leave it there.

We have Mr. Picard for seven minutes.

Go ahead, please.

Mr. Michel Picard: Thank you.

I will ask my questions in French, if you don't mind.

[*Translation*]

I will go back to a few points that we discussed about Canadian citizens potentially being targeted.

Clearly, the CSE does not investigate Canadians abroad. Also, when there is information that might involve a Canadian abroad, it is ignored; the information is destroyed.

The CSE is a partner with several departments in Canada, but also an international partner. It therefore exchanges information. How does the CSE have to manage information that comes from international partners that are not subject to restrictions when it comes to investigating Canadians?

[*English*]

Ms. Greta Bossenmaier: Again, it's focusing on our mandate, which is, again, to not focus on Canadians or anyone in Canada. I think it's recognizing that there could be incidental collection as we undertake our activities. It's also focusing on, if I understand the question correctly, how we work with foreign partners.

I'm joined here today also by our chief privacy officer and deputy chief responsible for policy and communications. Again, as privacy is part of his title, I'm going to ask Dom to speak a bit about how we work with partners and deal with private information.

[*Translation*]

Mr. Dominic Rochon (Deputy Chief, Policy and Communications, Communications Security Establishment): Thank you for the question.

[*English*]

I'll stay in English and try to answer by looking at this from the angle of foreign signals intelligence.

When we collect information, you're quite right that given the nature of how communications work, we may come across information related to a Canadian. Let me use a tangible example. We're looking at known bad guy X in country Y. This bad guy X is in line with an intelligence priority of the government. It stands to reason that they're a bad person wanting to do bad things that are an affront to national security. We're collecting against this person.

Now this person, unbeknownst to us, could phone you. When we collect that, we need to understand that the resulting call becomes a private communication. The Criminal Code is very clear that it is against the law to collect a private communication.

We have ministerial authorizations that cover the various activities that we use to collect information and that allow us to keep that information, if indeed it is of national security or intelligence interest. As you pointed out, we are to delete it immediately if it doesn't. If the phone call is to you and it's talking about something that is not related to national security, we are to delete it. We annotate that. We delete it immediately, and that is reviewed by our commissioner to make sure we delete these things on an annual basis.

If indeed it has a national security interest, then we keep it, but even in keeping it, we write a report that talks about the conversation you may have had, possibly about blowing up something somewhere that is of interest to Canada. We would still protect your identity in that report, by using a generic term to render your identity illegible.

Then it comes time for information sharing. Where does our report go? Obviously there are domestic agencies within the national security apparatus here in Canada—CSIS, RCMP, and others—that have an interest in reading the report. Now they may have a legal mandate to know the identity of that Canadian, so there are procedures in place to disclose that information to them.

Similarly, when we're writing reports, some of the information is obviously shared with foreign partners, and there are other things that govern that exchange of information. Again, though, if they wanted the disclosure of that information, they would have to show us why it was imperative for them to get that information.

Of course, we're bound by other things. We have a ministerial directive, for example, which was recently reissued by our minister, related to information sharing that may lead to the risk of mistreatment. We do an analysis of what our partners want that information for and what they are going to be using it for, and we do a risk analysis to make sure it isn't going to be leading to mistreatment. There's a calculus that happens before any information is shared.

● (1230)

[*Translation*]

Mr. Michel Picard: The aspect of the issue I wanted to address does not concern so much the information that goes abroad, but rather the foreign partner who informs you that, after their investigation and analysis, they have identified four persons, one of whom is Canadian. This foreign partner is not subject to the restriction of not investigating Canadians and sends you information. Since this is a person of interest to the foreign partner, does it change the status of the person and, therefore, the process you have just explained to us? Do you retain the information and confirm that this person represents a threat or, on the contrary, are you required to reject that information?

Mr. Dominic Rochon: Without going into too much detail, I would say that the example you give would be within the mandate of CSIS. If that partner has information about a Canadian, we then work in partnership with CSIS.

[*English*]

We would look to CSIS and say, “There's information possibly about a Canadian. That is your responsibility, not ours,” in terms of following up with regard to a specific Canadian.

[*Translation*]

Mr. Michel Picard: The CSE's mandate to protect Canadians from various outside threats goes beyond the military context.

Could the CSE help counter threats that would fall more under FINTRAC's mandate, for example, in the event of terrorist or criminal financing? Let's say that there are incoming communications that suggest that a financed terrorist event is being planned. This brings FINTRAC into the picture. However, it could also involve Industry Canada or other departments. In other words, the flexibility of the CSE support extends to all government agencies.

[*English*]

Ms. Greta Bossenmaier: I'll talk quickly about the parts of CSE's mandate. From a foreign intelligence collection perspective of the mandate, we have a responsibility to collect foreign intelligence across the intelligence priorities that the government sets. To your point, those intelligence priorities definitely go beyond solely supporting military and Canadian Armed Forces function. They're looking at threats to Canada writ large, and the government of the day determines what those intelligence priorities are.

The information we're collecting is really looking at safeguarding and protecting Canadians from a wide range of threats and risks.

The Chair: Unfortunately, we have to leave it there. Sorry.

I feel bad. I keep cutting you off, Ms. Bossenmaier.

Now we go to Mr. Paul-Hus, whom I've never cut off.

[*Translation*]

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

Welcome, everyone.

In part 3 of the bill, proposed section 4 of the new Communications Security Establishment Act states that the Governor in Council may, by order, designate any federal minister to be responsible for the CSE. According to the summary we have, this suggests that any cabinet minister could be designated as the lead for the CSE.

Based on your expertise, which minister would be most qualified to perform those functions? Do you think it would be the minister of Foreign Affairs, National Defence, Public Safety and Emergency Preparedness, or another one?

● (1235)

[*English*]

Ms. Greta Bossenmaier: Mr. Chair, as the chief of CSE, I can answer that the way the legislation is laid out, we report to the Minister of National Defence. He is the responsible minister for the Communications Security Establishment.

[*Translation*]

Mr. Pierre Paul-Hus: In your opinion, the Minister of National Defence must remain the minister responsible for your agency, even though Bill C-59 involves some kind of integration that suggests that the Minister of Public Safety and Emergency Preparedness could play a greater role.

As I understand it, you believe that the Minister of National Defence is the one who should take responsibility for the CSE. Is that correct?

[*English*]

Ms. Greta Bossenmaier: For Bill C-59 and the CSE act in particular, CSE is responsible to the Minister of National Defence.

[*Translation*]

Mr. Pierre Paul-Hus: I would now like to talk about information.

The amount of information you gather is huge. I cannot even imagine the amount of intelligence that goes into Canadian networks. That said, there are two parts: government networks and civilian, or private, networks.

Are you able to collect information from private networks? You are not only dealing with the government aspect, but also with the private aspect.

[*English*]

Ms. Greta Bossenmaier: I want to ensure I'm understanding the question correctly, Mr. Chair. I'm taking that this is with respect to our cyber-defence mandate, under which we have a responsibility to protect Government of Canada systems and to provide advice and guidance for systems of importance to the Government of Canada. As I noted in my earlier remarks, this legislation would allow CSE, upon the request of the owner of a network outside of the Government of Canada and for a system that the minister has designated to be of importance, to work with that system owner to help protect their systems from cyber-attacks. We're not focusing on Canadian information—it's not part of our mandate—but we could be asked to help protect a system of importance from a cyber-attack, which could include something outside of the Government of Canada.

[*Translation*]

Mr. Pierre Paul-Hus: For example, if CSIS needs information, does your centre have to look for it in private networks, for example in emails, on behalf of CSIS?

[*English*]

Ms. Greta Bossenmaier: Sorry, I'm not sure I understand the question.

[*Translation*]

Mr. Pierre Paul-Hus: Suppose I communicate with someone and CSIS suspects that communication would endanger Canada's security. However, it must obtain evidence. Under your mandate, do you have systems that allow you to get that evidence? Is that how things work on your side?

[*English*]

Ms. Greta Bossenmaier: Dom, do you want to pick that up based on your earlier conversation?

Mr. Dominic Rochon: In that particular example, CSIS would be interested in you as a Canadian. They have a legal mandate to do that. They could leverage us under our assistance mandate. We always talk about part (a) as foreign signals intelligence, part (b) as cybersecurity, and part (c) as our assistance mandate. Today, as with this new legislation, if CSIS is interested in you, they have to have a legal mandate to go after you, meaning they have to get a warrant. If they show us that they have a warrant, at that point in time they wouldn't have access to our systems. They would ask us to act on their behalf. We would then use our capabilities to help them collect information. Any information that we collect is segregated and is given back to them and is their information. Effectively, we're acting on behalf of CSIS.

[*Translation*]

Mr. Pierre Paul-Hus: If someone outside the country, for example from another government, contacted a Canadian, it would therefore be possible to get that information. You would need a warrant from a judge, of course.

Mr. Dominic Rochon: Yes.

Mr. Pierre Paul-Hus: That's great.

I—

[*English*]

The Chair: Unfortunately—

[*Translation*]

Mr. Pierre Paul-Hus: That's it already?

The Chair: I'm sorry.

[*English*]

Ms. Dabrusin, you have five minutes. Go ahead, please.

Ms. Julie Dabrusin: Thank you.

I want to bring it out a few layers. We've been getting into some details. I'd like you to clarify some things. You said that a billion times a day there are cyber-attacks on Canadian systems, and then, when you were speaking with Mr. Dubé, you talked about threat assessment and the changing environment that you're dealing with in your threat assessments.

Can you help me understand? In Bill C-59, what are the new tools you have that help you to respond to astronomical numbers, those so large I can't even say the word? Maybe you can help me with that.

● (1240)

Ms. Greta Bossenmaier: Sure, and I will ask Scott Jones, our deputy chief of IT security, to come in.

Perhaps to answer the question, Mr. Chair, I'll go to three different pieces of the proposed legislation.

First of all, to prevent cyber-attacks, we need to have not only good capabilities and tremendous Canadian men and women working on this but also good intelligence to try to understand what those threats are before they even come to Canada. In the legislation, there is a strengthening of our ability to ensure that we can continue to collect foreign signals intelligence, including that relating to cyber-threats. That's a piece of it.

The second piece I would draw attention to is that the cybersecurity aspect of the legislation talks about us being better able to share threat information with the private sector, and it also talks about us being able to—again, at their request—help defend their systems. That's another way this legislation would strengthen our ability to help do cyber-defence for Canadians.

The third piece I would focus on is the defence of cyber-capabilities. If there was a cyber-attack, instead of us sort of standing back with a shield with which we would try to protect against these billion malicious attempts per day and waiting for them to happen, if we could go and say, “Let's try to stop that cyber-attack from even happening”—there could be a server outside which we know is now trying to infiltrate a Canadian system and steal Canadians' information—we could, through this legislation, which would be a new piece for us, try to stop that attack before it got to our shores and into our systems.

With that overview, maybe I'll ask Scott Jones, our IT security—

Ms. Julie Dabrusin: If I can talk about that, part of what you're saying is that, in fact, the hope is we will reduce it from the billion down to the lower levels. Can you just explain it? When we're talking about this one billion number, what are we talking about? Can you clarify that for me?

Ms. Greta Bossenmaier: Of course.

Scott.

Mr. Scott Jones: Really, when we're talking about a billion malicious actions, we're talking about the gamut, all the way from people poking at our systems, looking to see where they're vulnerable, up to people trying to compromise or install malicious software called malware, or basically exploit any vulnerability that exists. It's a wide range of activities, but what we're trying to do is counter the full range, no matter where it originates. We want to counter any malicious activity that's coming at the Government of Canada, and the number is astonishing. I think that's really where we are going into a few different areas. Number one is making it better. How do we work to make the systems that we have more defendable? That's working with the commercial sector, and that's being able to share more information, being able to share some of our tools and techniques, and pushing it forward.

We've shared some of our tools publicly. We have a system called Assemblyline which we have made open-source and publicly available to anybody who could leverage that. That's how we, for example, defend the government and look at millions of malicious files a day.

The second piece is providing that level of defence that fills the gap between the best available commercial and the state-of-the-art threat activity that we're facing today. Bill C-59 would allow us to then use that on critical systems of importance, as designated by the minister, but also with the informed consent of the system's owners. Informed consent is something that's particularly important in this case.

The third piece is general information sharing, whether that is providing advice and guidance or being able to share what we're seeing, what's going on, and very much clarifying our authorities to share information.

That's where we kind of layer all these things together and start to deal with those billion events.

Ms. Julie Dabrusin: Thank you.

The Chair: Thank you.

Thank you for those astronomical and astonishing answers to very penetrating questions.

With that, Mr. Calkins, you have five minutes. Go ahead, please.

Mr. Blaine Calkins: Thank you, Chair.

I have some questions. I'm just really concerned about the overall security. I formerly was an IT professor at a college before I actually came here as a member of Parliament. That was a long time ago, 12 plus years, which means that my IT skills are basically non-existent anymore. Notwithstanding that, I have some questions. I understand the difficulty and the enormity of the task that's actually there, and I want to highlight that. Can you tell me how many people are actually employed by CSE to do the preventative or proactive elimination of threats? What size of a crew do we have working on that? Is that a number that you can share with the committee?

● (1245)

Ms. Greta Bossenmaier: Maybe I can talk about the composition of the organization overall. Sometimes it's hard to parse a person who perhaps, for example, is working on cyber-policy within our group, looking at cyber-policies, versus the person who is out there building the defensive tool versus the person who is collecting foreign signals intelligence that might identify a foreign threat. It's sort of hard to divide people into particular—

Mr. Blaine Calkins: I'm looking for some anyway, so...

Ms. Greta Bossenmaier: CSE overall has about 2,300 employees right now. We have Canada's best and brightest mathematicians and computer scientists, and we are hiring, in case you still are interested, in the IT field.

Mr. Blaine Calkins: I'd like to think I'll be gainfully employed in this as long as I like.

Ms. Greta Bossenmaier: In case there's anyone else out there....

We're about 2,300 people overall. If you look at Mr. Jones's organization, he's in particular focused on the IT security component of the organization.

I think, Scott, you've provided numbers in the past about the magnitude of your organization.

Mr. Scott Jones: It's around 500 right now and growing slightly.

Mr. Blaine Calkins: Here's my question, and it's not meant to be in any way a slight against the fantastic people we have. I'm sure we have the best and the brightest and I'm appreciative of that, but we know that China has an army of about 200,000 people. We know this from reports we've heard, so it's 200,000 against 500. I'm basically looking to you to tell me why Bill C-59 makes those 500 better off, in defence against what those 200,000 might be doing.

We've seen what's happening right now in the United States with sanctions against China under the guise of security, espionage, and all these kinds of.... It's no secret that the Chinese government has been doing this for years. We've had the current government actually very much engaged with China. We sold some assets to Chinese interests recently, and we've been doing so for years and years. This is not meant to be a partisan comment in any way, shape, or form. How is Bill C-59 helping our 500 against the 200,000? It seems like a formidable task.

Ms. Greta Bossenmaier: Thank you, Mr. Chair.

The reality is that it is a formidable task. That's why it's something we take extremely seriously. Again, we've been in the business for 70 years, and I'm sure we have the best technology, the best people we can have to work on this task, and to work on it in partnership. We often talk about this being a team imperative. No one organization can have all the information or all the answers, so we do work closely with academia. We work closely with other partners. We work closely with our allies in terms of developing knowledge and capability to be able to defend against this very, very challenging environment.

In addition to what was already discussed around budget 2018.... Budget 2018 is proposing an increase in resources and a consolidation of Government of Canada cyber-operational capabilities within CSE, so it provides a bit of a multiplier effect and a single source of trusted advice and guidance, but this legislation would also allow us to exercise additional authorities in the cyber-protection space. Again, that goes back to ensuring we can collect foreign intelligence in a very challenging world and that we can see threats before they reach our shores, have broader threat information sharing, and deploy our cyber-tools—some of the advanced tools Mr. Jones spoke about—on private infrastructure if that is requested and if it is designated.

Also in the defence of cyber-operations, instead of trying to defend only at the periphery of our networks, if we see something that is outside—in a foreign land, on a server, for example—trying to take down Canadian infrastructure or trying to steal Canadians' information, Bill C-59, this legislation, would authorize CSE to go out and try to protect Canada before that threat actually reaches our systems.

The Chair: Thank you, Mr. Calkins.

Mr. Spengemann, go ahead for five minutes, please.

Mr. Sven Spengemann (Mississauga—Lakeshore, Lib.): Thank you very much, Chair.

My first question is for Commodore Feltham. We spoke a lot about non-state actors and private-sector threats, as both initiators and recipients of activities. What about military-to-military cyber-attacks? What do you see as current trends? Russia is one problem. Who are the other problems? What trend lines and what observations can we make at the moment? Is there going to be an increase in military-on-military cyber-activity? If so, how does it break down from what you see so far?

Commodore Richard Feltham (Director General, Cyberspace, Department of National Defence): Thank you, Mr. Chair.

I can't give you the specific numbers of state and non-state actors we see trying to penetrate the networks both within our structure and outside of it on a daily basis, but I can tell you that both state and non-state actors are trying to penetrate networks, and that number is rising every week—every day, almost.

I can't give you the specific breakdown. I don't have those numbers with me today, but state and non-state actors are involved in that domain, and the numbers are rising.

● (1250)

Mr. Sven Spengemann: Is it fair to say that there is investment in cyber-capacity and offensive cyber-capacity by potentially hostile or openly hostile militaries?

Cmdre Richard Feltham: We are seeing increased numbers of people trying to gain access to our networks, which suggests increased investment. I don't know for a fact, but we are seeing large numbers of different entities trying to get into our networks.

I think you have a comment, Mr. Burt.

Mr. Stephen Burt (Assistant Chief of Defence Intelligence, Canadian Forces Intelligence Command, Department of National Defence): From the defence intelligence standpoint, the simple answer to your question is yes. It is a rising threat across nation-state actors within their militaries, and it is a crosscutting threat. We're interested in it the same way we're interested in growth, for example, in submarine fleets, because it is increasingly used across the board by large and small states.

Mr. Sven Spengemann: Can you qualify in any meaningful way the priority that this issue of potential hostile miliary on miliary is being given within DND?

Cmdre Richard Feltham: Mr. Chair, I can qualify that cyber as a domain of operations has now been certified as—much like air, land, sea, and space—its own domain.

We saw in the recent defence policy the increased mandate to incorporate an act of cyber. We've been defending military networks for a long, long time, so I wouldn't want to imply that we haven't been doing that.

The very fact that we are embarking upon an active cyber component to our cyber-operations is indicative of how we're taking this threat, and the accompanying investment within that domain. The short answer to your question is that we are looking at this domain very carefully. We are growing our forces and our ability to work in that domain every day, sir.

Mr. Sven Spengemann: Thank you very much.

My second question is for Ms. Bossenmaier and Mr. Jones.

You spoke about the dynamic cyber-threats environment earlier in your conversations and gave some precision on what that means for Canadians. I'm wondering about your assessment of Bill C-59 as an instrument that is sufficiently agile, adaptable, and flexible for a look beyond the horizon and into the future.

Ms. Bossenmaier, I think you mentioned AI, and I think quantum is another unknown unknown. We don't really know how these two dimensions are going to play out.

Is the instrument that we're contemplating and about to put on our books flexible enough to address future challenges as they may arise?

Ms. Greta Bossenmaier: It's a very important question, Mr. Chair, because, again, it is such a dynamic environment.

Whether it's quantum or artificial intelligence or the Internet of things or cloud computing, or whatever the new technology is going to be in the future, our sense is that this legislation will allow us to be able to respond and be proactive in looking at what those threats of the future are.

It's sort of technology-agnostic in the sense that it talks about various threats that could occur and, again, provides us with the authority to be able to work with whatever those undefined threats of the future may be.

Scott, you may have something to add on that as well.

Mr. Scott Jones: I think the key aspects are that the pace of change in technology is accelerating right now, so I think what we're going through.... For example, on quantum, we're working on this on a number of fronts. First of all, we do have a duty to protect the Government of Canada's most sensitive information, and so we're preparing for that future as well.

Also, as Canada's national cryptologic agency, we are the experts in cryptography, so we are working with partners across the private sector, National Research Council, etc. That's something we've been doing for 70 years.

A lot of these technology changes are things that fit well within our advice and guidance mandate in terms of preparing for the future, and also with the information-sharing mandate in terms of how we work as partners. The Internet is interconnected. We need to have a new way of approaching this, and that's very much about partnership and working together with companies, with academia, with other levels of government, and internationally as well.

Mr. Sven Spengemann: Thanks.

I think that's my time, Mr. Chair.

The Chair: Thank you.

Mr. Dubé, it's a good day for you today. Please finish up for the final three minutes.

Mr. Matthew Dubé: Thank you. I appreciate it, Chair.

I want to come back to the line of questioning I was on before.

Would interactions taking place on Facebook or information that's put out on any social media, quite frankly, fall under this bill's definition of global information infrastructure?

Ms. Greta Bossenmaier: I think we addressed this question before. I won't give you the same answer again, which doesn't seem to be completely answering the question, but I will ask Dom to speak a bit about publicly available information and how it has to fit within our mandate.

Mr. Matthew Dubé: I don't have very much time, so I'm wondering if I can get a yes or no.

Mr. Dominic Rochon: Yes, information on the GII, the global information infrastructure, would include all sorts of things. However, our mandate is very specific that we cannot collect information about Canadians under foreign intelligence.

● (1255)

Mr. Matthew Dubé: Okay, that's—

Mr. Dominic Rochon: It's always specific to our mandate, which is the Privacy Act. The Privacy Act—

Mr. Matthew Dubé: I appreciate that. I don't have much time. I apologize.

Clause 23 of the proposed CSE act, under part 3 of Bill C-59 says that activities can't be carried out against Canadians. Subclause 24(1) says that "Despite subsections 23(1) and (2)"—which is the prohibition—"the Establishment may carry out any of the following activities in furtherance of its mandate...". Then it talks about ensuring the protection of information on these networks.

Social media is part of these networks, and that information is at risk. You have been tasked by a minister to ensure that this information is safe, and you're exempt from the prohibitions on collecting Canadians' information as part of that research.

How can we be assured that Canadians' information will not be collected incidentally, as the possibility of the incidental collection of that information is specifically outlined in the bill?

Mr. Dominic Rochon: Unfortunately, the question is somewhat misleading.

Do we need to access the private communications in order to protect the networks? Is that what you're insinuating?

Mr. Matthew Dubé: No, I'm talking about this: if a company that's hired by a political party or a polling company is able to obtain its information legally, that information falls under the definition of publicly available information. So, if that information is able to be collected as part of the research that you're doing on the safety of these networks—and you've been tasked with looking into this type of situation, as Acting Minister Brison said this week—would that not then lead to the situation in which Canadians' information can fall under that?

Mr. Dominic Rochon: If I can come at it this way, the national security and intelligence review agency is going to be reviewing us to make sure that we're compliant with the law. It's going to look at all of our activities.

If we happen to collect this information, it's going to ask, "Why did you collect it?" Now if we only say, "Oh, because we're allowed to do it under publicly available information", that won't be sufficient. The agency will say, "No, the Privacy Act mandates you to only collect information if it's relevant to part (a), part (b), or part (c)." The carve-out is really only to say, "We needed that information because we're looking to target this foreigner, and we weren't sure whether they're Canadian or not." There needs to be something that explains that. The publicly available information is really only there to provide clarity for those review bodies so that they cannot completely take away our ability to do what I think everyone does in their regular day, which is use the Internet to get information to inform some decision that they're making.

The Chair: Unfortunately, we will have to leave that at this point.

Before I thank our witnesses, I just want to say that next week, a week from today, the meeting has been cancelled because we are moving to Friday hours on Thursday, so there will be no meeting this time next week. On Tuesday, Mr. Paul-Hus will be chairing, and I'm counting on the clerk to make sure that he chairs brilliantly, as I expect he will. I will be away, and I wish you all a happy Easter.

Thank you so much for your contribution to our deliberations.

Ms. Greta Bossenmaier: Thank you, Mr. Chair.

The Chair: That ends our evidence on Bill C-59. We will go to clause-by-clause after the Easter break.

Thank you.

The meeting is adjourned.