HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Public Safety and National Security

SECU • NUMBER 097 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, February 13, 2018

Chair

The Honourable John McKay

Standing Committee on Public Safety and National Security

Tuesday, February 13, 2018

● (1055)

[*English*]

The Chair (Hon. John McKay (Scarborough—Guildwood, Lib.)): Even though we are a few minutes early, I'm going to call this meeting to order and ask Mr. Brown to lead off.

We're here for two hours. I'm anticipating some order in the first hour when we ask our questions, and maybe a little less formality in the second hour as we dive deeper into Bill C-59.

I appreciate the interest of all of the departmental officials in the deliberations of the committee. This is an opportunity for the committee and various officials to interact on both a semi-formal and a less formal basis.

With that, we'll start with Mr. Brown.

Mr. Malcolm Brown (Deputy Minister, Department of Public Safety and Emergency Preparedness): Thank you very much, Mr. Chair.

I'll make a few opening comments, and then I think my colleague Shelly from the Communications Security Establishment will also have some opening comments.

I'm pleased to have the opportunity to appear with my colleagues today to discuss Bill C-59, the proposed National Security Act, 2017.

As you can see, I'm joined by officials from the Public Safety portfolio, including the RCMP and CSIS, the Communications Security Establishment, and the Department of Justice.

[*Translation*]

I want to begin by thanking all the members of this committee for reviewing this bill.

[*English*]

As you know, this bill is the focal point of Minister Goodale's mandate with regard to national security. It is also the result of an unprecedented nationwide public consultation, one in which this committee played an important role.

The consultations undertaken by Public Safety Canada and the Department of Justice involved an online questionnaire, in-person town halls across the country, social media engagement, and much more. In total, tens of thousands of views were heard, collected, documented, and analyzed.

Of course, this committee held numerous meetings of its own on the topic of national security.

[*Translation*]

The proposed legislation reflects all of this input - from citizens, parliamentarians, community leaders, national security experts, and academics.

[*English*]

Bill C-59 has three core themes.

Number one is to enhance accountability and transparency. This would be done through the proposed creation of an intelligence commissioner and a national security and intelligence review agency, both of which would complement the work of the newly established National Security and Intelligence Committee of Parliamentarians.

Number two is to fulfill mandate commitments with respect to the former Bill C-51. This includes proposed revisions to threat reduction activities under the CSIS Act, amendments to the Criminal Code, improvements to the Secure Air Travel Act, and revisions to the Security of Canada Information Sharing Act.

Number three is to ensure that our national security and intelligence agencies can keep pace with the evolving nature of security threats. This includes measures such as modernizing the CSIS Act, establishing the proposed Communications Security Establishment Act, and making other legislative updates.

● (1100)

[*Translation*]

In short, bill C-59 is designed to update and modernize Canada's national security framework to reflect current realities. Its overall objectice is to keep Canadians safe, while safeguaring our rights and freedoms.

[*English*]

To ensure that this bill achieves this objective, Minister Goodale signalled his intention for a thorough review and analysis of its contents as it proceeds through the parliamentary process.

Beginning this past summer and continuing through to the new year, officials from Public Safety Canada and from across the security and intelligence community have engaged key stakeholders. In many ways, this has been a continuation of conversations that began with the national security consultations in 2016, which I mentioned earlier.

[*Translation*]

The aim of these discussions and interactions has been not only to respond to technical questions about the content of the bill, but also, and mainly, to obtain feedback and input about how to improve the bill.

[*English*]

We've had meetings and exchanges with the Office of the Privacy Commissioner of Canada, the Security Intelligence Review Committee, the Office of the Communications Security Establishment Commissioner, and the Civilian Review and Complaints Commission for the RCMP.

[*Translation*]

We also had a number of exchanges with prominent academics in the field of national security in order to obtain constructive feedback to help ensure the bill achieve its objectives. I can assure you that these discussions were very helpful.

[*English*]

Similarly, we have taken a keen interest in the deliberations of this committee, including the testimony of witnesses and the detailed written briefs made available on the committee's website. I should note that, although separate from Bill C-59, the government announced in June that it would be adopting a national security transparency commitment to be applied across Canada's federal national security apparatus. Public Safety Canada is exercising a leadership and coordination role for implementing that commitment and supporting the establishment and operation of an advisory group. This work will complement the ultimate objectives of Bill C-59.

[*Translation*]

It is Minister Goodale's aim to have an open and thorough conversation in order to ensure that this bill is the best it can be.

[*English*]

It is in this spirit that my colleagues and I appear before you today. We look forward to responding to any questions the committee may have about the bill.

Thank you very much, Mr. Chair.

The Chair: Thank you.

Ms. Bruce.

Ms. Shelly Bruce (Associate Chief, Communications Security Establishment): Thank you.

[*Translation*]

Mr. Chair, distinguised members of the committee, As associate chief of the Communications Security Establishment. I want to thank you for the invitation to appear before you, as you continue your study of bill C-59, which sets out the Communications Security Establishment Act.

I am pleased to be here today to clarify and explain certain aspects of this important piece of legislation.

[*English*]

Let me begin by underscoring remarks made by Minister Sajjan when this legislation was last discussed in the House of Commons. The minister said:

> There can be no greater obligation than to protect the security of Canadians at home and abroad. Bill C-59 would provide CSE with the authorities and tools to maintain the highest standards in security protection while adhering to the high standards of accountability and transparency.

CSE has helped protect the security of Canadians for over 70 years by providing critical foreign intelligence about threats to our national security and our deployed forces, and by protecting Canada's most sensitive information and information systems. In order to deliver this important mandate, governments throughout those 70 years have expected CSE to respond to the priorities of the day and to ensure that it stays ahead of evolving global threats and constantly changing technology—and to meet those challenges while protecting Canadians' privacy, rights, and freedoms. That is what the proposed authorities and accountabilities in the proposed CSE act would do. They would provide CSE modernized authorities to help keep Canadians and Canada safe and secure against global threats, including cyber-threats, in a rapidly evolving technological world. They would provide new accountability measures to ensure that CSE's activities are authorized, reviewed, and are as transparent as possible.

As the committee has studied this bill a number of important questions have been raised. I would like to address a few of the more common ones now.

First, I'd like to address the provision in the proposed act around publicly available information. Questions have been raised about how CSE would use publicly available information and what impact that would have on the privacy of Canadians. To be clear, this provision exists only to allow CSE to conduct basic research in support of its mandate from the sorts of public resources that would be available to anyone in Canada. CSE does not and would not use publicly available information to investigate Canadians or persons in Canada, or build dossiers on them. That is not our mandate, and for us, mandate matters.

The proposed CSE act reinforces this by explicitly requiring that CSE have measures in place to protect the privacy of Canadians and persons in Canada in the use, retention, and disclosure of publicly available information.

How would we use that publicly available information? I can provide three quick examples. First, we could use it to provide general background information for a foreign intelligence or cyber-security report. Second, we could use it to assess the nationality of an individual or organization. Third, we could use it to consult technical manuals associated with new technologies or infrastructure.

Under no circumstances would CSE use this provision to acquire information that was unlawfully obtained. Hacked or stolen data would not constitute publicly available information under the CSE act.

This committee has also heard questions about the proposed active cyber-operations aspect of CSE's mandate, including questions on how they would be used and the potential impact on Canadian privacy. As this is a new authority for CSE, I want to clarify what this means. Active cyber operations would allow CSE, within strict legal parameters and with approvals at the highest levels of government, to take action online to disrupt foreign threats, including activities to protect our democratic institutions, to counter violent extremist and terrorist planning, or to counter cyber-aggression by foreign states. As examples, CSE could use active cyber operations to prevent a terrorist's mobile phone from detonating a car bomb; we could impede terrorists' ability to communicate by obstructing their communications infrastructure; or we could covertly disrupt a foreign threat actor from interfering in Canada's democratic processes.

The proposed legislation is also clear in the limits built into this authority. CSE would be prohibited from directing active cyber operations at Canadians, at any person in Canada, or at the global infrastructure in Canada. The act would also require that these activities be reasonable and proportionate. It would specifically prohibit CSE from causing death or bodily harm, or wilfully attempting to obstruct, pervert, or defeat the course of justice or democracy.

Let me underscore the fundamental change in our approach to ministerial authorizations.

● (1105)

Bill C-59 builds on CSE's current ministerial authorization regime by broadening its application and introducing new and important oversight and review functions. Under the act, CSE will seek a ministerial authorization for any activity that would interfere with the reasonable expectation of privacy of a Canadian or a person in Canada, or contravene an act of Parliament.

For CSE's foreign intelligence and cyber-security activities, these would be subject to approval by the Minister of National Defence and the intelligence commissioner. Active and defensive cyber operations are not collection activities and cannot be directed against Canadians or persons in Canada. As such, they would be approved by the Minister of National Defence and the Minister of Foreign Affairs. All of CSE's activities would also be subject to full review by dedicated independent review bodies.

[*Translation*]

Mr. Chair, I'll conclude by thanking the committee for inviting me and my colleagues here today to testify.

Thank you for your important deliberations on the Communications Security Establishment Act. We look forward to answering your questions.

Thank you.

[*English*]

The Chair: Thank you, Ms. Bruce. Welcome to the committee for the first time, I understand. I hope it's not the last time.

I believe that's the end of formal presentations.

With that, we'll turn to Mr. Spengemann for seven minutes.

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

Thank you to our witnesses for being here. Thank you for your service and expertise.

I'd like to start with a question to Mr. Brown.

Mr. Brown, I wonder if you could briefly sketch for the committee your assessment of the strategic threat setting that the country faces in 2018, with particular attention to the two principal threats, being cyber-directed activities, and also the risk of terrorist attacks, violence, extremism, radicalization, both domestically grown and/or foreign inspired.

How do those two compare against each other, and are there any other threats that we need to take note of in 2018?

Mr. Malcolm Brown: In six minutes?

Mr. Sven Spengemann: Not for that question, please. I have a number of other ones.

An hon. member: You'd need about an hour and a half for that one.

Mr. Malcolm Brown: In all seriousness, virtually everything that I say my colleagues will want to refine, correct, and make more precise, but I will take a stab at it.

I think you have identified two of the key issues. There is no question that in the current threat environment, in terms of counterterrorism and the realities we are all facing, both as individuals and as part of any entity that we participate in, whether it's social or professional or as a government in terms of the cyber-threats we're confronting, the reality is that it's multi-faceted.

I would also indicate, though, that I think we continue to face traditional threats. This is clear in publicly released documents both by the department and CSIS that the threat environment is more complex than the ones just mentioned above. It includes the kind of traditional intelligence gathering by countries that are either competitors or wish us ill. I think, as well, in terms of the counterterrorism environment, we continue to face both foreign as well domestic threats.

As I say, I could use up all of your allotted time very easily, but I think that's a snapshot and I'd be happy to take some questions.

● (1110)

Mr. Sven Spengemann: To summarize your answer, is it fair to say that both the risk of violence—terrorism and extremism—and of cyber-attacks are two that cannot be subordinated to, or prioritized over, each other? They are both equally significant in our current study.

Mr. Malcolm Brown: Well, one of the hardest parts of the jobs that my colleagues in the agencies before you manage is constantly juggling that. The reality is that all those threats you described, plus the other ones I've identified, are constantly the subject of scrutiny by the agencies.

At any given instance, finding the right balance is a very serious challenge.

Mr. Sven Spengemann: Thank you for that. That's helpful.

How confident are you that the bill in its current formulation captures what we might describe as "unknown unknowns", especially in the cyber domain? If you look, for example, at the areas of artificial intelligence and quantum computing and you connect that to the cyber-threat environment, is the bill flexible enough to address emerging issues that we may not have turned our minds to?

Mr. Malcolm Brown: It's hard to predict the future. I will say that as the bill was drafted, there was an effort to provide.... We recognize we do these things irregularly. The last time a significant overhaul or review with all-encompassing characteristics was undertaken really was a generation ago. I do think that the approach we all took, in terms of the provision of advice—which was reflected in the government's decision—was to create a framework that would in fact be flexible and adaptable enough to respond to emerging threats.

Mr. Sven Spengemann: Thank you very much.

My next question is for Ms. Bruce.

Thank you for your clarification of the active cyber-operations question. I think the Canadian public is really mindful of some issues that may not be apparent to them in the sense of how complex an environment this is and how identifiable in the minds of the Canadian public actions that ultimately would need to be taken to disrupt a threat are. Your testimony gave a couple of examples, such as disrupting or deactivating a cellphone that may be used in detonation. It's also quite clear that we would not engage actively to threaten lives or to destroy lives. What about the area of collateral damage, for example, having to take down a portion of an electricity grid that might then cause civilian infrastructure problems and potentially put people at risk, though not necessarily at risk of death? People might say, "Okay, what if we inadvertently deactivate power supplies to a hospital?" Are there rules of engagement that could be enunciated with greater granularity than what you've described at the moment which you could tell the committee about?

Ms. Shelly Bruce: The environment is incredibly complex, as you state. The work that CSE does under its traditional mandates of foreign intelligence and cyber-security allows us to build up a picture of the environment against which an active cyber operation might be delivered. In that sense, an incredible amount of research and work and intelligence needs to be compiled to understand the foreign targets, the foreign infrastructure, what it's connected to, and what the residual impacts might be if something were launched in that space. So a great deal of analysis needs to go into coming up with options for the government to consider, and they also need to consider whether or not they want CSE to conduct an active cyber operation against a greater objective. In this sense, there are some big restrictions around how that works, including the requirement for it to be reasonable and proportionate. Two ministers, the Minister of National Defence and the Minister of Foreign Affairs, need to sign off on that and understand what the implications could be.

I might turn to my colleague to talk about some of the other restrictions and limitations that exist within that space that would guide our decision-making.

● (1115)

The Chair: You might have to work that answer into another answer at some point, because we're out of time unfortunately.

Monsieur Paul-Hus.

[*Translation*]

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

Good morning, everyone. Thank you for being here today. Your comments will be most helpful.

My first question concerns the funding of terrorist groups. The question is for Mr. Brown or anyone else who would like to answer.

Mr. Michael Nesbitt appeared before the committee. He expressed his concern that Canada runs the risk of being a home for terrorist financing and other activities. This is a possibility.

Our party, through my colleague Mr. Tony Clement, introduced bill C-371, which is currently being studied in the House. This bill would address what are known as covert means. It appears that the government did not want to support the bill, arguing that bill C-59 and other Canadian legislation provides the tools required to prevent funding by covert means in support of terrorism.

Could you comment on that?

Mr. Malcolm Brown: I will answer and my colleagues can add to my comments.

[*English*]

The view is that, in addition to the changes that are proposed in Bill C-59, the framework that is already available to the government in terms of addressing issues associated with terrorist financing is sufficient. Generally speaking, in the context of Bill C-59, the government is open to suggestions. I do think that in the perspectives in the private member's bill that you've mentioned there are some practical considerations that, frankly, make it problematic.

That being said, I think we're constantly challenging ourselves to ensure that all of the agencies have the tools they need to confront the challenges around terrorist financing. There are a variety of steps we can take, and at that I'll let my colleagues jump in, if they'd like, in terms of the tools we have now that, we believe, give us the capacity to respond as necessary.

Gilles.

[*Translation*]

Deputy Commissioner Gilles Michaud (Deputy Commissioner, Federal Policing , Royal Canadian Mounted Police): In practical terms, what we see on the ground with respect to terrorist financing is actually related to all our investigations. We are always looking to discover whether there is a terrorism financing component.

However, we are always faced with the challenge of the use of funds. It is very difficult for us to prove how the money was used because it is used in countries that do not have an information sharing protocol or a protocol that meets the standard required to support evidence in Canada.

As Mr. Brown indicated, we are actively working on this. We believe that, through other mechanisms, we have the tools required to share information and financial data, which give at least an overview of the situation and allows us to focus on certain targets. However, once again, the challenge is still collecting the information and obtaining evidence that meets the standards of Canadian courts.

Mr. Pierre Paul-Hus: All right. Thank you.

My next question is about information sharing. The former director of CSIS told the committee that, although he hadn't counted, the number of times the words "protection of privacy" are mentioned in the bill is really quite astounding. He said he was as much in favour of privacy as everyone else, but that he sometimes wondered whether the fact that we are placing so much emphasis on it would scare some people with respect to national security.

Can you comment on this?

● (1120)

[*English*]

Mr. Malcolm Brown: I'll let my colleague, Tricia Geddes, reply on behalf of Canadian Security Intelligence Service.

Ms. Tricia Geddes (Assistant Director, Policy and Strategic Partnerships, Canadian Security Intelligence Service): Sure. I guess I would say that it's quite clear that this bill is able to deliver the effective tools and the authorities that we need, in order to be able to conduct our investigations. Ensuring that we have the confidence of Canadians and that we are able to do so in a manner that protects their privacy is very critical to our ability to carry out our mandate. I think the bill has achieved both of those objectives.

[*Translation*]

Mr. Pierre Paul-Hus: All right.

We also heard Mr. Fadden speak about China, which has about 200,000 people conducting cyberoperations.

Do you believe that the powers granted by bill C-59 open the door to effective action against the Chinese threat in cyberspace?

Mr. Malcolm Brown: I will begin to answer that question and then turn it over to Ms. Bruce.

I would say yes, without a doubt. I am sure that the modernization of...

[*English*]

our assets, in terms of our being able to respond, is long overdue, within the concept of a framework.

I will also indicate that the government is in the midst of a cyber-security strategy review and that the results of that will be known in the fullness of time. That's another element of a response to your question.

Would you like to respond, Shelly?

[*Translation*]

Ms. Shelly Bruce: Thank you for your question.

I will answer in English as I am more familiar with the vocabulary in that language.

[*English*]

I agree with Malcolm regarding the environment that we are working in. We're in a space where there is an increasing cyber-threat surface out there. Hostile state actors and non-state actors are using the Internet. We also have rapidly growing and evolving technology based within that space. We also have targets and our own citizens who are using that space, so all three of those combined makes this a very challenging environment for us, but the legislation will provide us with advanced tools and capabilities to address some of these issues. As well, this provides the government with an opportunity for CSE to use its capabilities and expertise for online activities in a way that could thwart or disrupt online threats, before they materialize or become a crisis within Canada.

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

Mr. Dubé, you have seven minutes, please.

Mr. Matthew Dubé (Beloeil—Chambly, NDP): Thank you, Chair, and thank you all for being here.

I'll apologize in advance if I seem rude. My time is fairly limited.

Ms. Bruce, you said that mandate is important. Is that a legally defined mandate or the mandate that the organization gives itself?

Ms. Shelly Bruce: It's a legally defined mandate.

Mr. Matthew Dubé: Thank you.

The Minister of National Defence is the one responsible for the powers that are in this bill. Can someone at the table, then, explain to me why it's been added to a bill that's been tabled by the public safety minister? The public safety minister comes before this committee, and the bill has come to a committee that doesn't necessarily have the institutional memory that the national defence committee would have.

Mr. Malcolm Brown: The short answer is that I think the decisions about which committee this should go to.... We are merely servants. We come to testify before whoever would like to ask us the questions. It's not for us to opine on the appropriateness of the forum.

Mr. Matthew Dubé: I appreciate that, so why were these measures dealing with the CSE specifically included in this bill?

Mr. Malcolm Brown: Because it's about updating a national security framework that includes the activities of an agency such as CSE.

Mr. Matthew Dubé: I appreciate that.

Ms. Bruce, we'll go back to you. Clause 25 in part 3 dealing with the privacy protections.... Some of the words that are used include, “and disclosure of”. The minister has explained that the changes to SCISA that now use the word “disclosure” refer to information already in the possession of different agencies or departments. In other words, when you're talking about the disclosure of information that you're obtaining through this research, does that mean of the information could be shared between different agencies and departments?

Ms. Shelly Bruce: Go ahead.

Mr. Scott Millar (Director General, Strategic Policy, Planning and Partnerships, Communications Security Establishment): Hi there.

Just to be clear, right now we share information with other departments and agencies under our existing authorities. When we do that, we do it through an end-product report, an intelligence report. That will continue the way it is now. There are privacy measures in place when we share that information, and those measures are reviewed. In fact, how we do that is reviewed and has been reviewed for 20 years. So this will enshrine the legislation of practice that exists now with CSE.

● (1125)

Mr. Matthew Dubé: I ask because one of the responses to the concerns.... You said that you're not using the information you're collecting under section 24 to create profiles or do any kind of investigation. Does that preclude other agencies from potentially doing the same thing, if you're disclosing the information you've collected to another agency, and it's beyond your mandate to be doing anything yourself with that information?

Ms. Shelly Bruce: When we say we need privacy measures in the disclosure of information, it means that in the course of our foreign intelligence or cyber-security operations, we may come across an entity, an IP address, an individual, or a company that is unknown to us. So we need to do research from open sources to contextualize that and to make sure we understand what we're dealing with.

If it turns out that the individual, that company, or that IP address is Canadian, then we put in place measures to mask that identity if that information leaves CSE. It's about protecting that information.

Mr. Matthew Dubé: As the bill reads, you “take measures”, but essentially, those are internal.... There's no retention period, for example, which is often something that we see.

Is there any way you can provide the committee with the specific measures you take to protect the privacy of information collected under section 24?

Ms. Shelly Bruce: As I said, the information that's collected.... Actually, it's not collected; it's consulted. It's research information that we use. If that information is germane to foreign intelligence or cyber-security reporting, then we will include a reference to that. But we would mask it. We would suppress any Canadian information and replace it with a generic term. Instead of listing the Canadian IP address or the Canadian name, we would say “a Canadian person” or “a Canadian IP address”.

Mr. Scott Millar: I'll just to that add, as well.

Again, we cannot direct our activities at Canadians. We direct them at foreign targets. If a foreign target talks about a Canadian, or, say, calls somebody in Canada and we pick that up, we have to destroy that information under current legislation, if it's not essential for international affairs security and defence. If we do retain it, then we have to count it. We would have to account for the fact that the information had been picked up, the fact that we had destroyed it, or if we had retained it, the reason we had retained it. That's reviewed now by the CSE commissioner.

There are policies and procedures and things baked into our system that we have available on our website in the form of a privacy fact sheet that breaks out all the different measures now in place, and our adherence to those measures is reviewed by the CSE commissioner.

Mr. Matthew Dubé: You'll forgive me, but it's section 24 that specifically says “despite section 23”, which is the one that mentions the prohibition against targeting Canadians or persons in Canada. It says that despite that, you “collect publicly available information for”, and it lists the reasons.

Section 25 mentions these vague notions of measures being taken to protect privacy. Can you point me to the specific part of the bill that explicitly outlines what's done to protect privacy, and the things you're explaining about destroying that information or not keeping it? Insofar as the information collected under section 24 is concerned, I just don't see that.

Mr. Scott Millar: Right now in the bill, the minister, in the ministerial authorization space, will lay out the privacy measures specific in that authorization on the use, retention, and disposition of that information, and we have to follow that. Again, some of those elements are listed on our website now. I can walk through them. There are policies, procedures, training, and what have you.

I think an important element to underscore is that the only way we would assist other law enforcement security agencies under their mandates is if they came to us with their own lawful authorities—under our assistance mandate—and then we would help them within the bounds of that lawful authority and that activity.

With respect to the kinds of things we're talking about here, for anything that we do in CSE, whether it's our intelligence collection, cyber-security, or dealing with publicly available information, we have to have privacy measures in place. There could be things that engage our privacy interests, so those measures have to be there.

There's a range of things, in terms of privacy measures, for the kinds of general research that we do, the kinds of intelligence-collection activities that we do in support of the Government of Canada's intelligence priorities, and the kinds of things that we do in response to requests from partners.

Mr. Matthew Dubé: When it comes to—

The Chair: Unfortunately....

I do intend to be a little bit more flexible in the second hour, so I think we can come back on a lot of these issues.

Ms. Damoff, for seven minutes, please.

● (1130)

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

I want to follow along the same line of questioning, because I'm still not clear about when Canadians get caught up in this information gathering. I have a couple of questions.

You mentioned that you mask the identity, but you keep it. For how long do you keep that information?

Ms. Shelly Bruce: CSE does have a retention schedule, but we have not published those retention schedules at this time.

Ms. Pam Damoff: Is it ever destroyed?

Ms. Shelly Bruce: Oh yes.

Ms. Pam Damoff: Is that public?

Mr. Scott Millar: We're required to, yes. There's a test right now that if it's not essential to international affairs, security, and defence, then that information has to be destroyed, and then we're reviewed for that.

Ms. Shelly Bruce: If it's retained, then it's protected.

Ms. Pam Damoff: What if it is essential to Canadian national security, if you're out trolling the Internet and you find something going on here, and it's a Canadian? What happens to that information?

Ms. Shelly Bruce: CSE doesn't really troll the Internet.

Ms. Pam Damoff: Sorry, that was a bad term—my apologies. I guess what I was saying is that you're not actively going out trying to find a Canadian—

Ms. Shelly Bruce: Absolutely not.

Ms. Pam Damoff: —but you're out there and you're monitoring things and a Canadian happens to fall into that. They haven't necessarily committed a crime, but they're implicated in the conversations that are happening. What do you do with that information?

Ms. Shelly Bruce: As my colleague mentioned, if in the course of targeting and directing our activities at foreign entities that are outside of Canada and are associated with a foreign intelligence requirement that the government has levied against us, we come across information about a Canadian that is not germane to the foreign intelligence at hand, then we destroy that information.

Ms. Pam Damoff: What if it's germane to Canada? What if you've collected something and it could pose and security threat? There was some mention about "unless it's a national security threat". What if you're collecting this information, and a Canadian could be implicated in a Canadian national security issue? You don't notify anybody and it just sits there?

Ms. Shelly Bruce: We do. If the information is germane to the foreign intelligence reporting that we're doing about a legitimate threat to the security of Canada, we would include that information and we would write it in an intelligence product, which would be circulated to clients within the Government of Canada who have top secret clearance and who are indoctrinated to receive the information. But that information would not explicitly identify a Canadian. It would have a term that has been used instead of the specific details. If the client who is receiving that information wanted to understand the underlying information, what's behind that marker, they can make an application to CSE in accordance with the Privacy Act. They have to create a justification. They have explain how it relates to their mandate and why they have the lawful authority to have this information. Then CSE may release that, and it will be logged and reviewed by the CSE commissioner on an annual basis.

Ms. Pam Damoff: One of the things I've asked a number of witnesses here—and I guess that's where it would come in—is whether ministerial authorization should be involved if you're going to be releasing that information to other departments when Canadians are involved. A number of witnesses here have said yes, it should.

Mr. Scott Millar: How the ministerial authorizations and the capture are distinct from publicly available information is that under the ministerial authorizations, for any information that we acquire where there's a reasonable expectation of privacy or we might interfere with it, that information is brought into the ambit of the ministerial authorization and also the secondary review by the intelligence commissioner.

That authorizes us to undertake a series of activities in support of the foreign intelligence mandate.

Ms. Pam Damoff: But I'm specifically talking about your sharing that information. You take your information and give it to CSIS. Right now, they apply, you decide, and you give it to them. Do we already have a ministerial authorization in the middle of it, that before you release any information on Canadians to another government agency you need that authorization?

Mr. Scott Millar: I guess the only thing I would say is that there are privacy protections that have to be laid out in the ministerial authorization. As well, the minister will designate under the proposed CSE Act who can receive that information. That is a new element in that ministerial designation, so the minister will be engaged. The commissioner will be engaged with the activities undertaken within a ministerial authorization, and NSIRA will review them as well.

● (1135)

Mr. Malcolm Brown: This is a really important question, and not just for the mythology around what CSE does or other organizations like CSE do in other countries.

The reality is there are layers of protection for the transfer of information to protect privacy, but also to ensure that information is shared in a timely way, and there are layers of review. We have all the things that Scott and Shelly have described governing the way they do it. It's not willy-nilly, that we'll just toss it over.

Ms. Pam Damoff: No, and I wasn't implying that.

Mr. Malcolm Brown: I know you weren't, but for greater certainty, I'm trying to make that point.

In that context, the other point is that the receiving organization has a whole series of obligations as well, in the way they treat that information. Our friend the Privacy Commissioner—and he is a friend—plays an important role in all of that. As well, people like me who run these departments have very serious obligations in protecting the way that information is used, and ensuring and justifying its retention for however long we might feel we need to have it.

Ms. Pam Damoff: I think the world has changed; 20 years ago the conversation would have been much different. You're talking about personal conversations. They might be phone conversations. Now you have so much personal information out there on the Internet, and the information you can gather is so much wider. Therefore, it's a very different conversation from what we would have had even 10 years ago.

Mr. Malcolm Brown: Yes and no. The way that warrants are now used by the authorities that all of these agencies have to go through to access information is a long tradition. The reality is that yes, it's different, but the underlying principles and the foundation in law are the same in the way information is treated. We have to update our procedures and practices, and from time to time examine and ensure that they're still relevant. I think what's in Bill C-59 demonstrates quite a capacity to absorb and propose change. It's important not to think that it's so different that we have to jump to a new framework —not immediately, because we have to think through the consequences.

I think the challenge is to find the right balance to ensure that the concerns you're describing, about people feeling their information isn't being shared willy-nilly, are addressed by the way we manage the information. The layers of scrutiny that are embedded in this bill are so significant that I think.... We'll see, it's a prediction, and I know I've got to stop because I'm taking up your time, but this is an important issue. You have heard witnesses who feel the layers of scrutiny embedded in this bill are too much of a burden.

The Chair: Yes. Thank you, Mr. Brown, and I emphasize to colleagues that we do have a second hour and you can come back to these issues if they raise serious concerns in your mind.

Mr. Motz, you have five minutes, please.

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

Thank you to the officials for being here.

I appreciate your role as bureaucrats and your hesitancy sometimes maybe to speak freely in a committee like this on a matter like this, but we know this is a national security issue and it's a chance we have while the bill is before us before second reading to make any adjustments, which we probably need, obviously.

I'm going to start with you, Ms. Bruce, and I'll ask Mr. Brown the same question as well.

You spoke about active and defensive cyber operations. The legislation here in this bill sets out some very clear limits on its authorities, and prohibits directing active cyber operations at Canadians, as I read it, regardless of where they might be in the world when that happens, or any person in Canada.

Are you confident or satisfied that these limitations and prohibitions are appropriate, given our current climate of domestic threats with Canadians on Canadian soil?

● (1140)

Ms. Shelly Bruce: Thank you for your question.

I believe that the authorities that have been given to CSE in this bill reflect where our capabilities and our focus best lie, and that's with foreign targets outside of Canada and on foreign infrastructure.

If there is a threat that materializes within Canada, we have the RCMP and CSIS that are already well placed with authorities to manage those threats. I think it plays to CSE's strengths and to where it naturally gravitates in that global network.

Mr. Malcolm Brown: The short answer is yes. I can enthusiastically respond in the affirmative that I think we are well positioned to be able to respond. The act gives a much more complete range of authorities, with the appropriate safeguards. I think our friends in CSIS have views on the same subject, if you'd permit them.

Mr. Glen Motz: Yes, I definitely want, as a continuation, to ask CSIS and our RCMP witnesses who are here whether they share the same enthusiasm and support for this bill providing them the legislative support they need to protect Canadians from domestic terrorism.

Ms. Tricia Geddes: Yes, sir, I'll speak for the service, first of all.

I would say that this is a clear expression of our authorities and our tools: data analytics, threat reduction, and the way in which we operate with human sources. I think these are really important clarifications that have been made.

To your question to Ms. Bruce, I would say that this is where our mandates are quite complementary because, of course, the threat reduction mandate and our role in cyber operations are permitted here in Canada, so this is where I think there is a nice synergy between what CSE is able to do and what we're able to do.

D/Commr Gilles Michaud: Maybe I can add something from a law enforcement perspective. This bill really touches more on changes to the Criminal Code and some of the provisions that exist there to assist us in making sure we keep Canadians safe.

It does not address the technological challenges that we have—and the essence of your questions were the backdrop of that. That would be where we have the biggest gap, from a law enforcement perspective. It's in our ability to navigate within our mandate with this new environment and these new challenges.

However, I'm not sure this is the bill that aims to address those issues.

Mr. Glen Motz: Thank you.

I apologize. At the beginning of my remarks, I used the term "bureaucrats". I should have said "public servants", so I apologize for that. I didn't mean it as a slam in any way, whatsoever. I apologize.

There are legitimate concerns that have been expressed about foreign interference in our electoral process, as has been alleged to have occurred in our 2015 election.

Are there enough oversight powers in Bill C-59 to deal with foreign threats to our electoral process?

Mr. Malcolm Brown: The whole question of foreign interference is very complex. It is, to be frank, a mixture of digital and analog. The reality is that the objectives are the same. In many cases, probably, the actors are the same. With regard to the additional powers or authorities you've already discussed with Shelly Bruce, I would say those are clearly filling a gap.

As for the other authorities, interference has been and remains a longstanding concern of the services in the Public Safety portfolio. I think the updating, the modernization, of the tools across the spectrum puts us in a much better position to manage these challenges.

Is it the final word? I think it's a mug's game to sort of say that we've done it and that we don't need to think about it. I think it's something that we're constantly examining, as we examine every threat, and we would provide advice to the government when and if we think there are issues where there are gaps.

● (1145)

The Chair: Thank you.

[*Translation*]

Mr. Picard, you have five minutes.

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

My question is for the representatives of the Communications Security Establishment.

You may be testifying before the committee for the first time, but you must know that your organization is central to the legal framework we are studying. We are talking about foreign threats. Given that you do not handle what happens on Canadian soil, if, in your surveillance and interdiction efforts, you were to hear a conversation involving a Canadian citizen, you would be required to destroy this information. Defending the rights and freedoms and protecting the lives of Canadians are always the excuses given. You would have to prove that there is a threat or a reasonable suspicion of a threat to obtain the warrants required to investigate.

How can you prove that there is a threat if, by destroying information concerning Canadians, you lose information about behaviour or behaviour patterns that could be used as proof of an emerging threat?

Obviously, my assumption is that the source is in another country but is relying on co-operation from Canadians.

Ms. Shelly Bruce: Thank you for your question.

[*English*]

In the case where we have acquired foreign intelligence intercepts that contain information about a Canadian that is germane and that does indicate that there's a threat vector to Canada, or that there are reasonable grounds to believe that it could be related to a threat, we keep that information. We do not destroy it.

I understand that, over time, patterns may build up, but those are the rules that we have. In the interest of protecting the privacy of Canadians, if at the time of review we determine there's no link or that it is not germane to the foreign intelligence, to a threat to Canada, then we destroy it.

[*Translation*]

Mr. Michel Picard: Your premise is a good one if you consider that the intercepted information is already a possible threat. That said, a person who is trying to recruit a Canadian does not ask, during their first conversation, if they are ready to kill for their country. That is rare. These people test the waters, evaluate their target and have mundane conversations, no matter who they recruit. The conversation is of no interest with regard to a possible threat because these people are only testing the waters.

Is that not a problem? At what point does the mundane conversation turn into a threat?

[*English*]

Ms. Shelly Bruce: As we are targeting foreign entities outside of Canada, we have to be very convinced that those foreign entities are linked to a foreign threat, or a foreign intelligence priority of the government. Just because that person is speaking once to somebody who has an innocuous conversation does not mean we stop targeting the foreign entity. Therefore, any subsequent conversations with that foreign entity would also be reviewed, and the analysts of those targets would appreciate, over time, if they sensed a change in the behaviour, or if there were a Canadian involved, he or she became more susceptible to radicalization.

[*Translation*]

Mr. Michel Picard: Thank you.

I would like to ask one last and more general question.

The most recent departmental report on the terrorist threat continues to indicate that the threat level is medium. This has not changed for four years. The last report for 2014 also indicated that the threat level was medium.

Does bill C-59 provide the tools required to keep the terrorist threat level at medium? Do you also have tools to help us reduce this threat level?

Mr. Malcolm Brown: Of course, I hope so. Seriously, there is no doubt that the bill contains important new tools to that end.

● (1150)

[*English*]

It's kind of a demand-driven environment. Can I say today—I'm making up a number—there are 15 threats and Bill C-59, or some version of it, is passed, and a year from now there will be 14? No.

Can I tell you I believe—and I think this is the view of the agencies—that Bill C-59 provides important tools and assets to help reduce the threats Canada faces? My response is the same as I gave earlier. Assuredly, yes. Does it reduce every threat? No.

The Chair: Thank you, Mr. Picard.

[*Translation*]

Mr. Paul-Hus, you have five minutes.

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

I have a quick question to ask you.

I would like to go back to foreign financing. I know that Global Affairs Canada can play a certain role, and I regret that the committee refused to invite people from that department to appear before us.

In order to block foreign financing, is your department or one of your organizations in contact with Global Affairs Canada?

[*English*]

Mr. Malcolm Brown: There's a broader interdepartmental group that tackles these issues: the Department of Finance, Global Affairs, FINTRAC, the RCMP, CSIS make up the portfolio, and some of our colleagues here. There is a broad group that looks at the financing of foreign terrorist organizations.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

I would like some explanations, but I am not sure who can provide them.

Several bodies report to the minister. We have the intelligence commissioner, the Privacy Commissioner, the new Committee of Parliamentarians. Several groups report in the interests of protecting privacy. But what about the operational aspect? I want to know how you will interact with all these groups and how that is going to work, especially in the case of CSIS.

Ms. Tricia Geddes: Thank you for your question.

[*English*]

I do believe we have an obligation to our minister to ensure that we are meeting all of these expectations when it comes to privacy. We are quite comfortable with review. We have had a long relationship with SIRC. It has been very good at ensuring that we are adhering to policies and procedures when it comes to the privacy of Canadians. The new bill actually introduces a number of new mechanisms to ensure that the privacy obligations are being met by the service.

As I said at the outset, it is extremely important to us to ensure that Canadians have confidence in their security agencies. So I don't think we are concerned about it. I think that the privacy answers we would be giving to the Privacy Commissioner or our review agencies would be identical, frankly.

[*Translation*]

Mr. Pierre Paul-Hus: We agree that protecting privacy is important to Canada, but can all these new players have a negative impact on security? Does the fact that there are many players run the risk of compromising national security? Is the balance between protecting privacy and national security an issue for you?

[*English*]

Ms. Tricia Geddes: Not in my opinion. As I've said, I honestly believe it's critical to have the confidence of Canadians. I think operations can be slowed down if Canadians lose confidence in the security agencies, or if, for example, we have to stop and fence off data. It's therefore critical to ensure that we have public confidence if we want to move swiftly through operations.

[*Translation*]

Mr. Pierre Paul-Hus: In a broader context, Bill C-59 was referred to the committee before going through second reading in the House of Commons. The minister wanted us to check whether improvements could be made to some elements of that huge bill. As public servants, you worked on developing the bill.

Now, in insight, would you say to the committee that the situation has changed or there are elements you had not considered at the time? You know how things are being done now. Are there any changes we could propose as amendments?

● (1155)

[*English*]

The Chair: There is a greater likelihood that you will be responding to the minister on that question, Mr. Paul-Hus.

Mr. Malcolm Brown: As good bureaucrats—

Voices: Oh, oh!

Mr. Malcolm Brown: —and here I'll speak for everyone.... You will understand that the advice we provide on this is given to the federal cabinet through our ministers. I will say, though, that I think the minister has made it clear that he, likeMinister Sajjan, is open to suggestions on how to improve the legislation. We look forward to advice. As I think we have both indicated, we've been in conversations with stakeholders, and these conversations continue to be held. We look forward to the advice of the committee on what the changes might be, and we will respond.

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

Ms. Dabrusin.

Ms. Julie Dabrusin (Toronto—Danforth, Lib.): Thank you.

We've been touching on a lot of issues surrounding the reasonable expectation of privacy. I might start there. This is a question relating to part 3 of the bill. I've read about this in a few places. I think it has been suggested by Professor Forcese and by the BCCLA that there should be amendments made to subclauses 23(3) and 23(4). The changes would add some words.

The existing subclause 23(1) reads:

> Activities carried out by the Establishment in furtherance of the foreign intelligence, cyber-security 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.

The suggested amendments would add the words, "involve the acquisition of information in which a Canadian or person in Canada has a reasonable expectation of privacy."

Then the text would go back to the wording that we now have in subclause 23(3), namely, "unless they are carried out under an authorization issued under subsection 27(1) or 41(1)."

Because we've been talking a fair bit about reasonable expectations of privacy and how we manage the constraints of adding that in, do you think this concern is covered by other parts or layers of the legislation, or do you see the value of making additions? I'm not asking from a policy point of view, but am trying to see if you see it covered somewhere else.

Mr. Malcolm Brown: I think this is a proposal by Professor Forcese, correct? I think we're a little constrained as public servants in responding to that. You said your question is not about policy, but frankly it is.

I will let Scott take a stab at trying to respond to the technical aspect of what you have raised.

Mr. Scott Millar: We are subject to the charter, and not all the elements of the charter are here. All legislation and activities are subject to the charter. As to where we interfere with the reasonable expectation of privacy, right now we operate under the understanding that any kind of information is subject to ministerial authorization. The only thing I would say is that Professor Forcese's suggestion on explicit mention is not inconsistent with the implicit requirement of a reasonable expectation of privacy and that this information needs to be covered under the ministerial authorization.

Ms. Julie Dabrusin: Okay, thanks.

I was reading an interesting piece on the CSE by the Citizen Lab, which said that in providing defensive services, ultimately there may have to be, say, purchases of malware or different types of things of that sort. How would we protect ourselves in our defensive operations from the people who are developing the problems that are causing us to engage in those defensive operations?

● (1200)

Ms. Shelly Bruce: The purchase of malware doesn't necessarily come from those people who are generating the malware. There are organizations, anti-virus companies, who will allow us to purchase that information from their own legitimate analysis and work. We work very closely with that community to understand what the threats are that are being covered by a commercial software and services so that we can focus, then, on those malware threats that are not currently covered, the more sophisticated ones that are not part of the current complement.

Ms. Julie Dabrusin: We've talked a little bit about publicly available information. I think one of the things that is maybe complicating things is that there are different layers of what people consider public. One thing that's been raised by some folks is, what if there is, for example, a hacking incident, and suddenly this information is made public? It's out there, but it was intended to be private in its first instance. How does that fall within the scope of public information? What are our safeguards there?

Ms. Shelly Bruce: In CSE's instance, that information, anything that has been hacked or stolen and then been made available for purchase, is not included in the definition of publicly available information.

The Chair: Thank you, Ms. Dabrusin.

Mr. Dubé, you have the final five minutes, please.

Mr. Matthew Dubé: Thank you very much.

Just on the active cyber operations, the minister of National Defence is the one calling the shots, if you'll allow me to use that expression, and you exist through the National Defence Act. But the CSE—and I know the answer to this, but just for the record—is a civilian organization, correct?

Ms. Shelly Bruce: That's correct.

Mr. Matthew Dubé: When cyber operations are being undertaken, you referred in your presentation—I'm going with the notes—to "cyber aggression by foreign states". You are not phrasing cyber aggression as an act of war per se. You also refer to disrupting "cyber aggression by foreign states". Is there not concern that a civilian organization answering to the Minister of National Defence, in essentially undertaking offensive actions against another state, could be perceived as engaging in an act or war? What would be the legal consequences of that? We've had witnesses who've explained that, because legally you're seen as a civilian organization, that muddies the waters significantly. That's where a lot of the concern comes from. I don't necessarily feel you've addressed that in your comments.

Ms. Shelly Bruce: There is no doubt that Canada and its allies face an increasing degree of threat from hostile state actors or hostile non-state actors out there. We work very closely with and are part of the National Defence portfolio, as you've mentioned. In the recent defence policy review, the military has declared its interest in working in the cyber domain and developing a framework and a platform for that. You'll note as well that the bill is set up in a way that would allow CSE to assist the Canadian Armed Forces under our assistance mandate, so that we would be able to work more closely with them, depending on the conditions and circumstances of activities that would need to be taken. There is a potential for us to work more closely in delivering capabilities for them on the military level.

Mr. Matthew Dubé: Just to be clear, if we need what I would almost call a counterattack to something being done by a foreign state actor, and the military is developing similar capabilities to what CSE has, if you're the Minister of National Defence, how do you respond? Are you looking to the military to take that action, or are you looking to CSE? If the military is developing those capabilities, why should a civilian organization be taking action that a military actor could take against a foreign state?

Ms. Shelly Bruce: It depends on the circumstances of the activity that is being defended against. In many cases, you will not be able to attribute that activity to a specific individual, but the more important issue is to stop that activity from happening before it becomes a crisis or before it materializes in the Canadian security space.

Mr. Matthew Dubé: Which would fall under defensive operations, then, and not active ones.

Mr. Scott Millar: I would add that the capability exists with CSE now. One of the reasons National Defence and the Canadian Armed Forces have been added to our assistance mandate is that should they engage in cyber operations in support of government-approved military operations, they could leverage our capabilities in that regard. Where it's in a military context, leveraging us, when it's outside of a military context....

We have to keep in mind that some of the things we're talking about here would be, for example, if intellectual property were stolen from a Canadian company, we could perhaps go upstream and render that unreadable. This is not always in the stream of aggression and cyber-war, and that kind of thing. There are civilian uses of this and there are prohibitions built in to keep us within the swim lane of that, whether it's prohibitions against bodily harm and the like.... Having the dual key of the Minister of National Defence and the Minister of Foreign Affairs ensures that the kinds of activities we're undertaking are consistent with international priorities and international law.

● (1205)

The Chair: Thank you.

That completes our first round of questioning, but in keeping with our stellar reputation as the hardest working committee on the Hill, we will have no lunch break and continue with a second round of questions.

I want to canvass colleagues as to whether we could drop it to five-minute questions and just go back and forth, using a similar structure, but for five minutes each. That would give us an opportunity to possibly get in two more questions.

Mr. Dubé.

Mr. Matthew Dubé: Using the same rotation, I have five minutes, and I get bumped down five or six speaking spots with only a five-minute round at the outset. Is that....?

The Chair: Well, if you look at the clock, you're cooked if I stay with the current structure. I'd take two five-minute rounds as opposed to one seven-minute round.

Mr. Matthew Dubé: If I discuss for seven and five, then I would get two fives instead?

The Chair: Yes. I know your level of generosity with your time is appreciated.

Mr. Fragiskatos, five minutes.

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

Thank you for all of the work that you're doing and for being here today.

My first question is for Ms. Bruce. Could you reiterate the types of acts that would constitute an offensive cyber capability, with particular examples, if you could?

Ms. Shelly Bruce: Sure.

I would preface this by saying that active cyber operations are meant to achieve an objective that the government has established, and that it's a team sport. That means we each are bringing our mandates, our authorities, and our capabilities to this table. It really is a way of working together to figure out who has the right authority to address the right issue at the right time based on their skills, their mandates, and their authorities.

In the case of CSE, I mentioned some of these operations in my opening remarks, such as interrupting or disrupting ISIL communications, networks, media machines in a way that would stop attack-planning before things reached a crisis pitch. There's also interrupting the spread of ransomware that's being pushed around the world, and interrupting subversion to the democratic process. As my colleague mentioned, we have had instances in the past where sensitive information has been stolen from Canadian systems and is now on foreign systems abroad; therefore, we could find ways to corrupt that data or to make it inaccessible to others who want to take advantage of it and use it for their own benefit.

Mr. Peter Fragiskatos: Finding ways to protect banking systems, finding ways to protect potential attacks on electricity systems, for instance, are they all part of it?

Ms. Shelly Bruce: Yes, critical infrastructure is included. In the legislative proposal, CSE would receive the authority to take the skills and the technology and the capabilities that have been developed to protect Government of Canada networks and to make that advice, guidance, and those services available to critical infrastructure owners if that critical infrastructure element has been designated by the minister as eligible for CSE assistance, and if that critical infrastructure element system owner has requested our assistance.

Mr. Peter Fragiskatos: I asked the question because I think it's quite important to demystify some of the ideas around what actually constitutes an offensive cyber capability. This is obviously a new means of ensuring national security and I think there are some myths built up around it.

For instance, this committee has heard testimony from organizations such as OpenMedia, the BC Civil Liberties Association, with the former implying quite directly that this committee and Canadians in general ought be on the watch, because the CSE could use this offensive cyber capability to undermine the democratic process of other states. This is not the intent here, correct?

Ms. Shelly Bruce: No. The active cyber operations directed at foreign entities outside of Canada require the approval of the Minister of Defence as well as the Minister of Foreign Affairs. Necessity, reasonableness, and proportionality are all factors they have to consider. They cannot be achieved by any other means, cannot cause bodily harm or death, but also cannot subvert or obstruct democracy or the course of justice. There's an explicit prohibition there.

● (1210)

Mr. Peter Fragiskatos: Okay, thank you very much for that reassurance.

Can you comment on where the proposed new offensive cyber capabilities that Bill C-59 offers would take us in comparison with our Five Eyes allies in this particular area?

Ms. Shelly Bruce: I am not an expert on all of our allies' authorities, but this generally brings us in line with the activities and the authorities that they have at their disposal, and positions us to be a coalition partner in various broader activities that go beyond a national scope.

Mr. Peter Fragiskatos: Thank you very much.

If I could, with the last question here, I'll ask anyone who wishes to to take it. I've been reading the 2017 public report on the terrorist threat to Canada, produced by Public Safety. In that report, there are a number of references to far-right extremism and what that means for Canada from a terrorist-threat perspective. The report says that a dedicated module on extreme right-wing groups is currently under development. It's being developed by the first responder terrorism awareness program team. The report says that while far-right activity, far-right extremism, has always been a concern, this is the first time—at least that's what the report implies—that a dedicated approach in the form of a module here has been created. Does this mean that the Department of Public Safety is particularly concerned, now more than ever, about the threat of far-right extremism in Canada?

The Chair: Unfortunately, Mr. Fragiskatos's time has expired, which is partly my fault, but I'm going to get you to respond, if you could, briefly so that we can get in as many questions as we can.

Mr. Malcolm Brown: Really briefly, I'm not sure I can say more than ever, but I will ask Gilles Michaud to respond to the specific question.

D/Commr Gilles Michaud: That specific module is really a law-enforcement push. We've seen the increase in activities, and we would say that an aspect of the threat that we have is that we had taken our eyes off the ball, I guess, for a number of years. Right now there's a push to really delve into it. With our police of jurisdiction, because that's mainly where those activities occur and where the responsibility lies, we're trying to get a better understanding as to the existence of that threat and the level.

The Chair: Thank you, Mr. Fragiskatos.

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

Mr. Glen Motz: Thank you, Mr. Chair.

Thank you again to the group for being here.

Back on November 30, when many of you were here, I asked for a full costing for the implementation of this bill to been done. I don't see that it was submitted to the committee. If you have, that's great. If you have not, could you please do that for us? If it could be specific to compliance requirements and the extra costs for this bill, that would be awesome. Thank you.

I want to get into the—

The Chair: Hold on for a second, Mr. Motz. Are you asking for that to be an undertaking to the committee?

Mr. Glen Motz: Yes, please.

The Chair: Mr. Brown would say yea or nay.

Mr. Malcolm Brown: Yea.

The Chair: Okay.

Mr. Malcolm Brown: Is “nay” an option?

Voices: Oh, oh!

Mr. Malcolm Brown: We'll endeavour to provide—

The Chair: You could claim some vague cabinet confidentiality or something.

Mr. Malcolm Brown: There's some constraint, but I think we can provide more information. As I was prepping for this yesterday, I have to say that I noticed you had asked the question and that we hadn't responded, so we will respond to the specific question and some other.... It may come in, in sequence, but we'll get you some answers.

Mr. Glen Motz: In light of the recent domestic terrorist attacks in the U.K., in Europe, and obviously here in Canada, which involved acquisition and the use of objects available to citizens—chemicals, vehicles, whatever—has the government reviewed the revisions in Bill C-59 to ensure that it permits appropriate emergency disruptive activities, specifically to CSIS, including without warrants where required? Are you satisfied with disruptive powers under this bill?

Ms. Tricia Geddes: Yes, I think we're very satisfied with this. We're glad to see that the government has reaffirmed its commitment to our warranted powers. I think it's another set of tools for the government to be able to respond, especially when threats are very fast-paced and emerge quite quickly from time to time. Obviously, we work very closely with the RCMP, but it is a very effective tool.

● (1215)

Mr. Glen Motz: I'm going to ask this follow-up question to that and have both colleagues from the RCMP answer it as well.

Is there anything we can improve in that area, in this bill, that isn't there yet? Is there anything about which you, on second thought, thought, “You know what, it would be great if we had this in it”?

The Chair: It's not likely they can actually answer that question.

Mr. Glen Motz: I appreciate that, but you'd think there would be some freedom to get this right.

Mr. Malcolm Brown: If I might, I think we're happy to take advice from the committee on how the bill might be improved, and then the government will undertake its assessment of those suggestions.

Mr. Glen Motz: Now I want to use the bureaucratic term again, but that's okay, I won't.

Mr. Malcolm Brown: Sometimes if it walks and talks—

Mr. Glen Motz: I hear you.

Thank you.

So the RCMP shares the same sentiment that the bill contains the provisions necessary and that it permits, where appropriate, the emergency disruptive activities without warrant that you require?

D/Commr Gilles Michaud: A lot of those authorities exist outside the bill, and we already possess them in order to intervene and disrupt any type of emerging threat.

Mr. Glen Motz: So with this bill, CSIS officers would have the authority in defined exigent circumstances to perform disruption activities to prevent imminent attack without a warrant?

Ms. Tricia Geddes: I'm just conferring with my colleague here.

Merydee, go ahead.

Ms. Merydee Duthie (Special Advisor, Canadian Security Intelligence Service): Threat reduction measures can be carried out with or without a warrant. The bill doesn't address the issue of exigent circumstances. Non-warranted measures can be carried out and, really, the time constraint is internal in terms of all the processes we have to go through and the consultation with our partners to make sure that it is the appropriate course of action.

Mr. Glen Motz: Thank you.

Go ahead.

Ms. Tricia Geddes: Can I just add that in those exigent circumstances it would more than likely be the RCMP that would be acting in those situations.

Mr. Glen Motz: Thank you.

I have a little bit of time left, I'm sure.

I have one yes or no question. A previous witness at this committee expressed concern and suggested that if Bill C-59 passes as written—and this applies I suppose to you, Ms. Bruce—then CSE may interfere in the democratic electoral process in another country.

Can you please confirm that CSE has no intention of using its new powers to interfere in any democratic electoral process in any foreign country?

Ms. Shelly Bruce: Yes, sir, in fact there's an explicit prohibition in the act that ensures that any active cyber operation is not used to pervert or obstruct the course of justice or democracy.

Mr. Glen Motz: Thank you.

The Chair: I can think of at least one head of state who would be relieved about that.

Mr. Dubé.

Mr. Matthew Dubé: It's not a party position, I imagine.

My question is for CSE, to start, since this was discussed in your presentation, but it's also for CSIS, because it is mentioned in part 4 as much as it is in part 3 of the bill when it comes to the definition of "publicly available information".

The sense I've gotten from people who know about it better than I do and have been before the committee is that, up until now, there's been no definition in Canadian law and no jurisprudence about what publicly available information is.

You've defined it as the sort of public resources that would be available to anyone in Canada. One example that the Canadian Bar Association offered was that of information being sold by Facebook to advertisers—which arguably would be available to anyone if they were in that business. It's unclear to me whether we're talking about googling someone whose Facebook page doesn't have strong privacy settings, or whether we're actually talking about things that technically are available to anyone, but wouldn't actually be.

Therefore, my first question is, can you drill down that definition? My second one is why is there no definition in the bill or anywhere in Canadian law of this, and should there be a definition in the bill to make that more explicit?

Mr. Scott Millar: There are a few things. One is to make clear that this element is actually making explicit something that occurs now with respect to CSE. We use infrastructure information, which, as the legislation states, can be linked to an identifiable Canadian.

We do that to understand the global information infrastructure in which we operate. We use it in some of the other ways Shelly referred to in her statement, when she talked about how it has to be consistent with our mandate. We're not a domestic investigative agency. We don't build dossiers on Canadians and can't cross-reference data for the purpose of going deeper into any Canadian's private activities.

As well, as mentioned, stolen or hacked information would not be available for our use. I draw attention to Justice Canada and the charter statement it released at the time of the tabling of this bill, which talks about publicly available information and the reasons it is a different kind of beast than the kind of information that has attached to it the reasonable expectation of privacy and would be subsumed within the ambit of the ministerial authorization process.

● (1220)

Mr. Matthew Dubé: I have a follow-up question, but go ahead.

Ms. Tricia Geddes: Just with regard to your question on the social media, our collection and use of information is going to continue to be guided by the charter and by an individual's reasonable expectation of privacy, which as you know, is evolving over time. We're going to ensure that that's kept consistent.

Further, with regard to the hacked or stolen datasets, we do not consider those to be publicly available. We could envision a scenario, though, where if our adversaries had access to a hacked or stolen dataset, we might still want to have the ability to retain it, but that would only be through the normal authorization process. We would have to go to the Federal Court if it were Canadians' information, or to the Information Commissioner if it were foreign.

Mr. Scott Millar: May I just add to that?

I'm sorry, sir, but I didn't completely answer your last question.

Mr. Matthew Dubé: Add it quickly because I have some—

Mr. Scott Millar: Publicly available information is included in the definitions in part 3, so there is a specific definition.

Mr. Matthew Dubé: Sorry, I don't have it in front of me. The definition is...?

Mr. Scott Millar: You don't have the act in front of you, so I'll read it to you:

> publicly available information means information that has been published or broadcast for public consumption, is accessible to the public on the global information infrastructure or otherwise or is available to the public on request, by subscription or by purchase.

Mr. Matthew Dubé: All right. Thank you.

When it comes to information acquired incidentally, is there any notion of why that would be retained? Right now, I think, it's in proposed subsection 24(4), which talks about information acquired incidentally through the research that's done. Is there any reason that you would retain that information and not just put it back, throw the fish back in the water, if that's happening?

I'm not clear on the authorizations when it comes to proposed section 24. I'm pretty clear on the authorizations for information acquired incidentally for datasets with CSIS, but I'm less so on part 3.

Mr. Scott Millar: I would just say that, where there is that reasonable expectation of privacy, any information that we use... If there's any element of, say, information notwithstanding the publicly available information definition and those elements, if there is anything that hits that trigger of “reasonable expectation”, that's brought within the ministerial authorization process.

We still will have the element of privacy measures applying to publicly available information in case there is a privacy interest triggered, but again, given that the Privacy Act requires that we only collect, use, and retain information consistent with our mandate, we cannot go outside of that mandate and use it in different ways.

We will be, obviously, reviewed for reasonableness, necessity, and our privacy measures, so the degree to which there might be any concerns going forward on that would be, I would think, captured by that review agency and drawn to our minister's attention.

The Chair: Thank you.

Mr. Spengemann.

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

Ms. Bruce, in the first round we ran out of time as you were about to delegate to your colleague Mr. Millar on the question of, if that's the right term, rules of engagement for active cyber operations abroad. You then had a follow-up discussion with my colleague Mr. Fragiskatos.

Mr. Millar, is there anything else you'd like to add in terms of clarifying what the framework is for conducting active cyber activities abroad, what the safeguards are?

Mr. Scott Millar: No. I think it's been covered. I guess the only thing that I would clarify is that our legislation uses the terms “active” and “defensive”. The term “offensive” or what might constitute something that's more in the military space would be something under the authorities and remit of the Canadian Armed Forces.

Mr. Sven Spengemann: Thank you very much.

Mr. Brown, with regard to the issue of domestic violence, terrorism, extremism, radicalization—perhaps using as one anecdotal example the incident in Sainte-Foy just over a year ago—in your assessment, how important is our proactive work with Canadian young people? I have the sense that the vast majority of these cases do involve young people under 35 years of age. By my anecdotal knowledge, 60- and 70-year-olds don't self-radicalize. What do we need to do within the framework that we have? How important is this work to counter violence and radicalization, and what are its principal elements?

● (1225)

Mr. Malcolm Brown: There's no question that it's a very important element. The principal element is the work that's led by the Canada centre that operates out of the department. It works with local community groups and provides funding and support for initiatives in Montreal, Calgary, Toronto, and across the country, in part because the solutions for Calgary will be different from the solutions for Montreal. That's really a key part of our response to that particularly vulnerable age group.

Mr. Sven Spengemann: Are we, as Canada, out front on this challenge, or are there experiences among, say, the Five Eyes that could be useful in constructing our own framework?

Mr. Malcolm Brown: I would say actually we are leaders. We work closely, particularly but not only, with Five Eyes partners on understanding trends, but again in the same way that the interventions in Calgary are different from the interventions in Montreal, the interventions in Sydney, Australia, will be different from the interventions in Canada. I would say we are very well positioned relative to our colleagues, and based on conversations we've had at a recent G7 meeting in the fall, it was very clear that Canada is playing a leadership role.

Mr. Sven Spengemann: Thank you very much.

My final question is for Mr. Breithaupt. On the assumption that we're dealing primarily with young people when we talk about domestic terror threats or radicalization and extremist threats, do you have any thoughts on the current framework of the bill that speaks particularly to the Youth Criminal Justice Act provisions, clauses 159 to 167?

Are there any ideas, any thoughts with regard to improving those provisions, or are you satisfied this will adequately protect Canadian youth?

Mr. Douglas Breithaupt (Director and General Counsel, Criminal Law Policy Section, Department of Justice): Thank you for the question.

I will just talk a little bit about the proposed amendments. The Youth Criminal Justice Act recognizes that young persons have special guarantees of rights and freedoms, and it contains a number of significant legal safeguards to ensure they are treated fairly and their rights are fully protected. Part 8 of the bill is aimed at ensuring that all youth who are involved in the criminal justice system due to terrorism-related conduct are afforded enhanced procedural and other protections that the Youth Criminal Justice Act provides. It ensures, for example, that youth protections apply in relation to recognizance orders and clarifies that youth justice courts have exclusive jurisdiction to impose these orders on youth.

For example, if a young person were to come before a youth justice court on an application for a terrorism peace bond and is not represented by a lawyer, the amendments here would require the court to advise the young person of his or her right to retain and instruct counsel, refer the young person to any available legal aid program, and if the young person is unable to obtain counsel through the program, direct that young person to be represented by counsel provided by the state upon request of the young person.

There is more discussion internationally about the effects of terrorism on the juvenile justice system, and these proposals for amendments to the Youth Criminal Justice Act are to enhance protections of youth in proceedings where recognizance with conditions in terrorism peace bonds apply, but it also provides for access to youth records for the purposes of administering the Canadian passport order, subject to the privacy protections of the act.

The Chair: Thank you very much.

[*Translation*]

Mr. Paul-Hus, you have five minutes.

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

I will talk about ISIS fighters. We know that 180 Canadians decided to wage Jihad around the world, especially in Irak and Syria, but also in other places, including Africa. Some 60 of them are known and have returned to Canada. Ten of them are followed more closely by our police services and CSIS, but there is a legal problem. Will Bill C-59 help Canada take measures to enable it to prosecute those people, even if it means deporting dual citizens?

● (1230)

[*English*]

Mr. Malcolm Brown: There are no uniquely specific provisions in Bill C-59 to deal with the question of violent extremist travellers. There are elements of Bill C-59 that provide the tools and assets for the agencies that will improve our ability to safeguard Canada from any threats that may present. I will also say, though, that there is a variety of tools that are available to the government, to all of us here and others, to manage and assess and take action as necessary to protect Canadians and ensure, where there is the evidence, that prosecutions can be launched against these individuals.

[*Translation*]

Mr. Pierre Paul-Hus: There is an example I would like to look at with you.

Jack Letts, alias Jihadi Jack, has Canadian citizenship and British citizenship. Of course, Great Britain does not want to take him in. We heard on Friday that Mr. Letts and his mother were trying to put pressure on our government to allow him to come here, to Canada. There is an issue with evidence. If Mr. Letts enters Canada, he will be free before we know it because we have a problem. We don't have the evidence needed to detain him.

Do you have a relationship with Five Eyes governments or those of other countries—I assume you do—through which you could get evidence that could incriminate him here, or do we have no way to take action?

[*English*]

Mr. Malcolm Brown: When talking about a specific case, we are all constrained, so I think we'll need to respond to your question in a general way.

With that, I'll turn it over to Monsieur Michaud.

[*Translation*]

D/Commr Gilles Michaud: That is one example of many. When it's time to investigate Canadians who have gone abroad, the work begins abroad. We have relationships with different police forces, including the police force of Five Eyes or of other countries. We start to compile evidence. Once the individual arrives in the country, we can implement other measures to continue our work and to try to determine whether that individual does indeed represent a threat and whether we have the evidence needed to lay charges.

So there is a criminal aspect involved, as well as a preventive aspect. Some individuals who come back to the country don't necessarily have a criminal past. They had other roles to play for the cause. In that case, we use other organizations to get involved and try to help them move forward in the file as soon as the individuals return to Canada.

Mr. Pierre Paul-Hus: Thank you.

I want to talk about CSE's role. Currently, unless I am mistaken, the relationship between CSE and the Department of National Defence is one of funding and operations. Under Bill C-59, there will be a transfer, or a severing of CSE from the Department of National Defence. As a result, Public Safety Canada will have more responsibilities.

Is that indeed the case?

[*English*]

Mr. Scott Millar: Yes. We are a stand-alone agency, under the portfolio of the Minister of National Defence, and that is within the bill itself, as I mentioned.

[*Translation*]

Mr. Pierre Paul-Hus: Basically, I want to know whether you think the provisions of Bill C-59 will change things, or if your role will remain the same without changing significantly.

[*English*]

The Chair: Could you provide a quick answer, please?

Mr. Scott Millar: In terms of, just as we are, as a stand-alone agency, is there a change in that?

Mr. Pierre Paul-Hus: Operationally speaking.

Mr. Scott Millar: No. Obviously, in terms of the mandate additions, that would be new, but in terms of how we function within the defence portfolio, that remains the same. In fact, this legislation has these housekeeping provisions in it. Before, we were a stand-alone agency by way of an order in council in 2011. Now, we'll be more of a creature of legislation with the stand-alone act. Again, it will make a number of the provisions under which we operate transparent as well.

[*Translation*]

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

Mr. Picard, you have five minutes.

● (1235)

Mr. Michel Picard: My question is for CSIS and the RCMP. Throughout the bill, we note the absence of FINTRAC. That is not an oversight. There is no denying that terrorist financing is a reality. That said, the current trend is to keep reducing the cost of terrorist attacks. For example, a truck may be stolen and crashed into a crowd. The financial aspect has changed.

In the current modern circumstances, would it be a good idea to reconsider the link with FINTRAC? Are our legal methods for working with the organization enough to keep us from having to establish a link with FINTRAC in Bill C-59?

D/Commr Gilles Michaud: I think that our current relationship with FINTRAC and the existing legislation help us do our work. That actually gives us some flexibility. The threat can increase and be expressed in a certain way over a period of time, and then the method can change. We can always share information with FINTRAC. The legislation makes those exchanges possible under any circumstances.

Mr. Malcolm Brown: I would like to add that there is now a five-year review of the terrorism legislation....

[*English*]

John what's the full title of the act?

Mr. John Davies (Director General, National Security Policy, Department of Public Safety and Emergency Preparedness): The Proceeds of Crime (Money Laundering) and Terrorist Financing Act is now in its five-year review. The Department of Finance has put out a discussion paper asking for feedback on how to improve the act.

Ms. Tricia Geddes: I would concur with my colleague.

We work very closely with FINTRAC. I don't believe there are any changes required there. We invest in counterterrorism investigations, and terror financing is one aspect of that.

Mr. Michel Picard: Thank you.

[*Translation*]

Mr. Brown, Bill C-59 changes the powers to oversee the various agencies mentioned in it.

What impact will that have on the Civilian Review and Complaints Commission for the RCMP?

Mr. Malcolm Brown: I think that question was raised during the first hour. Of course, it will have a positive impact because

[*English*]

Agencies will, I think, have greater clarity over what their expectations are.

This was an issue that we discussed, frankly, in the early days of the deliberations around the legislation. There was a recognition that there were gaps in the accountability regime, and we wanted to ensure that those gaps were filled in a way that didn't have a direct and negative impact on the operational capabilities of the agencies. Part of that is through greater clarity and expectation.

The other expectation is quite clear, and it's in the NSICOP legislation, for example. We expect NSICOP and NSIRA to consult and work with each other to ensure that they don't overlap unnecessarily and that they coordinate their activities.

There's no question that this will result—I would think this is one of the objectives—in greater transparency and greater public understanding of what we all do on a daily basis.

We're also taking steps to simplify the process through the transparency initiative, where the objective is that information that shouldn't be withheld can be shared publicly. This should eliminate going through access to information or whatever kinds of processes are required to release information. If we can release it proactively, we're lightening the burden.

I fully recognize that there has been some commentary about an increased burden, but as Tricia has mentioned, each of the deputy heads have indicated that they welcome and can function effectively within the proposed framework for oversight and review.

The Chair: Thank you, Mr. Picard.

Mr. Motz, you have five minutes.

● (1240)

Mr. Glen Motz: Thank you, Mr. Chair.

My colleague started this conversation, and this issue was mentioned by a witness before this committee. It's the issue of intelligence and evidence, and the inability to bring intelligence gathered elsewhere into the courts as evidence without compromising national security, an informant, or other issues. Does this bill do anything to empower our law enforcement officials or Public Prosecutions on the issues of national security?

Mr. Malcolm Brown: You may have noticed some nodding and long faces. This is a very complicated issue.

Mr. Glen Motz: Yes.

Mr. Malcolm Brown: Working with our friends in the Department of Justice, there are conversations and discussions going on, because it is a Justice and Public Safety dialogue with our colleagues in the provinces and the territories. There is, I would say, a general consensus that we need to do better, but Bill C-59 doesn't propose changes. We are actively engaging with our colleagues in the Department of Justice, as I say, on ways to improve the status quo, and that also involves engagement with provincial jurisdictions.

Mr. Glen Motz: Thank you, Mr. Brown.

If I can be so bold as to interpret what you've just told me, it's that maybe Bill C-59 should be strengthened in that area?

Mr. Malcolm Brown: Well, that's for the committee to make a determination on.

Mr. Glen Motz: Yes, I appreciate that.

Mr. Malcolm Brown: I will say that it's a very complicated issue that, frankly, from the officials' perspective and engaging, I don't think I'm revealing anything.... I probably am, but....

Voices: Oh, oh!

Mr. Malcolm Brown: I don't think I'm revealing anything about our deliberations with provincial colleagues. It's an issue under active discussion and there is no consensus, and that is a problem, a challenge for all of us.

Mr. Glen Motz: I won't pursue that line. I would be so brave as to suggest, then, that just maybe Bill C-59 should include some provision to work with other departments in order to make that happen—and stronger, if I'm hearing what you're providing for us.

Mr. Malcolm Brown: I'm not sure we need a legislated provision for that. This is an issue that is really important, and we are, as I say, actively engaged. The challenge, to be frank, is that there are quite profound issues around the way information is gathered and the constraints on how it can be shared, the extent to which it's effective, and its impact on the functioning of the court system at both the federal and provincial levels.

There are discussions and processes currently under way, and I would say that officials are seized with trying to make progress. I think one of the challenges is that there are very strongly held views on this issue across the spectrum.

Mr. Glen Motz: Thank you, Mr. Brown.

Last, there's nothing I can see in this bill that really speaks to or deals with issues like the proposed takeover of Aecon and the sale of sensitive or national assets to China or other similar types of countries. Can you walk us through what role CSIS might play in this process and if there are any changes needed in this act to improve that?

Other departments here can also comment in the time that I have remaining.

Ms. Tricia Geddes: Certainly this is part of our mandate, and we participate with other government agencies and departments in providing advice to the government. That is obviously quite secret advice that we provide, but the Governor in Council can certainly allow, disallow, or impose mitigation measures on investments. You probably know how the process works. We do have capacity within CSIS to support this, but as you note, it is certainly an area where there is a significant amount of pressure, and it requires a considerable amount of effort from the service.

Mr. Glen Motz: Does Bill C-59 offer any strength to your role in that process?

Ms. Tricia Geddes: I think the tools and the authorities that we're provided in Bill C-59 —I would probably look at the data analytics provision as one example—are certainly going to support us in that work.

● (1245)

The Chair: Ms. Damoff, you have five minutes.

Ms. Pam Damoff: Thank you, Mr. Chair. I just have one question, following up the questions that my colleague was asking.

In terms of changes that have been made in Bill C-59 to the CRCC, the Civilian Review and Complaints Commission, and the RCMP specifically, how will these impact the RCMP, and do you anticipate that the latter will work better under Bill C-59? Can you give us a little more information?

Mr. Brown, I'm not sure whether it would be you or the RCMP who would respond to that.

Mr. Malcolm Brown: Really briefly, in some ways we're trying to clarify where CRCC's lines are and where NSIRA will be in terms of the conduct of national security reviews. I think conduct complaints and those kinds of things are clarified.

Gilles.

D/Commr Gilles Michaud: From an agency perspective, that is a welcome change, because when it comes to our national security mandate, very rarely do we exercise it in isolation. It's always working with our partners, those who are sitting at the table: CBSA, and so on. As a review is ordered on some of our activities, it is very difficult for a single agency to look at it unless you look across the spectrum of those who are involved.

From our perspective, it is a welcome change.

Ms. Pam Damoff: Thank you. I don't have any other questions.

The Chair: Thank you.

Mr. Dubé, you have five minutes, and then, shockingly, I might exercise a chair prerogative and ask a question or two of my own.

Mr. Matthew Dubé: Thank you, Chair.

This is perhaps for our representative from the Department of Justice, but in the charter compliance statement, there is mention about the expectation of privacy when it comes to publicly available information, which would be considered low for that type of information.

How is that concept changed in law in terms of the expectation that people have? I say that as someone who's not a lawyer. In other words, going back to that example, I think very few people are really aware of information that could be purchased legally, for example, that could technically fall under that definition. Is the expectation of privacy and the reasonable expectation of privacy changed in the advent of the use of things such as social media, where we can arguably state that there's a lack of knowledge on that front?

Mr. Scott Millar: I know that Doug is here more in the policy capacity than a charter expert capacity, so I'm happy to address that.

There are a couple of things to keep in mind. One, again, is that it will be reviewed for lawfulness. With the ministerial authorizations that we will have or will seek that capture any information that comes into our possession, where there would be reasonable expectation of privacy, when we put together those authorizations, the Department of Justice is part of reviewing those authorizations, which are like affidavits, to make sure that we've sufficiently captured that space.

As the publicly available information is laid out here, the idea is that it was public, it was intended to be public, so to that degree, any information we acquire under those provisions would have to meet those kinds of tests, and those tests will be reviewed and commented on going forward.

Mr. Matthew Dubé: If we take the example of assessing the nationality of an individual or organization, can you walk me through what that means specifically?

Ms. Shelly Bruce: As my colleague has already mentioned, this is not new. CSE has to take these kinds of unknown entities and elements of information and try to flesh them out to understand exactly what we're dealing with. It could be as simple as a Google search. It could be looking or working with other databases that are out there that might help us contextualize this. In the case of an IP address, there are registries that exist online that tell you where an IP address is geographically registered.

Mr. Matthew Dubé: When you say “other databases”, that's pretty wide open. Can you give an example of something such as that? That seems troubling to me, that kind of phrasing, with all due respect.

Ms. Shelly Bruce: Probably the best I can do to reassure you is to say that we've had a commissioner who has reviewed CSE's activities for privacy for more than 20 years. In assessing our activities and looking for privacy concerns or lawfulness, he touches on these kinds of activities, the open source research that we do to support our activities, because a lot of our activities require this to be effective. To my knowledge, he has never found any issue with the degree of research that CSE has done, the sources that we have accessed, or how we have handled and managed that information.

● (1250)

Mr. Scott Millar: No, that's correct.

I guess the other thing to underscore is that, again, these activities are in furtherance of our mandate. I think there's an important thing to underscore here, and it's something we haven't had the opportunity to talk about much yet. Keep in mind that some of those activities involve us doing cyber-security on Government of Canada networks and systems. They're the same networks that hold taxpayer information and employment insurance information—very sensitive, private Canadian information. Our sensors block up to a billion malicious cyber incidents a day. Those are cyber-threat actors looking for vulnerabilities or indeed trying to attack.

I mention that because I recognize, in the discussion about the degree to which private information is.... Are we dealing with both security and the privacy of information in a reasonable and proportionate way? I'll underscore as well that part of our mandate is actually protecting the private information of Canadians. The degree to which we do these activities is in furtherance of that kind of information protection mandate.

Mr. Matthew Dubé: In terms of the measures you take that aren't known to the public, this is the challenge, right? You mentioned that there are some things you do with regard to protecting the privacy of information in terms of, for example, what's in proposed section 25 and that kind of thing. Is there any way in which we as parliamentarians can be made aware of what's being done? Unfortunately, from my reading of the bill, it seems that these measures are there, you're saying you take them, and beyond that we don't necessarily know.

Ms. Shelly Bruce: On our website we do have a fact sheet that outlines the measures we take to protect privacy at the moment. As technology evolves, as information evolves, we need to make sure we are staying current and are adopting more and more effective measures to protect privacy. So they are not captured in legislation, they are captured in ministerial authorizations. The minister can lay out his expectations and he can increase those expectations and any parameters in terms of how we work as part of those authorizations, which are required to be renewed every year.

Mr. Scott Millar: If I may, I answered incompletely a previous question about what changes for us under this legislation. We talked about mandates and other things. The accountability and review measures build upon the existing robust measures we've had to date with the CSE commissioner, but that element of NSIRA, the review agency, with the committee of parliamentarians gives that element where folks who are cleared and can see the full aspect of what we do, whether in an unclassified or classified space, can review us for all those elements of reasonableness and proportionality.

The legislation also makes more transparent—as transparent as you can be in a piece of legislation—the activities that we undertake, under what restrictions we do them, and the prohibitions and so on. We are trying to put out more and more on our website. We are a clandestine agency that needs to act clandestinely in order to understand the threat picture and protect Canada. But we're getting out there. We're on Twitter. We're pushing out reports on democratic institutions and threats against democratic institutions. We'll always be looking for ways in which we can share more about what it is we do.

Ms. Shelly Bruce: I would say as well—

The Chair: Mr. Dubé is well past his time.

I do have a question, if you don't mind. I want to pick up on the exchange between Ms. Bruce and Mr. Fragiskatos concerning the private infrastructure, if you will.

This conversation has largely been devoted to public infrastructure. It reminded me of a conversation I had last week with a representative of the banking industry. His comment was that when we feed information into the security services, it just disappears and we never hear from them again. It seems to me that this cyber infrastructure is actually shared between the private and public sectors, and that Bill C-59 doesn't speak to—it's not obvious, at least—that private infrastructure piece. This issue has consumed the British. The British government has intervened quite actively in protecting private infrastructure.

First, on Bill C-59 as is, what contribution in terms of a framework does it make? Second, what is the next piece, if you will, in addressing that issue?

● (1255)

Ms. Shelly Bruce: The bill does not refer specifically to critical infrastructure, but I think it makes reference to non-governmental systems, which are tantamount to critical infrastructure, because as you say, our global information infrastructure is made up of public and private enterprises.

In that space, CSE, which is currently focused on defending and blocking activities on the government infrastructure, is limited right now to providing advice and guidance only to critical infrastructure owners in a way such that the information is available to the general public.

In this regard, Bill C-59 opens up CSE to take the expertise that has been developed—the tools, the capabilities.... In fact, some of that capability has been exposed to critical infrastructure owners in the form of a tool called “Assembly Line”. We've put it out there. It's a tool that was developed in-house, but we've made it available to others who can use it to help triage and understand malware that might be affecting their systems.

CSE would be able to go even further with this legislation to helping critical infrastructure owners who request our assistance and whom the minister has designated as eligible to receive assistance from CSE.

The Chair: How will that occur in a formal way? I can think of institutions that have massive structures, possibly as large as government structures. How will that operate in a practical way so that everyone's interest is protected?

Ms. Shelly Bruce: It's a good question.

As the legislation firms up and we understand what the scope is, should these authorities be granted it will be up to CSE to work with Public Safety, critical infrastructure owners, and the minister to look at where the risks are and to start designating and prioritizing, because as you point out, it will be impossible to address all of the concerns and all of the infrastructures that exist in Canada.

Mr. Malcolm Brown: Some of this falls under the ambit of the Minister of Public Safety. You're asking a framework question on the way in which the government is going to approach it. This is an important building block. It was a gap within CSE's mandates that they were constrained on the help they could provide in the existing context.

As I said before, the government is conducting a cyber-security review. The results of that will be available shortly, I hope. One of the key pieces in this—and here I would add that Public Safety manages the relationship with critical infrastructure sectors—is about knowing where to go, who to call when there's an issue. It's not about the size of the systems; it's about having the right connections. Right now, they sometimes call CSE, and they call our critical cyber-emergency response team, CCIRC, at Public Safety. We need to do a better job of coordinating that.

Much of this information is in an ecosystem where it needs to get shared really quickly, and that's a key role that CSE can play. It's about technical expertise. I will use the analogy of a fire. We send firefighters to a fire. In this instance, it might be one firefighter, because it's actually just a connection that needs to be made so that people understand that there's a fix, and this fix can be applied across the entire infrastructure.

There's an unnamed large American company that dealt with a lot of people's private data. It was one simple fix that was missed, and it had a profound impact on the entire organization.

It's important to frame this. I think we will see a further elaboration in the coming months. This is one important building block.

The Chair: Thank you, Mr. Brown, for that penultimate word.

Colleagues, we have one more day on this. We have two witnesses scheduled for next Thursday, but a certain unnamed academic has suggested that we hear from the Civilian Review and Complaints Commission for the RCMP. They are available, and I propose that we add them to the list. That will do it for Thursday. I also propose that the subcommittee get together Thursday afternoon, after we

have heard the witnesses, and sketch out how we'll get to clause-by-clause.

With that, I want to thank each and every one of you for your contribution to our deliberations. You've certainly been very able and responsive to all of the questions we've asked.

The meeting is adjourned.